



**Internet of Things
for Industry and Human Applications** VOLUME 3
ASSESSMENT and IMPLEMENTATION



Internet of Things for Industry and Human Applications

Volume 3
Assessment and Implementation



Ministry of Education and Science of Ukraine
National Aerospace University “Kharkiv Aviation Institute”

**Internet of Things for Industry and Human
Applications**

Volume 3

Assessment and Implementation

Edited by V. S. Kharchenko

Project ERASMUS+ ALIOT
“Internet of Things:
Emerging Curriculum for Industry and Human Applications”
(573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP)

2019

UDK 62:004=111

173

Reviewers: Dr. Mario Fusani, ISTI-CNR, Pisa, Italy
Dr. Olga Kordas, KTH University, Stockholm, Sweden
Viktor Kordas, KTH University, Stockholm, Sweden

I73 Internet of Things for Industry and Human Application. In Volumes 1-3. Volume 3. Assessment and Implementation / V. S. Kharchenko (ed.) – Ministry of Education and Science of Ukraine, National Aerospace University KhAI, 2019. – 918 p.

ISBN 978-617-7361-80-9

ISBN 978-617-7361-83-0

Three-volume book contains theoretical materials for lectures and training modules developed in frameworks of project “Internet of Things: Emerging Curriculum for Industry and Human Applications /ALIOT” (Project Number: 573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP, 2016-2019) funded by EU Program ERASMUS+. Volume 3 describes techniques and tools for creation, assessment and implementation of Internet of Things (IoT) in different industry and human domains. The book consists of 6 parts for corresponding training courses: IoT for smart energy grid (sections 32-35), IoT for smart buildings and cities (sections 36-39), IoT for intelligent transportation systems (sections 40-43), IoT for healthcare systems (sections 44-47), IoT for ecology, safety and security monitoring systems (sections 48-51), IoT for industrial systems (sections 52-56). The book prepared by Ukrainian university teams with support of EU academic colleagues of the ALIOT consortium.

The book is intended for MSc and PhD students studying IoT technologies, software and computer engineering and science, cyber security. It could be useful for lecturers of universities and training centers, researchers and developers of IoT systems.

Fig.: 305. Ref.: 721. Tables: 66.

Approved by Academic Council of National Aerospace University “Kharkiv Aviation Institute” (record № 4, December 19, 2018).

УДК 62:004=111

ISBN 978-617-7361-83-0

© R.M.Babakov, T.O.Biloborodova, A.O.Bojko, V.V.Bousher, E.V.Brezhniev, P.Y.Bykovyy, M.V.Derkach, Z.I.Dombrowskyi, S.I.Dotsenko, O.V.Drozd, H.V.Fesenko, O.S.Gerasin, G.M.Hladiy, O.O.Illiaschenko, V.S.Kharchenko, V.V.Kochan, M.O.Kolisnyk, Yu.P.Kondratenko, O.V.Korobko, O.V.Kozlov, Y.M.Krainyk, Y.O.Kritska, S.D.Leoshchenko, D.A.Maevsky, O.Yu.Maevskaya, O.M.Martynyuk, S.V.Morshchavka, M.P.Musiyenko, A.O.Oliinyk, O.O.Orehkov, O.R.Osolinskyi, A.V.Parkhomenko, D.V.Pavlenko, .O.Sachenko, I.S.Skarga-Bandurova, O.O.Solovyov, A.O.Stadnik, A.A.Strielkina, S.O.Subbotin, A.M.Topalov, D.D.Uzun, Al-Khafaji Ahmed Waleed, O.V.Yurchak, D.I.Zahorodnia, I.M.Zhuravska

This work is subject to copyright. All rights are reserved by the authors, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms, or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or here after developed.

Національний аерокосмічний університет
ім. М. Є. Жуковського «Харківський Авіаційний Інститут»

**Інтернет речей
для
індустріальних і гуманітарних застосунків**

Том 3

Оцінювання та впровадження

Редактор Харченко В.С.

Проект ERASMUS+ ALIOT
“Інтернет речей: нова освітня програма для потреб
промисловості та суспільства”
(573818-EPP-1-2016-1-UK-EPPKA2-SVHE-JP

2019

УДК 62:004=111

173

Рецензенти: Др. Маріо Фузані, ISTI-CNR, Піза, Італія
Др. Ольга Кордас, KTH University, Стокгольм, Швеція
Віктор Кордас, KTH University, Stockholm, Sweden

173 Інтернет речей для індустріальних і гуманітарних застосунків. У трьох томах. Том 3. Оцінювання та впровадження / За ред. В. С. Харченка. – Міністерство освіти і науки України, Національний аерокосмічний університет ХАІ, 2019. – 918 с.

ISBN 978-617-7361-80-9

ISBN 978-617-7361-83-0

Книга, що складається з трьох томів, містить теоретичні матеріали для лекцій та тренінгів, розроблених в рамках проекту Internet of Things: Emerging Curriculum for Industry and Human Applications / ALIOT, 573818-EPP-1-2016-1-UK-EPPKA2-SBHE-JP, 2016-2019, що фінансується програмою ЄС ERASMUS +. Том 3 описує методи і інструменти для створення, оцінки та впровадження Інтернету речей (IoT) в різних областях індустрії та гуманітарних застосунків. Книга складається з 6 частин для відповідних навчальних курсів: IoT для інтелектуальних енергосистем (розділи 32-35), IoT для інтелектуальних будівель і міст (розділи 36-39), IoT для інтелектуальних транспортних систем (розділи 40-43), IoT для медичних систем (розділи 44-47), IoT для систем моніторингу екології та безпеки (розділи 48-51), IoT для промислових систем (розділи 52-56).

Книга підготовлена українськими університетськими командами за підтримки колег з академічних закладів країн ЄС, що входять в консорціуму проекту ALIOT.

Книга призначена для магістрантів і аспірантів, які вивчають технології IoT, програмну і комп'ютерну інженерію, комп'ютерні науки. Може бути корисною для викладачів університетів і навчальних центрів, дослідників і розробників систем IoT.

Рис.: 350. Посилань: 721. Таблиць: 66.

Рекомендовано до видання вченою радою Національного аерокосмічного університету імені М.Є. Жуковського «Харківський авіаційний інститут» (протокол № 4 від 19 грудня 2018 г.).

УДК 62:004=111

ISBN 978-617-7361-83-0

© Р.М. Бабаков, Т.О. Білобородова, А.О. Бойко, В.В. Бушер, Є.В. Брежнев, П.Є. Биковий, М.В. Деркач, З.І. Домбровський, С.І. Доценко, О.В. Дрозд, Г.В. Фесенко, О.С. Герасін, Г.М. Гладій, О.О. Ілляшенко, В.С. Харченко, В.В. Кочан, М.О. Колісник, Ю.П. Кондратенко, О.В. Коробко, О.В. Козлов, Я.М. Крайник, Я.О. Критська, С.Д. Леошенко, Д.А. Маєвський, О. Ю. Масвська, О.М. Мартинюк, С.В. Моршавка, М.П. Мусянко, А.О. Олійник, О.О. Орехов, О.Р. Осолінський, А.В. Пархоменко, Д.В. Павленко, А.О. Саченко, І.С. Скарга-Бандурова, О.О. Соловьев, А.О. Стадник, А.А. Стрелкіна, С.О. Субботін, А.М. Топалов, Д.Д. Узун, Аль-хафаджі Ахмед Валід, О.В. Юрчак, Д.І. Загородня, І.М. Журавська

Ця робота захищена авторським правом. Всі права зарезервовані авторами, незалежно від того, чи стосується це всього матеріалу або його частини, зокрема права на переклади на інші мови, перевидання, повторне використання ілюстрацій, декламацію, трансляцію, відтворення на мікрофільмах або будь-яким іншим фізичним способом, а також передачу, зберігання та електронну адаптацію за допомогою комп'ютерного програмного забезпечення в будь-якому вигляді, або ж аналогічним або іншим відомим способом, або ж таким, який буде розроблений в майбутньому.

CONTENTS

Preface 11

PART IX. IOT FOR SMART ENERGY GRID 21

32. INTEGRATION OF IOT AND SMART GRID COMPONENTS 21

32.1. Structure of the integrated IoT and smart grid system..... 23

32.2 Communication protocols and interfaces of IoT smart grids 32

32.3 Cloud computing and Big Data as a part of the IoT smart grid... 44

32.4 Work related analysis 47

33. IOT INFRASTRUCTURE FOR SMART ENERGY GRID BASED ON EMBEDDED SYSTEMS DEVICES 53

33.1 Development of I&C and harvesting systems for local SEG 55

33.2 Hardware components for local SEG (sensors, measurement units, control units – Raspberry Pi, STM32 boards, ESP8266, PLC, Phoenix, etc.)..... 61

33.3 Software components of SEG..... 71

33.4 Work related analysis 77

34. AVAILABILITY ASSESSMENT OF IOT BASED IT INFRASTRUCTURE OF POWER GRIDS..... 83

Abbreviations 84

34.1 Reliability assessment of IoT based IT infrastructure 85

34.2 IoT based predictive diagnostics and maintenance of power grid equipment 100

34.2.3 Reliability and cyber-security issues for predictive analytics software based systems. Cases 109

34.3 Availability assessment of IoT based IT infrastructure 111

34.4 Work related analysis 123

35. IOT FOR SMART GRID SAFETY AND SECURITY MANAGEMENT	129
35.1 Introduction into smart grid safety and security	131
35.2 Analysis of smart grid safety and security	154
35.3 IoT based smart grid safety and security management system..	156
35.4 Resilience-oriented measurement of quality of IoT based smart grid service assess.....	171
35.5 Work related analysis	184
PART X. IOT FOR SMART BUILDINGS AND CITY	195
36. HIERARCHY AND INTERACTIONS BETWEEN SMART IOT SYSTEMS	195
36.1. Elements of system theory for IoT	197
36.2. Internet of Thing: Hierarchy of Smart Systems.....	203
36.3. Expert assessment method and its applications for the IoT risk analysis	208
36.4. Work related analysis.....	215
37. DEVELOPMENT OF SMART BUILDING AND CITY SYSTEMS	221
37.1 Classification of the building management system, the purpose and basic properties of control, executive and sensor elements.....	223
37.2 Organization of the interaction of subsystems and elements of Smart House and IoT	237
37.3. Construction of Smart House and IoT subsystems based on Moeller / Eaton xComfort.....	243
37.4 Work related analysis	245
38. ENGINEERING OF SOFTWARE/HARDWARE PLATFORM FOR SMART BUILDING SYSTEM	249
38.1 Embedded systems as the basis of the IoT infrastructure.....	251
38.2 Implementation of the software/hardware platform for Smart Building System	263

38.3 The application of the remote laboratory Smart House&IoT for Smart Building System prototyping	268
38.4 Work related analysis	276
39. TECHNOLOGIES OF INTERACTION IN THE SMART BUILDING AND CITY SYSTEMS.....	284
39.1 Technologies of component interactions in systems of IoT at the level of their formal specifications	286
39.2 Technologies of component interactions of Smart Building on a behavioural level	295
39.3 Technologies of component interactions of Smart City at the level of process synchronization	304
39.4 Work related analysis	313
PART XI. INTELLIGENT TRANSPORTATION SYSTEMS AND IOT	322
40. INTELLIGENT SYSTEM FOR MONITORING THE TRANSPORT FLOWS	322
40.1. Studying the hardware of traffic intensity monitoring	324
40.2. Recognition and data processing of objects in a video frame...341	
40.3. Recognizing and data processing of objects array in a video stream	356
40.4 Control system of the traffic flow intensity.....	365
40.5 Work related analysis	367
41. IOT FOR PUBLIC TRANSPORT INFORMATION SERVICE DELIVERING	373
41.1 Public transport (PT) systems.....	376
41.2 Tools and techniques for real-time public transport information acquisition and arrival time prediction based on GPS data.....	380
41.3 PT monitoring, analysis, and management.....	388
41.4 Work related analysis	395

42. IOT AND COOPERATIVE HUMAN-MACHINE INTERFACES FOR TRANSPORT SAFETY	402
42.1 Introduction into cooperative HMI.....	404
42.2 IoT based infrastructure for cooperative human-machine systems	412
42.3 Development and modelling of IoT based cooperative HMI systems	417
42.4 Work related analysis	429
43. INTERNET OF DRONE BASED SYSTEMS	436
43.1 Introduction into Drone Fleets.....	439
43.2 Internet of Drones.....	444
43.3 Case studies	456
43.4 Security, safety and reliability of Internet of Drone based systems	463
43.5 Work related analysis	477
PART XII. IOT FOR HEALTHCARE SYSTEMS	484
44. INFRASTRUCTURE OF THE IOT FOR HEALTHCARE SYSTEMS	484
44.1. Standards requirements to IoT for healthcare systems	486
44.2 Techniques of IoT for healthcare systems realization	489
44.3 Developing and modelling infrastructure of the IoT for healthcare systems	495
44.4 Work related analysis	504
45. SECURITY AND PRIVACY IN IOT FOR HEALTHCARE SYSTEMS	509
45.1. Standards and requirements to security and privacy of healthcare IoT systems.....	511
45.2 Techniques and tools of healthcare IoT security and privacy assessment	515

44.3 Markov’s chains and queue theory analysis of healthcare IoT security and availability.....	522
45.4 Work related analysis	529
46 WEARABLE AND EMBEDDED IOT BASED SOLUTIONS FOR BIOMEDICAL APPLICATIONS.....	535
46.1 Biomedical sensors and data acquisition techniques	537
46.2 Biomedical signal processing models for real time health data analytics.....	543
46.3 Developing and testing smart wearable devices.....	547
46.4 Work related analysis	570
47. IOT BASED SYSTEMS FOR REMOTE HEALTH MONITORING.....	576
47.1 A personal mobile sensing system for motor symptoms assessment of Parkinson's disease	578
47.2 Medical aspect.....	578
47.3 Sensors and devices for Parkinson's disease assessment.....	579
47.4 System architecture.....	582
47.5 Basic system components utilized and launched on the smartphone	583
47.6 A mobile application of the personal health monitoring system.....	585
47.7 Cloud infrastructure.....	585
47.8 Implementation and results.....	587
47.9 Work related analysis	592
PART XIII. IOT FOR ECOLOGY, SAFETY AND SECURITY MONITORING SYSTEMS.....	597
48. IOT SYSTEMS FOR CONTROLLING SMALL ARTIFICIAL ECOLOGICAL SYSTEMS.....	597
48.1 Sensors for monitoring artificial ecosystems, the basics of work and physical principles	599

48.2 Features of the collection and analysis of information about the state of ecosystems by using IoT devices.....	608
48.3 Examples of control systems for small artificial ecosystems	615
48.4 Work related analysis	624
49. IOT BASED WATER QUALITY MONITORING SYSTEM	629
49.1 IoT based Water Quality Monitoring System: Basic framework	632
49.2 Parameters and data management in IoT WQMS	639
49.3. IoT WQMS evolution: from collecting data and data visualization to real-time predictive analytics	647
49.4 Case study.....	649
49.5 Work related analysis	665
50. IOT BASED SYSTEMS FOR MONITORING OF SEVERE ACCIDENTS	672
50.1 General Information on systems for monitoring of critical industry objects/NPP accidents.....	675
50.2 Multi-version drone based Systems for monitoring of NPP severe accidents	690
50.3 Reliability of IoD based systems for monitoring of NPP severe accidents	696
50.4 Work related analysis	706
51. IOT BASED PHYSICAL SECURITY SYSTEMS OF BUILDINGS AND CAMPUSES	713
51.1 Physical security systems assessment and development tasks ..	715
51.2 IoT based physical security systems development	718
51.3 Models of physical security systems risk analysis	723
51.4 PSMECA based assessment of physical security systems.....	730
51.5 Work related analysis	733
PART XIV. IOT FOR INDUSTRIAL SYSTEMS	738

52. STRUCTURES, MODELS AND TECHNOLOGIES FOR DEVELOPMENT OF INDUSTRIAL IOT BASED SYSTEMS..	738
Abbreviations	739
52.1 General approach to structures and models building of IoT-based industrial systems	740
52.2 IoT technologies for monitoring and control tasks implementation in industry	747
52.3 Security problems in industrial IoT-based systems	756
52.4 Work related analysis	763
53. ADVANCED TECHNIQUES AND MEANS FOR DESIGN, MODERNIZATION AND IMPLEMENTATION OF INDUSTRIAL IOT BASED SYSTEMS.....	772
53.1 Design and implementation of IoT based control and monitoring systems for floating docks	774
53.2 Design and implementation of IoT based control and monitoring systems in robotics	781
53.3 Approaches to modernization of complex objects in different industrial systems based on IoT.....	789
53.4 Work related analysis	798
54. APPLICATION OF IOT TECHNOLOGIES IN ENTERPRISE MANAGEMENT AND ENGINEERING.....	806
54.1 Application of IoT technologies in the processes of high-tech enterprise management. Smart logistics, material resource and service maintenance management.....	808
54.2 Intelligent information technologies and mathematical support of IoT in mechanical engineering	811
54.3 Application of IoT technologies for diagnostics, monitoring and prediction of complex technical system state	818
54.4 Work related analysis	829

55. DEVELOPMENT AND HARDWARE OPTIMIZATION OF CONTROL UNITS FOR IOT DEVICES IN INDUSTRY SYSTEMS	834
55.1 The problem of hardware expenses optimization in IoT devices	836
55.2 The IoT device control unit in the form of finite state machine with canonical structure.....	837
55.3 The IoT device control unit in the form of finite state machine with counter	839
55.4 Generalizations for an FSM with counter.....	840
55.5 Datapath of transitions.....	850
55.6 Synthesis of IoT device control unit in the form of finite state machine with datapath of transitions	853
55.7 Evaluation of the effectiveness of FSM with DT as IoT device control unit.....	858
55.8 Integration of FSM with DT into IoT device.....	859
55.9 Work related analysis	861
56. INDUSTRY 4.0/5.0 AND INDUSTRIAL INTERNET OF THINGS	866
56.1. Association of Industrial Automation of Ukraine as a driver of Industry 4.0.....	868
56.2. The possibilities of Ukraine in context of Industry 4.0	869
56.3. Strategy and directions of Industry 4.0.....	872
56.4 Trends in Industry 4.0 and Industrial Internet of Things	883
56.5 Industry 5.0 and Internet of Things	893
56.6 Work related analysis	896
Анотація	902
Аннотация	910

PREFACE

ALIOT ERASMUS+ project. Three-volume book contains material for lectures and training modules developed during carrying out of project “**Internet of Things: Emerging Curriculum for Industry and Human Applications /ALIOT**”¹ (Project Number: 573818-EPP-1-2016-1-UK-EPPKA2-CBHE-JP, 2016-2019) funded by EU Program ERASMUS+. Main ALIOT project objectives are development and transfer of innovative Internet of Things (IoT) and Internet of Everything (IoE) related research ideas and practices between the academic and industrial sectors and for society as whole.

The tasks of the ALIOT project are the following:

1) to introduce a Multi-domain and Integrated Internet of Things (IoT) programme and develop 4 courses for MSc students:

- MC1 Fundamentals of IoT and IoE,
- MC2 Data science for IoT and IoE,
- MC3 Mobile and hybrid IoT-based computing,
- MC4 IoT technologies for cyber physical systems;

2) to introduce a Multi-Domain and Integrated IoT programme and develop 4 courses for doctoral students:

- PC1 Simulation of IoT and IoE-based systems,
- PC2 Software defined networks and IoT,
- PC3 Dependability and security of IoT,
- PC4 Development and implementation of IoT-based systems;

3) to establish multi-domain IoT cluster network and develop 6 training courses for human and industry applications:

- ITM1 IoT for smart energy grid,
- ITM 2 IoT for smart building and city,
- ITM 3 IoT for intelligent transport systems,
- ITM 4 IoT for health systems,
- ITM 5 IoT for ecology monitoring systems,
- ITM 6 IoT for industrial systems.

¹ *The European Commission's support for the production of this publication does not constitute an endorsement of the contents, which reflect the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein.*

The tasks of the project have been solved by ALIOT consortium of Ukraine and EU countries universities and organizations:

- Newcastle University (NU), United Kingdom (grant holder and EU coordinator);

- National Aerospace University "Kharkiv Aviation Institute" (KhAI), Ukraine (national coordinator);

- Leeds Beckett University (LBU), United Kingdom;

- Coimbra University (CU), Portugal;

- University KTH, Stockholm, Sweden;

- Institute of Information Science and Technologies ISTI-CNR, Pisa,

Italy;

- Chernivtsi National University (ChNU), Ukraine;

- East Ukraine National University (EANU), Ukraine;

- Odesa National Polytechnic University (ONPU), Ukraine;

- Ternopil National Economic University (TNEU), Ukraine;

- Petro Mohyla Black Sea National University (PMBSNU),

Mykolaiv, Ukraine;

- Zaporizhzhya National Technical University (ZNTU), Ukraine;

- Pukhov Institute for Modelling in Energy Engineering (IPME), National Academy of Science of Ukraine, Kyiv, Ukraine;

- IT-Alliance (ITA), Ukraine;

- Smart.ME company (SM), Ukraine.

ALIOT books. To assure the ALIOT courses the following books are edited:

- Three volume multi-book "Internet of Things for Industry and Human Applications" for theoretical/lecture part of courses:

- Volume 1. Fundamentals and Technologies (MSc study),

- Volume 2. Modelling and Development (PhD study),

- Volume 3. Assessment and Implementation (training modules);

- 4 practicum books for MSc courses;

- 4 practicum books for PhD courses;

- 6 books for domain oriented training modules.

The volumes consists of 14 parts according with list of MSc (Parts I-IV), PhD (Parts V-VIII) and training (Parts IX-XIV) courses. Parts are called according with corresponding courses (Parts I-IV as MC1-MC4, Part V-VIII as PC1-PC14, Parts IX-XIV as ITM1-ITM6).

Parts consist of the sections 1-56 (4 sections for courses MC1-MC2, MC4, PC1-PC4, ITM1-ITM5; 3 sections MC3, 5 sections for ITM6). Section 0 introduces into the multi-book.

Contents and authors of the Volume 3. Volume 3 consists of parts IX-XIV, sections 32-55.

PART IX. IOT FOR SMART ENERGY GRID.

Section 32 presents a comprehensive knowledge on SG components with information technologies in the context of IoT. In addition, this study gives an overview of different SG communication applications and technologies, their benefits, characteristics, and requirements. Finally, this Section discusses problems with the use of new directions such as cloud computing and big data for SGs.

Authors of the section 32 are Assoc. Prof., Dr. G. M. Hladiy, Dr. Z. I. Dombrowskyi, Prof., DrS A. O. Sachenko (TNEU).

Embedded systems devices and their role in organization of local SEG as part of IoT infrastructure have been considered in the section 33. This chapter provides overview of the approaches to local SEG organization and outlines main technologies and hardware device as fundamental part of local SEG part. Alongside with hardware components, software parts are also taken into discussion to describe full image of technologies connections in the investigated field. It has been emphasized that despite being lower level of global grid, local SEG is a complex solution that integrates multiple software and hardware components that tightly cooperate with each other as well as with higher levels of the systems.

Authors of the section 33 are Prof., DrS M. P. Musiyenko, Assoc. Prof., Dr. I. M. Zhuravska, Dr. Y. M. Krainyk (PMBSNU).

Section describes smart grid systems and application of IoT. It presents a comprehensive information in regards to reliability assessment of IoT based IT infrastructure, I&C failures classification, highlights on models of reliability and techniques of its assessment and assurance. Method of safety assessment taking into account the reliability of systems (subsystems) is considered in this section. The features of the implementation of machine and deep learning of neural networks, predictive analytics for the Internet of things systems are considered. Markov models of functioning of the Internet of Things systems are proposed and investigated.

Authors of the section 34 are Prof., DrS Brezhniev E.V., Assoc. Prof., Dr. Kolisnyk M.O. (KhAI).

Section 35 presents a comprehensive description of IoT - based SG safety and security modeling. In addition, this study gives an overview of challenges in smart grid safety and security in context IoT which are existing due to influences between SG systems. This study also gives the short overview of safety and security assessment and assurance's approaches, presents SG safety strategies. The role of IoT devices (such as sensors) in implementation of safety/security management is described. This Section presents a comprehensive demonstration of smart grid safety/security management. The highlights for Resilience-oriented measurement of quality of IoT based SG services and SDOE-based development of resilient digital substation is given.

Author of the section 35 is Prof., DrS. Brezhniev E.V. (KhAI).

PART X. IOT FOR SMART BUILDINGS AND CITY.

The section 36 presents methods for assessing risks in the Internet of things system. To perform the assessment, a hierarchical division of the Internet of things into subsystems is proposed in accordance with the functional purpose of the subsystems. For this purpose, elements of the general theory of systems were used. A risk scale has been developed and an assessment method has been described using expert assessments. Studies have shown that the greatest risks for subsystems arise from the failure of adjacent subsystems.

Authors of the section 36 are Prof., DrS D. A. Maevsky, Assoc. Prof., Dr. O. Yu. Maevskaya (ONPU).

The section 37 is devoted to the analysis and principles of operation of smart home systems. The industrial sensors for monitoring the external environment and their interaction with microprocessor devices are considered. Considered in detail the construction and operation of all systems of the smart home - lighting, climate control, security system. The interaction of smart home devices using technologies of the Internet of Things is considered.

Authors of the section 37 are Prof., DrS V. V. Bousher, Prof., DrS A.O. Bojko (ONPU).

Modern technologies and tools for Smart Building system software/hardware platform development are presented in the Section 38. The features of embedded systems design as the basis of Internet of Things infrastructure are shown. The issues of Smart Building system architecture development are discussed, as well as the features of Raspberry Pi and

OpenHAB platforms usage for system control. The possibilities of remote laboratory Smart House&IoT application for Smart Building system prototyping are described in details.

Author of the section 38 is Assoc. Prof., Dr. A. V. Parkhomenko (ZNTU).

The technology of interaction of smart home systems and the city in their architecture, behavior and synchronization is considered in Section 39. The formal specifications of entities, their relationship, data, conditions, events, actions and functions of the architecture are defined. The modeling of interactions in the processes of the smart home and city systems is presented. The specifications and modeling of interactions at the functional level for smart home systems, at the synchronization level for smart city systems are considered.

Authors of the section 39 are Assoc. Prof., Dr. O. M. Martynyuk, Prof., DrS O. V. Drozd.

PART XI. IOT FOR INTELLIGENT TRANSPORTATION SYSTEMS.

Section 40 presents the intelligent system for monitoring the transport flows that gets information from video cameras, handles its further processing, transmitting and decision making using IoT technology. To implement such intelligent system the both hardware and software are considered. Methods of recognition and classification of transport objects in video stream are analyzed. Intelligent system for controlling the transport flows intensity has developed.

Authors of the section 40 are Prof., Dr. V. V. Kochan, Dr. O. R. Osolinskyi, Dr. D. I. Zahorodnia, Assoc. Prof., Dr. P. Y. Bykovyy, Prof., DrS A. O. Sachenko (TNEU).

The main contribution of the section 41 is an integrated, formal and automated methodology for public transport information services. Section 41 reflects the results of the development and implementation of the architecture for the deployment of an information services infrastructure for public passenger transport. The concept of real-time data collection and the selection of an efficient model for predicting the vehicle arrival time were developed. As a result, public transport services are improved using GPS data and data provided by IoT applications.

Authors of the section 41 are Prof., DrS I. S. Skarga-Bandurova, PhD Student M. V. Derkach (EUNU).

In section 42, the principles and requirements to designing cooperative human-machine interfaces for the intelligent transport systems are studied. The architecture of the system based on the Internet of Things and the communication protocol are suggested. The efficiency and functional safety assessment of human-machine interfaces are studied. The prototype of the transport system cooperative interface is provided.

Authors of the section 42 are Prof., Dr. O. O. Orekhov, Prof., DrS. V. S. Kharchenko, Dr. A. O. Stadnik A. (KhAI).

A conceptual architecture for a drone fleet is discussed in Section 43. Communication technologies used for unmanned aerial vehicles are considered. The main features for Internet of Drones technology are displayed. The main security issues related to Internet of Drone-based applications are highlighted. Phases for the aircraft system safety risk assessment are discussed. A concept of Internet of Drone-based post-emergency monitoring system is presented, and the reliability models for various variants of the system are developed.

Author of the section 43 is Assoc. Prof., Dr. H. V. Fesenko (KhAI).

PART XII. IOT FOR HEALTHCARE SYSTEMS.

The infrastructure of the IoT for healthcare systems is considered in the section 44. The standards requirements analysis to IoT for healthcare systems is presented. Existed and prospective techniques of IoT for healthcare systems realization are described in this chapter. The process of infrastructure development and modeling of the IoT for healthcare systems is shown.

The security and privacy issues of the IoT for healthcare systems is described in the section 45. The standards requirements to IoT for healthcare systems security and privacy are presented. The hierarchical cybersecurity model for healthcare IoT system is developed. It shows how to protect information, devices and humans' life by securing each layer of IoT system. The overview of the healthcare IoT system failures and attacks is presented. IoT infrastructure, a method for analyzing fault/attack trees was examined, which makes it possible to estimate the probability of failure/attack on the healthcare IoT system. A Markov models set for the healthcare IoT infrastructure that allows taking into account the specificity of end user devices, communication channels, technologies of data flows and safety and security issues of these components has been developed.

Authors of the sections 44 and 45 are Prof. V. S. Kharchenko, Dr. D.D. Uzun, PhD student A. A. Strielkina, Dr. O. O. Illiashenko (KhAI).

In section 46, the materials for module of training course “Wearable IoT-based systems for biomedical applications” are presented. They can be used for preparation to lectures and self-learning. The aim of the module is to give PhD students a deep knowledge of principles and aspects of the IoT-based technologies in health and biomedical systems: teach to developing and testing smart biomedical devices, perform real-time data analyzing.

Section 47 is provide a summary of Parkinson’s disease attributed to the selection of certain physiological indicators. The overview of systems for monitoring the motor symptoms of Parkinson's disease, sensors, devices, hardware, detection parameters and methods for data analysis are discussed. System architecture, functionality, main characteristics, as well as data processing technique are presented. The implementation of the developed system is presented: a mobile application, tests, techniques for data acquisition, transferring and processing.

Authors of the sections 46 and 47 are Prof., DrS I. S. Skarga-Bandurova, Assoc. Prof., Dr. T. O. Biloborodova (EUNU).

PART XIII. IOT FOR ECOLOGY, SAFETY AND SECURITY MONITORING SYSTEMS.

Section 48 considers the basic principles of using the Internet of Things in various agricultural technologies, as managing the state of artificial ecological systems, such as greenhouses or irrigation systems, monitoring the state of weather conditions or the state of open field crops. Features of the sensors used and the physical parameters that they measure were preliminarily discussed as well as features of the basic methods of processing data from the sensors.

Authors of the section 48 are Assoc. Prof., Dr. S. V. Morshchavka (ZNTU).

In the section 49, the study will expand the current research on IoT sensors for environmental monitoring and analytical methods for different IoT based systems for water monitoring applications. It addresses perspectives and challenges during developing IoT-based system for water quality monitoring and discusses the following: parameters measured for all types of water objects; data collection tools and coexistence possibilities of various IoT systems involved in the control of water objects; development of proprietary IoT-system: device, hardware and software tools, a

dashboard for on-line monitoring water objects; IoT water resource management: water quality real-time data acquisition, aggregation, and analysis; application of data management systems for analysis of large datasets.

Authors of the section 49 are Prof., DrS I. S. Skarga-Bandurova, PhD student Y. O. Kritska (EUNU).

Classification of radiation monitoring systems is given and structures of the systems are analyzed in Section 50. A general structure and underlying principles for creating an Internet-of-Drone-based multi-version post-severe nuclear power plant accident monitoring system are described. Reliability block diagrams for the system and its subsystems are built. On the basis of reliability block diagrams, reliability models of the system and their subsystems are developed.

Authors of the section 50 are Assoc. Prof., Dr. H. V. Fesenko, Prof., DrS V. S. Kharchenko (KhAI).

Section 51 presents the theoretical and practical development and assessment aspects of the physical security systems (PSS) of buildings and campuses based on the Internet of Things. The need to implement physical security systems is explained, structures and approaches to the development and implementation of IoT based PSSs are given. The technique PSMECA of PSS assessment failures criticality is described.

Authors of the section 51 are Assoc. Prof., Dr. D. D. Uzun, PhD student Al-Khafaji Ahmed Waleed, Prof., DrS V. S. Kharchenko, Dr. O. O. Illiashenko, PhD student O.O. Solovyov (KhAI).

PART XIV. IOT FOR INDUSTRIAL SYSTEMS.

Structures, models and technologies for development of industrial IoT-based systems are considered in the section 52. Main trends and peculiarities in industrial IoT-based systems are selected from big variety of IoT applications. Besides, software components and protocols of wired and wireless technologies for IoT networks building are considered. Also, security problems in industrial IoT-based systems are analysed: main types of attacks, data encryption standards and security policy of industrial systems based on IoT.

Advanced techniques and means for design, modernization and implementation of industrial IoT-based systems are considered in the section 53. There is description of IoT-based control and monitoring systems for floating docks as well as design and implementation of

corresponding IoT-based systems. Hardware and software means for implementation of mentioned above IoT-based control and monitoring systems is presented in details. Also, approaches to modernization of complex objects in different industrial systems based on IoT are considered for specialized pyrolysis complex and industrial robot's adaptive gripper.

Authors of the sections 52 and 53 are Prof., DrS. Yu. P. Kondratenko, Assoc. Prof., Dr. O. V. Kozlov, O. V. Korobko, PhD Student O. S. Gerasin, PhD Student A. M. Topalov (PMBSNU).

Section 54 is devoted to the introduction and using of IoT technologies in aviation, in particular, diagnostics of the state of aircraft engines and aircraft. Considering the large amount of data characterizing the technical condition of the aviation system, the technology of cloud storing and transmission of the data is used. On its basis, the strategy of using neural networks for data analysis, decision making and remote management of the object of diagnosis is implemented. Using the apparatus of neural networks helps to determine the technical condition with high accuracy and, on the basis of the data obtained, to make a prediction of subsequent changes. The introduction of a bundle of IoT technologies and neural network allows to significantly reduce the cost of testing and subsequent support of equipment. IoT technologies also allow for real-time diagnostics, which often helps prevent serious breakdowns and save human lives.

Authors of the section 54 are Dr. A.O. Oliinyk, Prof., DrS S. O. Subbotin, Dr. D.V. Pavlenko, PhD student S.D. Leoshchenko (ZNTU).

Section 55 considers hardware optimization in the logical circuit of the IoT device control units, implemented in the form of a finite state machine. The principle of operational transformation of state codes is described in detail, in accordance with which the transition function of the finite state machine is implemented by the datapath. The structural organization, synthesis and determination of the effectiveness of a finite state machine with datapath of transitions are considered.

Author of the section 55 is Assoc. Prof., Dr. R. M. Babakov (Vasyl' Stus Donetsk National University, Vinnytsia).

Section 56 describes goals, strategy and landscapes of movement Industry 4.0 in Ukraine. Activities of Association of Industrial Automation of Ukraine (APPAU) are considered. Challenges for implementation of IIoT are discussed. Gartner's Top Trends of technologies are analysed in

point of intelligence, autonomy and mesh. Integrated safety&security management system for manufactures Industry 4.0 is described. Future of Industry 5.0 is considered.

Authors of the section 55 are O. V. Yurchak (APPAU), Prof., DrS V. S. Kharchenko (KhAI), Dr O. O. Illiashenko (KhAI), Assoc. Prof., Dr M. O. Kolisnyk (KhAI), Prof., DrS S. I. Dotsenko (USURT).

Volumes 1-3 edited by Prof., DrS. V. S. Kharchenko (KhAI). Camera-ready versions of Volumes 1-3 were prepared by Dr. O. O. Illiashenko (KhAI).

Acknowledgements. The editor and authors would like to express their appreciation and gratitude to all colleagues from partner universities and organizations for discussion, advises and support.

We thank colleagues who develop the project ERASMUS+ ALIOT “Internet of Things: Emerging Curriculum for Industry and Human Applications” <http://aliot.eu.org/> and participate in discussions of topics related to IoT during a few meetings and schools in Sweden (Stockholm, December 2016), Ukraine (February 2017, 2018, Chernivtsi; May 2017, Mykolaiv; May 2018, Kyiv; February 2019, Ternopil; May 2019, Zaporizhzhya), Portugal (Coimbra, October 2017), United Kingdom (Newcastle-Leeds, July 2018).

We thank participants of International Workshops on Cyber Physical Systems and Internet of Things Dependability (WS CyberIoT-DESSERT) at the conferences IDAACS (September 2017, Bucharest, Romania), DESSERT (May 2018, Kyiv, Ukraine) and monthly Seminar on Critical Computer Technologies and Systems (CriCTechS, KhAI, 2017-2019) at the Department of Computer Systems, Networks and Cybersecurity for discussion of preliminary project results in point of view research, development and education issues.

We would like to thank reviewers of the multi-book:

- Dr. Mario Fusani (ISTI-CNR, Pisa, Italy);
- Dr. Olga Kordas (KTH University, Stockholm, Sweden)
- Senior Project Manager Viktor Kordas (KTH University, Stockholm, Sweden)

for very helpful advises and valuable recommendations.

IX. IOT FOR SMART ENERGY GRID

32. INTEGRATION OF IOT AND SMART GRID COMPONENTS

Assoc. Prof., Dr. G. M. Hladiy, Dr. Z. I. Dombrowskyi,
Prof., DrS A. O. Sachenko (TNEU)

Contents

32 Integration of IoT and smart grid components	1
32.1. Structure of the integrated IoT and smart grid system	3
32.1.1. Selecting the architectural model of smart grid system	3
32.1.2. Key components of smart grid	10
32.2 Communication protocols and interfaces of IoT smart grids	12
32.2.1 Cyber-physical issues of protocols and interface of smart grids	12
32.2.2 IoT smart grid communication protocols	15
32.2.3 Smart meters communications networks	20
32.3 Cloud computing and Big Data as a part of IoT smart grid	23
32.3.1 Big Data in smart grid systems	23
32.3.2 Cloud computing as operation platform for smart grids	25
32.4 Work related analysis	27
Conclusions and questions	28
References	29

Abbreviations

BAN – Building Area Network

CEN – European Committee for Standardization

CENELEC – Comité Européen de Normalisation Électrotechnique
(European Committee for Electrotechnical Standardization)

CIS – Customer Information System

CPS – Cyber-Physical Systems

DER – Distributed Energy Resources

DMS – Distribution Management System

ETSI – European Telecommunications Standards Institute

FAN – Field Area Network

GIS – Geographic Information System

GPS – Global Positioning System

HAN – Home Area Network

IAN – Industrial Area Network

IAP – Interoperability Architectural Perspective

ITU-T – International Telecommunication Union, telecommunication
standardization sector

M2M – Machine-to-Machine

NAN – Neighborhood Area Networks

NIST – National Institute of Standards and Technology

OMS – Outage Management System

RFID – Radio Frequency Identification

SCADA – Supervisory Control and Data Acquisition System

SG – Smart Grid

SGAM – Smart Grid Architecture Model

SGIRM – Smart Grid Interoperability Reference Model

WAN – Wide Area Network

WSN – Wireless Sensor Networks

32.1. Structure of the integrated IoT and smart grid system

32.1.1. *Selecting the architectural model of smart grid system*

The concept of Smart Grid (SG) is quite comprehensive, but there is no unique definition. The IEEE P2030 Project [1] has some conceptual ideas and formulations. One of them defines a SG as follows:

“A **smart grid** is the integration of power, communications, and information technologies for an improved electric power infrastructure serving loads while providing for an ongoing evolution of end-use applications”.

The SG is an electricity network that uses digital and other advanced technologies to monitor and manage the transport of electricity from all generation sources to meet the varying electricity demands of end-users. SGs co-ordinate the needs and capabilities of all generators, grid operators, end-users and electricity market stakeholders to operate all parts of the system as efficiently as possible, minimizing costs and environmental impacts while maximizing system reliability, resilience and stability [2].

The SG is a complex system of systems, serving the diverse needs of many stakeholders. It must support: devices and systems developed independently by many different solution providers; many different utilities; millions of industrial, business, and residential customers; different regulatory environments.

To analyze this system of systems, its architecture must be defined. Many international organizations, such as NIST (National Institute of Standards and Technology), ITU-T (International Telecommunication Union) and IEEE, propose their own models. These models are conceptual and represent only guidance for understanding the overall operation of the system, as well as a basis for discussing the characteristics, usage, behavior, interfaces, requirements and standards of the SG. Therefore, these models are just a tool for describing the SG architecture.

The development of the energy infrastructure based on the modern SG is a rather complicated engineering task. In order to achieve this goal, it is necessary to formulate properly the problem at different

levels of abstraction based on the top-down approach. The SG is comprised of many networks (domains) that have to be interconnected to provide end-to-end services. The challenge is to design network architectures that can meet the interoperability requirements for inter-domain and intra-domain communications.

Fig. 32.1 illustrates the IEEE P2030 conceptual representation of the SG architecture from three different perspectives such as power systems, communications, and information technology platforms.

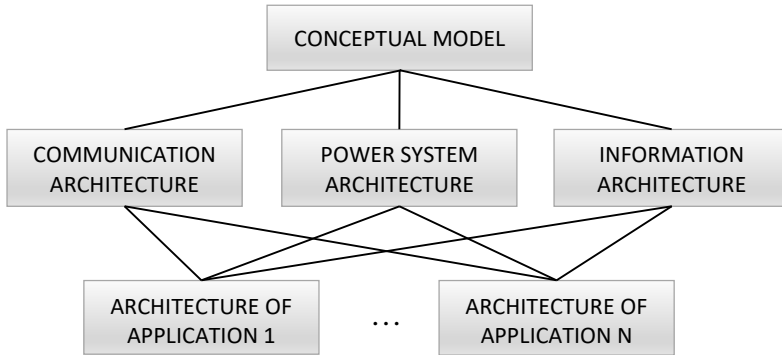


Fig. 32.1 – The hierarchical approach to SG architecture development

At the upper level, the conceptual model is determined. We discuss here some of the famous models.

The NIST conceptual model describes the overall composition of electric grid systems and applications. It is meant to provide a high-level view of the system that can be understood by many stakeholders [3].

This conceptual domain model supports planning, requirements development, documentation, and organization of the diverse, expanding collection of interconnected networks and equipment that will compose the SG. For this purpose, NIST has adopted the approach of dividing the SG into seven domains (Fig. 32.2).

Each domain – and its sub-domains – encompass SG conceptual roles and services. They include types of services, interactions, and stakeholders that make decisions and exchange information necessary for performing identified goals, such as: customer management,

distributed generation aggregation, and outage management. Services are performed by one or more roles within a domain.

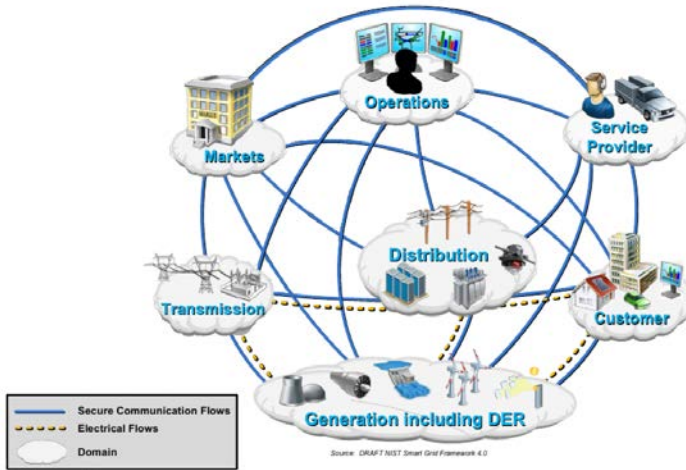


Fig. 32.2 – The NIST conceptual model of SG

The conceptual model consists of several domains, each of which contains many applications and roles that are connected by associations, through interfaces. Associations are logical connections between roles that establish bilateral relationships. In Fig. 32.2, the electrical associations between domains are shown as dashed lines, and the communications associations – as solid lines. Interfaces represent the point of access between domains. Each of these interfaces may be bidirectional. Communications interfaces represent logical connections in the SG information network interconnecting various domains.

Recently the NIST decomposed the conceptual domain model into layers of increasing technical focus to understand how various SG requirements are satisfied within each interaction of architecture. These levels are: 1) conceptual; 2) logical; 3) physical; 4) implementation.

Fig. 32.3 [4] is a conceptual diagram for logical model SG information network, showing the interconnections of networks between various domains.

For the implementation of the conceptual model, developers need a reference architecture, formed from the conceptual model by identifying functional blocks and interfaces.

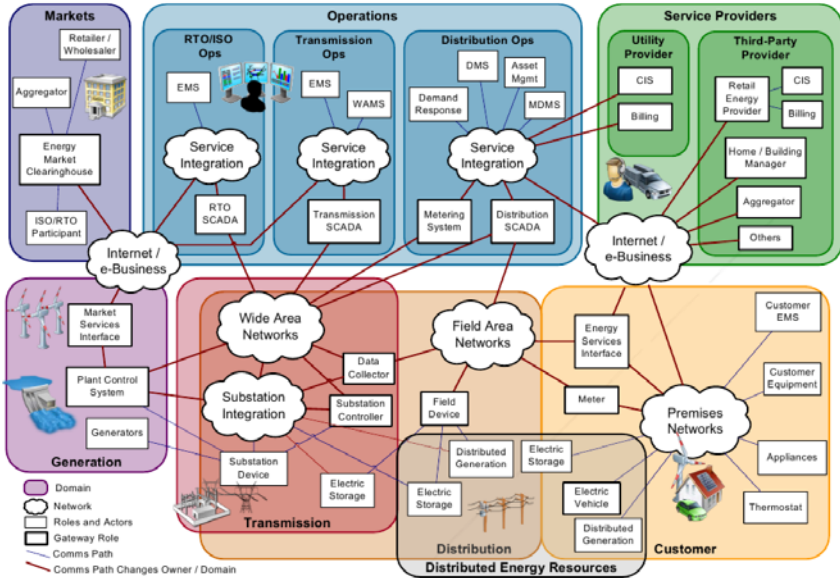


Fig. 32.3 – Logical model with conceptual domains for SG information networks

The IEEE P2030 SGIRM (Smart Grid Interoperability Reference Model) [1] extends the NIST conceptual model, considering three interoperability architectural perspectives (IAPs) which represent the main areas involved in the SG: power systems (PS-IAP), communications technologies (CT-IAP) and information technology (IT-IAP). Each IAP defines the main functional blocks for each domain of the conceptual model, as well as the interfaces between functional blocks, and the interfaces between domains. The defined IAPs are further particularized for the most important applications in the SG area (Fig. 32.1)

The NIST conceptual model was a first model, but it required an adaptation to the European context. The CEN/CENELEC/ETSI strategic partnership has further developed the NIST conceptual model

and has adapted it to the specific requirements of the European electricity grid. As a result, a three-dimensional Smart Grid Architecture Model (SGAM) (Fig. 32.4) has created [5].

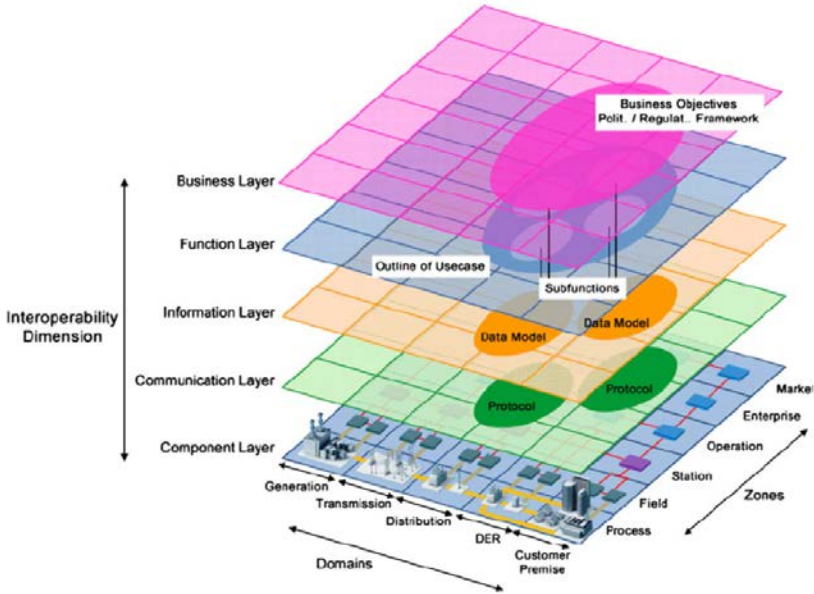


Fig. 32.4 – CEN/CENELEC/ETSI 3D architectural model

The advantage of this model is that it can be used in a technology-neutral manner. In addition, it supports comparison of different approaches to SG solutions so that differences and commonalities between various paradigms, roadmaps, and viewpoints can be identified. By supporting the principles of universality, localization, consistency, flexibility and interoperability, it also provides a systematic approach to addressing the complexity of SGs, which allows presenting the current state of implementations in the power grid as well as the evolution to future SG scenarios.

The SGAM is a reference model to analyze and visualize SG use cases in respect to interoperability, domains and zones. The domains regard the energy conversion chain and include: *Generation*, *Transmission*, *Distribution*, *DER* (distributed energy resources) and *Customer Premises*. The hierarchy of power system management is

reflected within the SGAM by the following zones: *Process*, *Field*, *Station*, *Operation*, *Enterprise*, and *Market*.

Finally, as it constitutes major requirements towards distributed systems the SGAM defines Interoperability Layers, which cover entities ranging from business objectives to physical components. The technical views are modeled in SGAM on the four lower layers.

The *Function layer* describes functions and services including their relationships following business needs. Functions are represented independent of their physical implementation (represented by elements in the component layer). The *Information layer* describes the information that is being used and exchanged between functions. It contains information objects and the underlying canonical data models. The *Communication layer* describes mechanisms and protocols for the interoperable exchange of information between functions. The *Component layer* describes all physical elements that realize a function, logical elements thereof, as well as their relations. Physical elements can include power system equipment, protection and tele-control devices, network infrastructure, or any kind of computers. In addition, logical parts, the aforementioned elements, like components or software applications, can be depicted on the component layer.

The SG architecture could also be considered in terms of the use of IoT technologies. Some overview of existing IoT-based architectures is given in [6]. Usually, developed architectures are divided into two groups – home area network (HAN) architecture and multi-layered architecture.

Fig. 32.5 shows an example of four-layer architecture of SG based on the characteristics of information and communication systems.

Today, the SG already widely used information sensing, transmission and processing of information, and now the technology ICT plays an important role in power grid constructing. IoT technology provides a real-time, interactive network connection to users and devices through various communication technologies, to power equipment through various IoT smart devices. Such cooperation is necessary for real-time realization of two-way and high-speed data exchange in various applications, increasing the overall efficiency of SG.

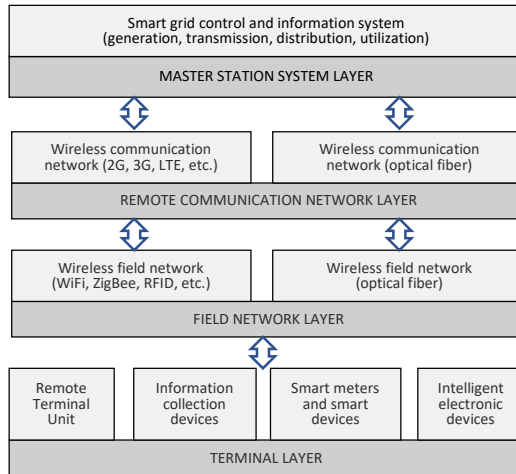


Fig. 32.5 – Four-layered architecture of IoT-based SG

The application of the IoT in SGs can be classified into three types:

- 1) deploying various IoT smart devices for the monitoring of equipment states;
- 2) information collection from equipment with the help of its connected IoT smart devices through various communication technologies;
- 3) controlling the SG through application interfaces.

IoT sensing devices typically consist of RFID, wireless sensors, M2M devices, infrared sensors, laser scanners, cameras, GPS and others various devices. Information sensing in SG can be highly supported and improved with the help of IP technology. The IoT technology also plays an important role in deploying data sensing and transfer infrastructure for SG, contributing to network construction, safety management, operation, maintenance, information gathering, security monitoring, measurement, user interaction, etc. The IoT allows integrating information flow, power flow and flowing distribution in SG.

32.1.2. Key components of smart grid

This subsection discusses the key components of the SG, the main ones of which are detailed in the following chapters. The key components of SG are shown in Fig. 32.6.

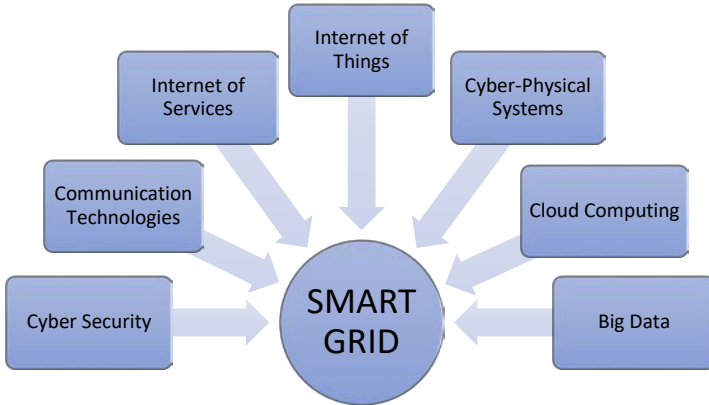


Fig. 32.6 – The key components of SG

Internet of Thing. In SG, the IoT has several potential benefits in various applications, such as smart homes, smart cities, smart security etc. The fundamental principle of IoT is to offer users seamless interoperability, advanced connectivity between machines, humans, services, disparate networks, and in particular control systems for enabling real-time transfers of knowledge among organizations and inside organizations. Thus, the use of IoT in SG allows making intelligent systems, management decision support systems, and predictive diagnostic systems in order to increase the power generation capacity and thus result in significant financial benefits.

Cyber-Physical Systems (CPS). The other key enabler of the SG is CPS, where closely intertwined software and physical objects and allows different components to exchange information by interacting with each other via IoT. In SG, the modern IoT enabled ICTs connects all relevant components to observe real-time information for monitoring, control and maintenance purposes. The embedded systems are one of the key technical methods in CPSs. However, different from

the traditional embedded system, a CPSs-enabled system in SG usually designed with cyber twined and physical input and output services. Thus, CPSs with feedback loop mechanisms monitor and control the physical processes by interacting with the embedded computers and networks.

Big Data. The SG is becoming more complex and more knowledge-intensive with an aggressive push toward the IoT and CPSs technologies in SG. As a result, the data is becoming more and more accessible and ubiquitous in SG. In SG, the data mainly accumulates due to pervasive integration of the various objects, used for various SG applications, such as electricity price data, metering data, energy using data, SGs health data, demand and response, advanced control and monitoring and others. In the coming future, it is expected that the amount of data will continuously grow with the increasing number of CPSs used in in the SG. This huge amount of heterogeneous data stored in the distributed clouds will be available in real time via IoT technology.

Cloud Computing. In SG, a vast volume of analog and digital data is generated by several IoT-enabled CPS sources, which requires a big data storage, cleaning, mining and high-performance computing techniques. In this context, the cloud is an advanced technology to transform resources into services by employing the support of virtualization, cloud computing, IoT and service-oriented technologies. The cloud currently is an important platform that provides a highly stable connection between the network and application layer components for utilizing these resources and services efficiently. The cloud computing technology offers a number of various types of services to users in SG. These computational services and resources can be accessed on-demand, anytime from anywhere on the Internet for all types of SG end users.

Internet of Services (IoS) is a key enabler of IoT and other main components of SG. The idea of IoS is similar to the IoT, however, unlike IoT, the IoS is applied to services rather than physical entities. The IoS infrastructure uses the Internet as a medium to offer and sell services for gaining a competitive advantage over competitors in energy markets. This includes different types of software, hardware, standards, tools and platforms for developing SG applications and delivering

services to customers. The cloud computing technology is the key foundation of the IoS deployment to service energy utilities.

Cyber Security. In SG, various types of seemingly independent systems, including IoT, IoS, CPS, cloud computing, and applications are interconnected with diverse underlying computer technologies, ownership and management yielding high complexity in the SG. The cyber security not only focuses on unintended compromises of valuable information in a case of natural disasters, equipment failures or user errors, but also deliberate attacks from terrorists, disgruntled employees and industrial espionage in SG. The cyber-attacks will not only yield cascade effects on significant losses of the grid technological and financial benefits, but also hurt the energy concerns reputation.

Communication Technologies is the key component that forms the basis for SG. The key aim of the communication technologies is to provide a sophisticated, reliable and fast communication infrastructure that enables the automated exchange of information among the huge amount of distributed CPSs in SG. This real-time exchange of meaningful information will allow energy utility companies to monitor, control and manage grid operations in a more efficient, reliable and flexible manner. The advancements in communication technologies will form the interface between the physical and the virtual worlds for exchanging information in SG.

More details of these components are discussed in the following subchapters.

32.2 Communication protocols and interfaces of IoT smart grids

32.2.1 Cyber-physical issues of protocols and interface of smart grids

An important component of the fourth industrial revolution is the fusion of the physical and the virtual (cyber) world. CPS makes this fusion possible. The term of CPS, coined in 2006 by the U.S. National Science Foundation, describes essentially a broad range of complex, multidisciplinary, physically aware next-generation engineered systems that integrate embedded computing technologies (cyber part) into the physical world. The U.S. vision of CPS is more concentrated on

connection between embedded systems and the physical world, while the European version highlights interaction with the cloud/cyberspace and human factors [7].

CPS are “integrations of computation and physical processes. Embedded computers and networks monitor and control the physical processes, usually with feedback loops where physical processes affect computations and vice versa” [8].

The integration of IoT and IoS in the manufacturing process has initiated the fourth industrial revolution. The IoT allows “ ‘things’ and ‘objects’, such as RFID, sensors, actuators, mobile phones, which, through unique addressing schemas, (...) interact with each other and cooperate with their neighboring ‘smart’ components, to reach common goals” [9]. Based on the definition of CPS given above, ‘things’ and ‘objects’ can be understood as CPS.

Therefore, the IoT can be defined as a network in which CPS cooperate with each other through unique addressing schemas.

Cyber-physical systems are complex systems, which monitor and control the physical environment and support humans during tasks. They are interconnected, heterogeneous systems that combine software and hardware components. CPS make use of latest technology and developers must deal with constant technological change.

In CPSs, the embedded computers and networks serve as headquarters for monitoring and controlling the feedback loops and performance of the physical processes in the SG. Consequently, the CPSs provide highly synchronized information related to the physical shop floor and the virtual computational space, which leads to the new degree of control, efficiency, transparency and surveillance in the SG. The CPSs full potentialities in various SG applications can efficiently manage distributed processes by using data processing and analyzing, controlling the actuators and connecting to digital network services via multi-model human-machine interfaces. Thus, it helps to avoid any problems related to the energy infrastructure if appropriate action is taken instantaneously.

The fundamental architecture of CPS consists of two parallel networks, namely physical network and cyber network to control efficiently the various processes in SG. The amalgamation of both

comprised of the structure of the interconnected components and the reliable communication links among these embedded devices.

CPS depth integrates usually computing power, communication ability, and autonomous control ability and makes this three compatible. It is an interaction of information system and physics system. The essence of CPS is a control network with the function of calculation, communication and control fully based on the perception of environment. Based on the Internet, emphasizing on the environmental awareness, CPS realizes real-time information control and information service, can test or control the physical entity in a safe, reliable, efficient and real-time way. Advanced information technology is the necessary security of SG. Micro-grid is the important component of SG. An overall framework of the Micro-grid CPS is established as shown in Fig. 32.7 [10].

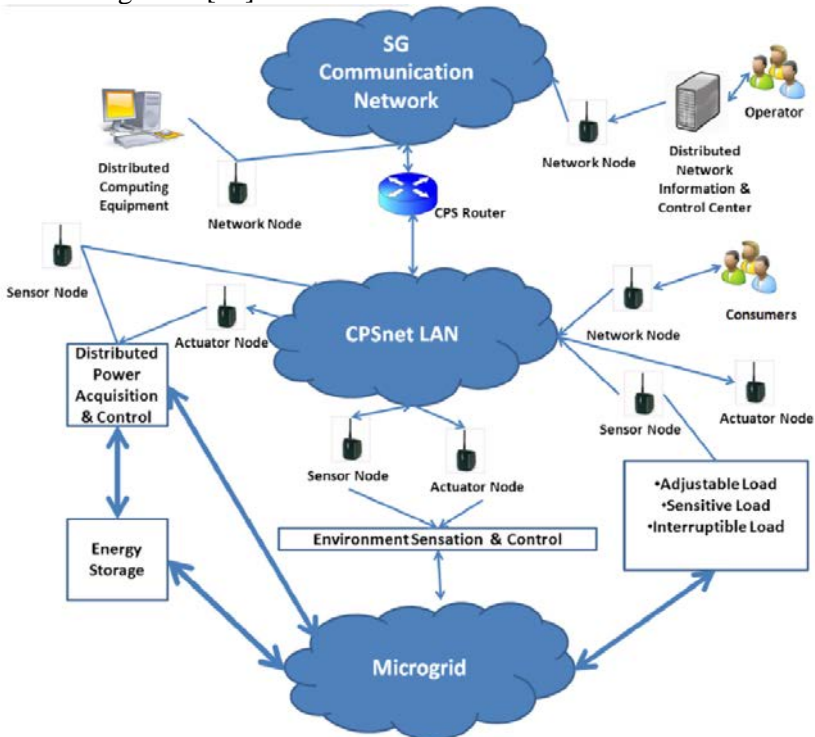


Fig. 32.7 – System architecture of CPS in SG

In Fig. 32.7, the thick arrow lines say power flow, fine arrow lines stand for information. Micro-grid CPS framework including two parts: power network and information network. Physical equipment is mainly power equipment, such as distributed power supply, electronics device, energy storage, load, etc. Information equipment include sensors, distributed computing equipment, server, CPS real-time network, etc., connected by communication network. Through transmission lines, electric power equipment merged, to form a controllable small system, connected into power system, can be in an emergency independent operation by disconnecting static switch.

Micro-grid CPS can be a local area network of future SG, connected great power grid CPS with the CPS router. CPS router should be able to implement easily IP address addressing and the transformation of the heterogeneous data format. Local information and control center is set in the distribution network, can integrate all of the data near the CPS to analysis, and simulate real-time process collection of data, check the legitimacy of user identity, according to local users' demand of the data analysis, request to the actuator control node.

32.2.2 IoT smart grid communication protocols

The SG is an interactive platform consisting different layers (see Fig. 32.4). The communication layer is one of the most critical elements that enables SG applications. The emphasis of the communication layer is to describe protocols and mechanisms for the interoperable exchange of information between components in the context of the underlying use case, function or service and related information objects or data models.

In the SG environment, a communication network can be represented by a hierarchical multi-layer architecture. Classified by data rate and coverage range, this architecture comprises:

- Customer premises area network: Home Area Network (HAN) / Building Area Network (BAN) / Industrial Area Network (IAN);
- Neighborhood Area Networks (NAN)/Field Area Network (FAN);
- Wide Area Network (WAN).

SG users communicate in two-way directions by utilizing several wireless and wired communication protocols such as Zigbee, WiFi, Homeplug, power line carrier, GPRS, WiMax, LET, Lease line, and Fibers [11]. Several software packages were updated and many are being developed to accommodate the new grid operation, maintenance and management such as, distribution management system (DMS), geographic information systems (GIS), outage management systems (OMS), customer information systems (CIS), and supervisory control and data acquisition system (SCADA).

Because of the SG evolution, some recent enabling technologies have emerged to reduce the number of communication protocols and handle big amounts of data. IoT is one the most recent enabler for the SG.

SG communications are based on wireless and wired networks technologies. Regardless of the technology, these networks can be classified based on their functionality within the SG. These classifications are home area network, neighborhood area network, access network, backhaul network, core and external networks. These networks connect many SG objects such as home appliances, smart meters, switches, reclosers, capacitors bank, integrated electronic devices, transformer, relays, actuators, access points, concentrators, routers, computers, printers, scanners, cameras, field testing devices, and other devices. All these appliances and devices are geographically distributed throughout the grid, starting from residential units to substations and up to utility data and command centers.

As it was mentioned above, each device can access and exchange data via different communication protocols.

Fig. 32.8 shows the SG communications protocols layers [11]. The bandwidth and latency requirements for the SG appliances and devices vary from few millisecond to several minutes and from few kbps to few hundreds kbps as shown in Table 32.1 [12].

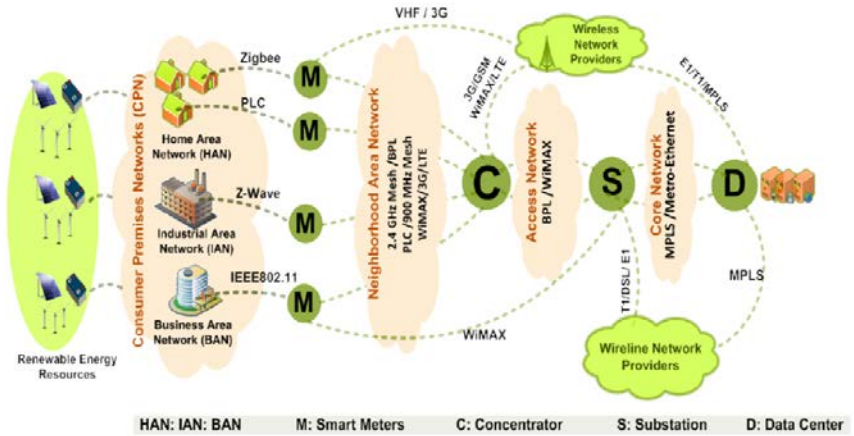


Fig. 32.8 – Smart grid communications protocols

Table 32.1 – Smart grid applications bandwidth and latency requirements

SG Application	Bandwidth	Latency
Substation Automation	9.6-56 kbps	15-200 ms
WASA	600-1500 kbps	15-200 ms
Outage Management	56 kbps	2000 ms
Distribution Automation	9.6-100 kbps	100 ms - 2 sec
Distributed Energy Resources	9.6-56 kbps	100 ms - 2 sec
Smart Meter Reading	10-100 kbps/meter 500 kbps/concentrator	2000 ms
Demand Response	14-100 kbps	500 ms - min
Demand Side Management	14-100 kbps	500 ms - min
Assets Management	56 kbps	2000 ms

As mentioned in the previous sections, smart homes have several appliances and some form of renewable energy resources. These appliances and resources can be considered as IoT technologies. Each can upload and download data and commands from utilities and homeowners. In addition, the grid at large has many devices that can be considered as IoT objects such as reclosers, switches, capacitor banks, transformers, IEDs, smart sensors, and actuators in the substations. In general, smart grids for large cities or countries may have millions of home appliances and thousands of grid devices.

This research proposes that each one of the appliances and devices can have a unique IP address. For example, a dishwasher has a unique IP address a transformer's IP address. This requires the smart grid to have a large number of IP addresses. This is not an issue as the IPV4 is extending from 32-bits to 128-bits address size IP addresses. The IPV4 can address up to 232 devices (4-billionunique addresses). Moreover, IPV6 can address up to 2128 (Trillions of unique addresses) [13].

One outcome of such addressing schema is the 6LowPAN communication protocol.

It embarks on top of IPV6 and is designed to be used over the IEEE 802.15.4 standard [13]. The 6LowPAN frame sized is limited to 127 bytes including a payload of 21 bytes for TCP and 33 bytes for UDP [13]. With some techniques, the payload may increase to 65-75 bytes. This is adequate for the smart grid appliances devices monitoring, and controlling applications. This protocol is the backbone of the IoT communication media.

To model the smart grid within the IoT context, smart home appliances, renewable energy resources, substation devices and workforce tools will be assigned IPV6 address as follows [14]:

1. Smart home appliances.

Recent smart homes are equipped with smart appliances and each appliance is considered as a thing (object).

These things can be an air-conditioner, water-heater, dishwasher, refrigerator, smart energy/gas/water meters, in-home-display, automated lights, solar energy cell, wind mill, electrical rechargeable vehicle, and storage battery [12-13]. In the proposed model, a unique IP address is assigned to each appliance and device. Each appliance or device can be accessed through the internet by authorized personnel

such as a utility's operator or homeowner. The appliance status can be transmitted (uploaded) or control command to be received (downloaded). The exchange data and control commands utilize the payload portion of the 6LoWPAN frame (Fig. 32.9).

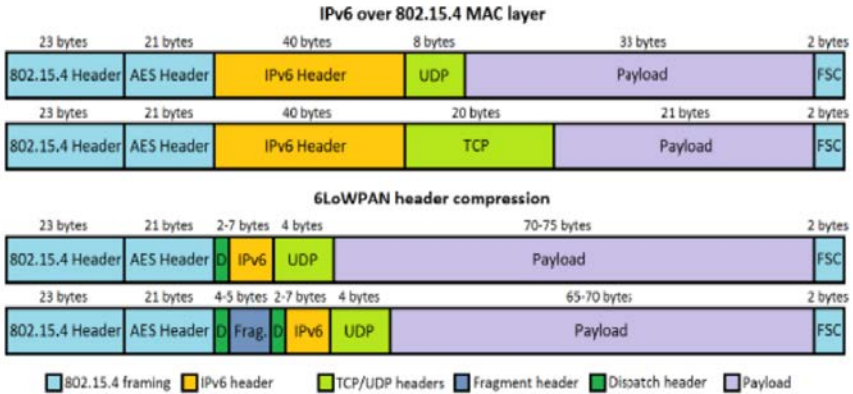


Fig. 32.9 – 6LoWPAN frame structure for smart grid applications

2. Substations devices.

The power substation has many devices (things) such as transformers, breakers, switches, reclosers, meters, relays, IEDs, capacitor banks, voltage regulators, cameras, and several other things. Similarly, to smart homes, each device (thing) in the substation is considered as an object and is assigned a unique IP address. Each object (thing) can transmit its status and receive control commands from the utility authorized operator via the Internet.

The payload is few bytes and can be accommodated using the 6LoWPAN protocol as shown in Fig. 32.10 [14].



Fig. 32.10 – 6LoWPAN frame structure for smart grid applications

3. Distributed renewable energy resources.

The distributed renewable energy resources are one of the major SG enablers that can be installed around the residential neighborhoods, distributed transformers and substations. It supplements power sources that can be installed quickly to be used during the peak hours, as well as on other times of the day when is needed. Each one of these source can supply power to operate, monitor and control. An IP address can be assigned to each appliance and device. The payload size and other related 6LoWPAN frames are shown in Fig. 32.9.

4. Mobile workforce tools and devices.

To operate the grid efficiently, a mobile workforce should be on the move 24 hours a day, 7 days a week to fix issues related to residential power outages, feeders, transformers, meters, power lines, and other related issues. The workforce operators are equipped with rugged laptop, smart meters, mobile phone, and cameras. Each of these devices is assigned an IP address and can be accessed as in the above-mentioned devices and appliances.

5. Utility data and control center infrastructure.

This center has many applications and database services such as DMS, GIS, OMS, CIS, and SCADA. Each service has its own IP address.

6. Echo systems.

The echo systems could be external power server providers, marketing and third parties power providers. Each of which should have point of access through an IP address.

32.2.3 Smart meters communications networks

A smart metering communication system consists of the following components:

- Smart meter which is a two-way communicating device that measures energy consuming at the appliances (electricity, gas, water or heat);

- Home Area Network (HAN) which is an information and communication network formed by appliances and devices within a home to support different distributed applications (e.g. smart metering and energy management in the consumer premises);

- Neighborhood Area Network (NAN) that collects data from multiple HANs and deliver the data to a data concentrator;

- Wide Area Network (WAN) which is the data transport network that carries metering data to central control centers;

- Gateway, which is the device that collects or measures energy usage information from the HAN members (and of the home as a whole) and transmits this data to interested parties.

Table 32.2 indicates the typical communication requirements and the potential technologies that could be employed to realize the different types of network mentioned above.

Fig. 32.11 shows a typical smart metering architecture. At the most basic level, the home will be equipped with a series of smart meters, one each for electricity, gas, water and heat (if applicable). These will be connected to a metering gateway in the home, which may or may not be part of an existing home gateway device. The HAN through which they communicate with the metering gateway may be multi-standard. This is mainly due to differing meter locations and power availability; for example, gas and water meters may have to use only battery power. Multiple HANs are further connected into a NAN via a wireless mesh network.

Table 32.2 – Communication requirements and capabilities of the different types of networks

Type of Network	Range	Data Rate Requirements	Potential Technologies
HAN	Tens of meters	Application dependent but generally low bit rate control information	ZigBee, Wi-Fi, Ethernet, PLC
NAN	Hundreds of meters	Depends on node density in the network (e.g. 2Kbps in the case of 500 meters sending 60 byte metering data every 2 minutes per NAN)	ZigBee, Wi-Fi, PLC, cellular
WAN	Tens of kilometers	High capability device such as a high speed router/switch (a few hundred Mbps to a few Gbps)	Ethernet, microwave, WiMax, 3G/LTE, fibre optic links

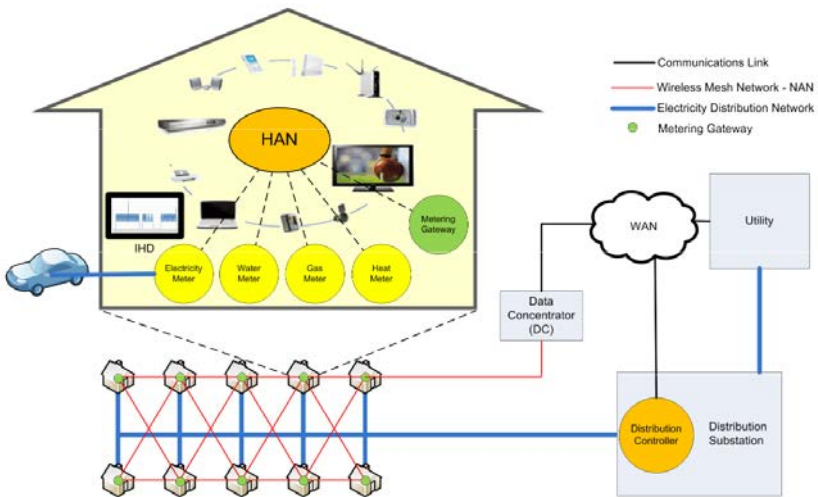


Fig. 32.11 – Typical smart metering architecture

In Fig. 32.11, the smart metering gateway is connected to both the utility (via a WAN) and the distribution control system (DCS) because the utility company may not necessarily own the DCS. The utility is mainly responsible for services like billing, service management and tariffs, and the distribution control system is responsible for demand response, commands to disable certain devices/appliances, renewable energy integration, etc.

A key feature of SG is the interconnection of a potentially large number of disparate energy distribution networks, power generating sources and energy consumers. The components of each of these entities will need a way of communicating that will be independent of the physical medium used and also independent of manufacturers and the type of devices. The communication architecture of the future SG is yet to be defined. As a result, multiple communication technologies and standards could coexist in different parts of the system.

Wireless sensor networks (WSN) research should be extended to SG and metering. WSN has been an active research topic for nearly ten years and has found many applications. Smart grid/metering appears to be a major application for WSN, especially related to IoT and machine-to-machine (M2M) communications. Existing industry efforts include IETF 6LoWPAN and ROLL. Internetworking between cellular networks and local area networks (e.g. WLAN) has received a lot of attention because of the need for seamless mobility and quality of service requirements.

Because of the scale and deployment complexity of SGs, telecommunication network systems supporting SGs are likely to rely on the existing public networks such as cellular and fixed wired access technologies, as well as private and dedicated networks belonging to different administrative domains. The purpose of such networks can be seen not only as a communications medium to exchange monitoring and control information, but also as an enabler of new services and applications. In many ways, the complexity and heterogeneity characteristics of SG communications networks will be similar to that of a wireless radio access network supporting voice and data services.

Smart metering and micro-grid are the most important components that have been incorporated in the smart grid architecture.

32.3 Cloud computing and Big Data as a part of the IoT smart grid

32.3.1 Big Data in smart grid systems

The integration of IoT technology with SG comes with a cost of managing huge volumes of data, with frequent processing and storage. Such data includes consumers load demand, energy consumption, network components status, power lines faults, advanced metering records, outage management records and forecast conditions. This means that the utility companies must have hardware and software capabilities to store, manage and process the collected data from IoT devices efficiently and effectively.

Big data is defined as data with huge volume, variety and velocity (three V's). The high frequency of data collection by IoT devices in SG makes the data size very large. The variety is represented by the different sensors that produce different data. The data velocity represents the required speed for the data collection and processing. Hence, IoT-based SG systems can apply the techniques of big data management and processing (such as hardware, software and algorithms).

The frequency of data processing and storage for IoT-based SG systems varies from application to application. For instance, some applications perform their tasks during a specific time of a day, such as weather forecasting, which can be performed daily at the nighttime. Other applications perform their tasks all the times, such as real-time online monitoring of transmission power lines, so these requirements need consideration in managing and processing their data. Big data analytics can help to manage real-time and huge data.

In SG, the SCADA system is the main element of decision-making. It collects data from IoT devices that are distributed over the grid and provides real-time online monitoring and controlling. Additionally, it helps to manage the power flow throughout the network in order to achieve consumption efficiency and power supply reliability. Generally, it is located on local computers at various sites of the utility companies. With the growing size of SGs, utility companies face a challenge in keeping SCADA systems updated and upgraded. In order to solve this problem, cloud computing is a good solution to host

SCADA systems. Cloud computing enables on-demand access to a shared pool of computing resources, such as storage, computation, network, applications, servers and services.

IoT-based SG systems involve processing data that requires Big Data techniques (Fig. 32.12).

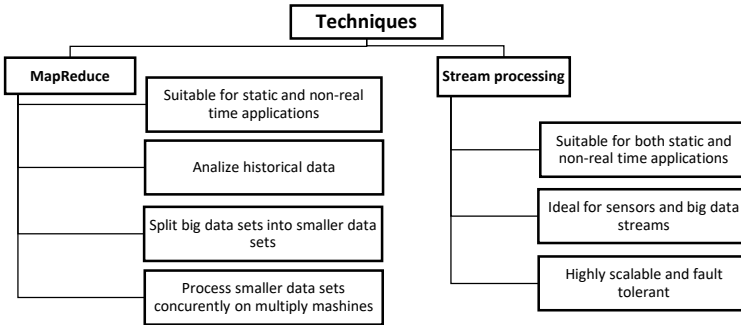


Fig. 32.12 – Big Data techniques for SG

The techniques for big data processing include MapReduce and stream processing. MapReduce is suitable for static and non-real time applications and it analyzes large historical data. It splits big data sets into smaller data sets and processes these smaller data sets concurrently on multiple machines. Stream processing is suitable for both real and non-real time applications and is ideal for sensors and big data streams. It is fault tolerant, and it has a great potential for big data management in IoT-based SG systems.

32.3.2 Cloud computing as operation platform for smart grid

The operation platforms for big data management in SG systems include cloud computing and fog computing.

Cloud computing is a model that enables convenient, ubiquitous, on-demand access to a pool of computing resources (e.g. servers, networks, applications, storage, and services) that are configurable. With minimal management effort, resources can be provisioned and

released seamlessly. NIST's visual model of cloud computing definition is shown in Fig. 32.13.

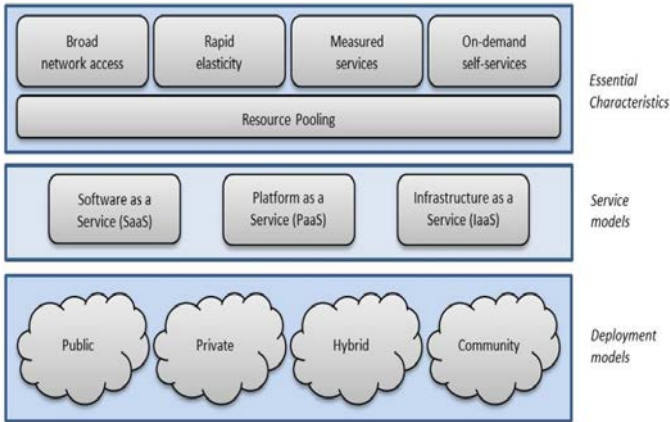


Fig. 32.13 – NIST Visual model of cloud computing definition

It delivers infrastructure, platform, and software to customers as subscription-based services in a pay-as-you-go model. The advantages, essential characteristics, of using a cloud-computing model are as follows:

- *On-demand self-service:* A consumer can individually provision computing capabilities as needed automatically without requiring human interaction with each service provider.
- *Broad network access:* Capabilities are available over the network. It can be accessed through standard mechanisms, to be used by heterogeneous thin or thick client platforms.
- *Resource pooling:* A multi-tenant model is used to serve multiple consumers from a pool of computing resources. The customer has no control over the exact location of the provided resources.
- *Rapid elasticity:* Cloud computing supports elastic nature of storage and memory devices. It can expand and reduce itself according to the demand from the users, as needed.
- *Measured service:* Cloud computing offers metering infrastructure to customers. Cost optimization mechanisms are offered to users, enabling them to provision and pay for their consumed resources only.

Cloud computing provides on-demand access to a shared pool of computing resources. Sending and storing data on the Cloud raises security risk issues, due to the shared storage among several users, which makes it vulnerable to attacks. Hence, fog computing is used to solve this security risk.

Fog computing, a low latency and highly distributed model, extends the paradigm of Cloud computing to network 'edge' to overcome this issue. In fog computing, there is no need to transfer data to the Cloud, and locally stored data is processed by devices located at the edge of the network. Hence, fog computing is a good alternative to Cloud computing for SG systems. Fog computing and microgrids together can be used for reducing the energy consumption of SG system.

The IoT-Fog-Cloud infrastructure (Fig. 32.14) is a composition of fog and cloud to support IoT applications, therefore constituting a three-tiered infrastructure. It is the hierarchy of computing capacity as fog nodes, cloudlets or micro data centres.

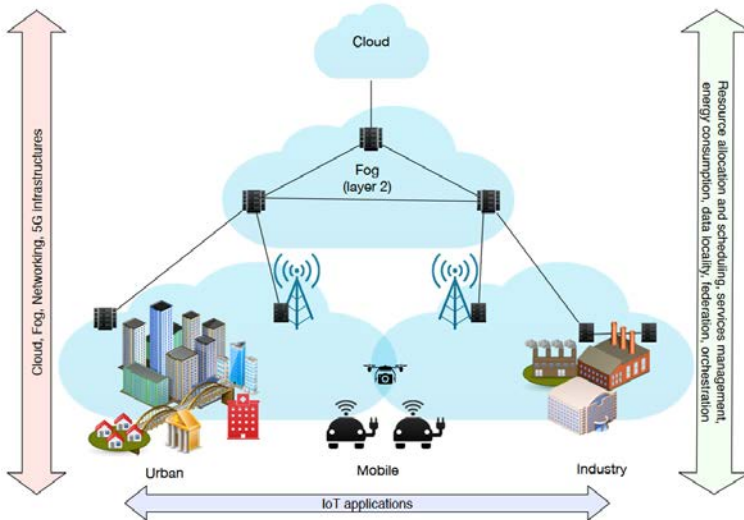


Fig. 32.14 – IoT-Fog-Cloud infrastructure [16]

32.4 Work related analysis

Newcastle University is to lead a new £20 million national centre that will permit the testing of the entire energy system in real-time. Energy experts at Newcastle University are heading the UK's largest Smart Grid project to look at how sources of power can be managed at a reasonable cost. The focus of Newcastle University's Smart Grid Lab is the simulation of distribution networks under future scenarios [20]. Scientists use technology of multi-agent systems and simulation tools for managing SG systems, including micro-grids within the home management system [21, 22]. They pay attention to the application of various information technologies based on IoT, in particular cloud computing [23].

Studies estimate that by 2020 we will have a vast IoT network comprising 50 billion connected devices. The concept of CPS, or the sensing and control of physical phenomena through networks of devices that work together to achieve common goals, has been implicit in the IoT-based SG. The researchers from University of Coimbra [18, 19] focuses on the Human-in-the-loop CPSs that incorporate human responses in IoT equation. The other areas of their interest is the wireless networks and their applications to the IoT, including to SG [24], and adaptation of the electricity distribution industry to SG technologies and related business models [25]. In addition, scientists study cloud and fog computing, their application in complex network structures, which are SGs [16]. This is a promising area of research that involves the integration of heterogeneous devices and technologies in the Internet of Everything [17].

The authors from Leeds Beckett University are considering the late problems of cloud computing in relation to IoT applications, for example IoT-enabled devices in distributed cloud computing environment [26].

The SG systems are also explored at the KTH Royal Institute of Technology (Stockholm). These include problems communication and security technologies for SG [28], communication aspects of IoT-grid [27], simulation of various components of smart grids, ranging from micro-grids to the national level [29].

Conclusions and questions

The fourth industrial revolution known as Industry 4.0 has paved the way for a systematical deployment of the modernized power grid to manage continuously growing energy demand by integrating renewable energy resources. In this context, a SG by employing advanced information and communication technologies, intelligent information processing and future-oriented techniques allows energy utilities to monitor and control power generation, transmission and distribution processes in more efficient, flexible, reliable, sustainable, decentralized, secure and economic manners.

This Section presents a comprehensive knowledge on SG components with information technologies in the context of IoT. In addition, this study gives an overview of different SG communication applications and technologies, their benefits, characteristics, and requirements. Finally, this Section discusses problems with the use of new directions such as cloud computing and big data for SGs.

In order to better understand and assimilate the educational material that is presented in this section, we invite you to answer the following questions.

1. What is smart grid? Give a definition of smart grid.
2. How is a smart grid different from the existing grid?
3. How Internet technology affects smart grid?
4. What are the key components of modern smart grids?
5. Name the domains of the conceptual model IoT smart grid and give them a brief description.
6. What networks form smart grid at the national level?
7. What is a cyberphysical system?
8. What kind of cyber-physical equipment used in smart grid systems?
9. Describe the communication protocols in the IoT smart grid.
10. What is 6LowPAN frame structure for smart grid applications?
11. What are smart meters communications networks?
12. What techniques of Big Data are used for IoT smart grids?
13. What operation platform is used to cloud computing for IoT?
14. What cloud services are used in smart grids?

15. What are the prospects of using the cloud computing in the area of IoT smart grid?

References

1. IEEE Standards Coordinating Committee 21 (2011). IEEE Guide for Smart Grid Interoperability of Energy Technology and Information Technology Operation with the Electric Power System (EPS), End-Use Applications, and Loads.
2. International Energy Agency Smart Grid Roadmap (2011): <https://www.iea.org/publications/freepublications/publication/smartgridsroadmap.pdf>
3. Update of the NIST Smart Grid Conceptual Model (2018) – https://www.nist.gov/sites/default/files/documents/2018/09/25/draft_smart_grid_conceptual_model_update.pdf.
4. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0. NIST Special Publication 1108r3. – September 2014.
5. CEN-CENELEC-ETSI Smart Grid Coordination Group. Smart Grid Reference Architecture. November 2012. – https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf.
6. Saleem Y., Crespi N., Rehmani M.H., Copeland R. (2017) Internet of Things-aided Smart Grid: Technologies, Architectures, Applications, Prototypes, and Future Research Directions. arXiv:1704.08977.
7. Gunes V., S. Peter, T. Givargis, and F. Vahid, (2015) A survey on concepts, applications, challenges in cyber-physical systems, KSII Trans. Internet Inf. Syst., 2015, 4242–4268. doi: 10.3837/tiis.2014.12.001
8. Lee E. A. (2008) Cyber Physical Systems: Design Challenges. 11th IEEE Symposium on Object Oriented Real-Time Distributed Computing (ISORC), 363-369.
9. Giusto D., Iera A., Morabito G., Atzori L. (Eds.). (2010) The Internet of Things, Springer, 2010.
10. Jin X., He Z., Liu Z. (2011) Multi-agent-based cloud architecture of smart grid, Energy Procedia, 2011, 12, 60-66.
11. Al-Omar B., Al-Ali A. R., Ahmed R., Landolsi, T. (2012) Role of Information and Communication Technologies in the Smart Grid. Journal of Emerging Trends in Computing and Information Sciences, 3, 707-716.
12. Gungor V. C., Sahin D., Kocak T., Ergut S., Buccella C., Cecati C., Hancke G. P. (2013) A Survey on Smart Grid Potential Applications and Communication Requirements. IEEE Transactions on Industrial Informatics, 9, 28-42. <http://dx.doi.org/10.1109/TII.2012.2218253>

13. Huang Z. C., Yuan F. (2015) Implementation of 6LoWPAN and Its Application in Smart Lighting. *Journal of Computer and Communications*, 3, 80-85.
14. Al -Ali A. R., Aburukba R. (2015) Role of Internet of Things in the Smart Grid Technology. *Journal of Computer and Communications*, 3, 229-233.
15. Naveen P., Ing W. K., Danquah M. K., Sidhu A. S., Abu-Siada A. (2016) Cloud computing for energy management in smart grid – an application survey. *CUTSE2015. OP Conf. Series: Materials Science and Engineering*.
16. Bittencourt L., Immich R., Sakellariou R., Fonseca N., Madeira E., Curado M., Villas L., DaSilva L., Lee C., Rana O. (2018) The internet of things, fog and cloud continuum: Integration and challenges, *Internet of Things*, 2018, vol. 3-4, 134-155.
17. Velasquez K., Abreu D. P., Assis M. R. M., Senna C., Aranha D. F., Bittencourt L. F., Laranjeiro N., Curado M., Vieira M., Monteiro E., Madeira E. (2018) Fog orchestration for the internet of everything: state-of-the-art and research challenges, *Journal of Internet Services and Applications*, 2018, 9 (1).
18. Nunes D., Sá Silva J., Boavida F. (2017) *A Practical Introduction to Human-in-the-loop Cyber-physical Systems*. – John Wiley & Sons Ltd., 2017.
19. Nunes D. S., Pei Z., Sá Silva J. (2015) A survey on human-in-the-loop applications towards an internet of all. *IEEE Communications Surveys & Tutorials*. Vol.17, Issue 2, 944-965.
20. Newcastle University. Science Central Smart Energy Labs. – <https://www.ncl.ac.uk/media/wwwnclacuk/instituteforsustainability/files/Smart-Energy-Labs-Online.pdf>
21. Li W., Ng C., Logenthiran T., Phan V.-T., Woo W. L. (2018) Smart Grid Distribution Management System (SGDMS) for Optimised Electricity Bills, *Journal of Power and Energy Engineering*, 2018, 6, 49-62.
22. Li W., Logenthiran T., Phan V.-T., Woo W. L. (2016) Intelligent multi-agent system for power grid communication, *Region 10 Conference (TENCON)*, 2016 IEEE, 3386-3389.
23. Zeng W., Koutny M., Watson P. (2015) *Opacity in Internet of Things with Cloud Computing*. University of Newcastle upon Tyne, England, 2015.
24. Granjal J., Monteiro E., Sá Silva J. (2015) Security for the Internet of Things: A Survey of Existing Protocols and Open Research issues, *IEEE Communications Surveys & Tutorials*, Vol. 17, Issue 3, 1294-1312.
25. Pereira G. I., Specht J. M., Silva P. P., Madlener R. (2018) Technology, business model, and market design adaptation toward smart electricity distribution: Insights for policymaking, *Energy Policy*, Vol.121, 426-440.

26. Amin R., Kumar N., Biswas G. P., Iqbal R., Chang V. (2018) A light weight authentication protocol for IoT-enabled devices in distributed Cloud Computing environment, *Future Generation Computer Systems*, V.78, 1005-1019.

27. Tanyingyong V., Olsson R., Cho J., Hidell M., Sjodin P. (2016) IoT-Grid: IoT Communication for Smart DC Grids, 2016 IEEE Global Communications Conference (GLOBECOM), Washington, DC, 2016, 1-7.

28. Dhaou I. B., Kondoro A., Kelati A., Rwegasira D. S., Naiman S., Mvungi N. H., Tenhunen H. (2017) Communication and Security Technologies for Smart Grid, *International Journal of Embedded and Real-Time Communication Systems*, vol. 2, no. 8, 40-65.

29. Kondoro A., Dhaou I. B., Rwegasira D., Kelati A., Shililiandumi N., Mvungi N., Tenhunen H. (2017) Simulation Tools for a Smart Micro-Grid: Comparison and Outlook, *Proceeding of the 21st Conference of FRUCT*, Helsinki, Finland.

33. IOT INFRASTRUCTURE FOR SMART ENERGY GRID BASED ON EMBEDDED SYSTEMS DEVICES

Prof., DrS. M. P. Musiyenko, Ass. Prof., Dr. I. M. Zhuravska,
Dr. Y. M. Krainyk (PMBSNU)

Contents

33.1 Development of I&C and harvesting systems for local SEG	55
33.1.1 Complex interdependencies that characterize local SEG	55
33.1.2 Architecture of I&C and harvesting systems	58
33.1.3 Devising methods of I&C and harvesting systems	60
33.2 Hardware components for local SEG (sensors, measurement units, control units – Raspberry Pi, STM32 boards, ESP8266, PLC, Phoenix, etc.)	61
33.2.1 Sensors, measurement units. Energy measurement systems using PLC technology (IEEE 1901)	61
33.2.2 IoT control solutions based on STM32 boards, ESP8266	62
33.2.3 PLC in SEG architecture. Mini-computers for local SEG	69
33.3 Software components of SEG	71
33.3.1 Protocols for device communication	71
33.3.2 Cloud infrastructure used by local SEG	74
33.3.3 Local software for SEG. Software platform named “mbed” for local infrastructure IoT solution	75
33.4 Work related analysis	77
Conclusions and questions	79
References	81

Abbreviations

AMI – Advanced Metering Infrastructure

CoAP – Constrained Application Protocol

CPS – Cyber Physical System

HAN – Home Area Network

HTTP – Hyper-Text Transfer Protocol

IDE – Integrated Development Environment

IoT – Internet of Things

JSON – JavaScript Object Notation

MAC – Medium Access Control

MQTT – Message Queue Transfer Telemetry

NAN – Neighborhood Area Network

PHY – Physical layer

PLC – Power Line Communications

SEG – Smart Energy Grid

SPI – Serial Peripheral Interface

TCP – Transfer Control Protocol

UART – Universal Asynchronous Receiver/Transmitter

UDP – User Datagram Protocol

WAN – Wide Area Network

WSN – Wireless Sensor Network

XML – Extensible Markup Language

33.1 Development of I&C and harvesting systems for local SEG

33.1.1 Complex interdependencies that characterize local SEG

Smart Energy Grid (SEG) is the modern concept of energy control, harvesting, consumption, and distribution that supposes high integration of all components related to energy. Despite being a concept, it is widely supported and implemented in various forms all over the world. The concept grasps from the low level (consumers' houses and premises) up to energy strategy on city or even state level. Different specific devices and technologies characterize each level of the SEG. At the top level there sophisticated and complex systems that control power plants and devise schemes of optimal distribution according to the analysis of consumption data. However, the local level of SEG is also of great interest for researches as well. Local consumers form the biggest amount of total energy consumers. Taking into consideration the fact that they also actively participate in generation of electricity for their own needs, local SEG is a perspective area for new models and methods of energy control. In addition, local SEG is the area where deployment of IoT-devices can be performed in an essential way and advance with the latest benefits of IoT-technologies. In general, this segment is much easier to adopt for new technologies due to much less limitations than in other layers of SEG.

Local SEG can be interpreted as small-scale SEG part related to household or group of households that actively participate in consuming and also producing energy in the grid. This introduces new notion "prosumers" for local SEG that is capable of consuming and producing energy at the same time. Contemporary energy generating systems based on alternative energy sources (wind, solar energy) are usually installed in local SEG to produce energy immediately for consumers' requirements. However, there are also other basic components of local SEG that introduce elemental level of SEG in general. Those components can be installed by default or may be further set up individually. According to the widely used notation, local SEG is comprised of elements of Home Area Network (HAN) and

Neighborhood Area Network (NAN) [10]. The main elements of HAN in this infrastructure are:

1. Consuming devices (fridges, vacuum cleaners, multimedia devices, boilers, etc.).
2. Networking devices (routers, gates, consumers' personal devices, etc.).
3. IoT-devices for local SEG (specialized gadgets or sets of gadgets to perform information, control, and analysis functions inside local SEG; all of them form the core of the IoT in local SEG).
4. Advanced Metering Infrastructure (AMI).
5. Energy generating devices.
6. Energy storage devices (accumulators).

From the IoT point of view, all specified devices must have connection to the local network either immediately or via other devices. Network connectivity is the critical point for IoT development. Primarily, the main idea is to provide reading, control, observation over electrical devices in the household to optimize total consumption of energy. Networking devices not only connect to the network but also ensure connection to the network for other devices, first of all, consuming devices. Devices that belong to this category are microcontrollers and wireless modules with necessary peripheral interfaces included.

The main challenge for IoT in local SEG is heterogeneity of the environment. It can be alleged that unification of smart devices for local SEG is only at the beginning despite lots of researches investigate this problem. Heterogeneity is observed on every level of local SEG infrastructure but mostly, this is a peculiar feature of the level comprised of IoT-devices. Market of smart devices is full of miscellaneous solutions with different software and hardware basis.

Typically, application layer, network layer, and perception layer are distinguished in the researches on architecture of SEG. However, devices concerned with energy usually omitted in this structure. At the same time, they make a huge impact on the architecture of local SEG in each specific case. That is why, we suggest usage of additional energy infrastructure layer that includes all abovementioned devices that consume, generate, and store energy. General architecture regarding proposed changes is shown in Fig. 33.1.

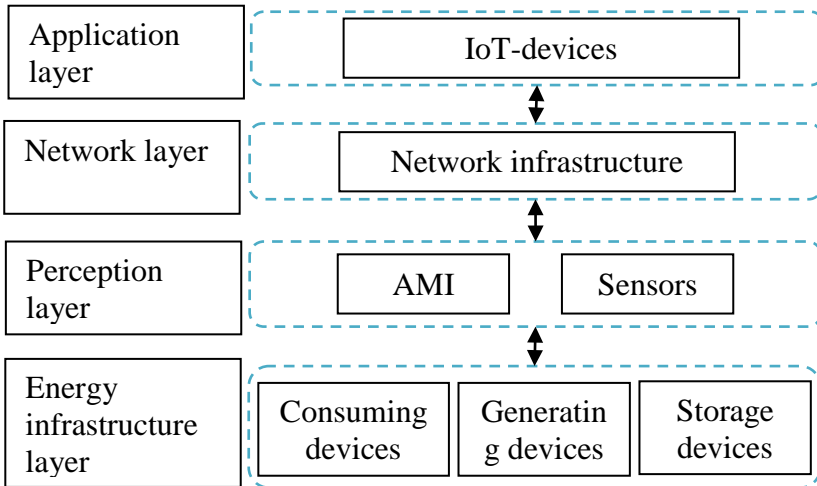


Fig. 33.1 – General architecture of local SEG with IoT

Although direct two-sided interconnection is depicted for each layer with the next one, in fact, real-world local SEGs can be rather different and vary in many ways. Some IoT-devices can perform networking functions, which means overlapping between application and network layers. Beside with direct responsibility of measuring consumption parameters, AMI also offers some basic network functions as well as primitive control activities from user side. Some network devices implement applications to communicate with sensors directly. Sensors are usually connected directly to IoT-devices that are limited in computational capabilities. However, they are closely coupled with sensor and perform reading, writing, and configuration of sensors. They also contain small amount of business-logic in firmware to optimize communications inside network. Just like small IoT-devices, user's personal devices play significant role in the architecture. Customer communicates with entire system via application software in his/her smartphone or other multimedia device. Energy consuming, generating, and storage devices relate to each other. We consider this layer as the most basic form of energy distribution in local SEG scope. Application layer perceives information about consumption and generation through perception layer. Then it performs actions according to the objective to

minimize expenses on energy bills. It is aware of cost of energy during periods of day and all details about local customer's assets. Based on this information, application layer automates control over electronic equipment to consume energy frugally.

Only most common and basic scenarios for the considered architecture have been shown previously. Real-world implementations of the model could be even more complex in case they contain all modern technologies. We can conclude that with emergence of IoT in the field of local SEG new challenges start. Local SEG is getting more complex as it requires more device to deploy. The number of connections among devices with different purposes inside network is constantly increasing. That requires complex solutions that should take into account all peculiarities of the system.

33.1.2 Architecture of I&C and harvesting systems

From the architectural point of view, different approaches are applied to describe architecture of SEG in general and particularly local SEG. Architecture depends on devices used in the network, interactions among devices, software running on IoT-part of the system, functions performed by each node, etc. Layered architectures are dominating in SEG research as they provide clear and unified bottom-top approach to organize every node in the grid. We can distinguish the following types of architectures [1, 2, 4]: three-layered, four-layered, energy efficient, last-meter, web-enabled.

All of them include information and control (I&C) components. But only the last one involves harvesting component. As has been mentioned earlier, consumer's side may contain sources of energy (solar, wind power, etc.) of its own. However, last-meter architecture is tightly related to local SEG with IoT. In our opinion, combination of these two architectures is the best option to depict IoT-enabled local SEG with energy harvesting capabilities. We depicted our vision of the united architecture in Fig. 33.2.

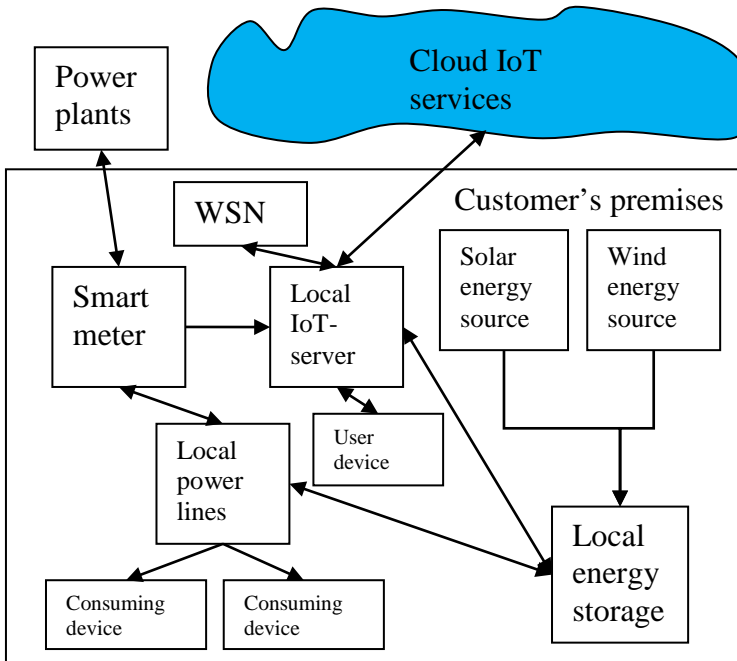


Fig. 33.2 – Architecture of local SEG with harvesting capabilities

As displayed in Fig. 33.2, architecture contains sources of energy connected to local power lines. Control and analysis of consumption are performed using local IoT-server. It relies on the data received from smart meters, sensor network, user devices, and power lines and performs analysis to reduce cost of energy for the customer. Customer accesses server using application installed on his/her devices. Application is granted to perform control over whole IoT system in local SEG. Thus, it can also set autonomous mode when every action takes place under default circumstances without control from the user side. According to the analysis results, IoT-server makes decision about usage of accumulated energy available in storage. There are many factors that impact on final decision:

- time of the day;
- total load of power network;
- cost of energy according to bill plan;

- available amount of energy in the storage;
- expected generation from local energy sources;
- presence of the users in building and number of users and others.

All the components of the architecture are described in the following material.

33.1.3 Devising methods of I&C and harvesting systems

Depending on the actual architecture of local SEG with IoT capabilities, different methods can be applied for information transmission and collection, control, and harvesting energy resource inside the network.

The central element of I&C and harvesting system is IoT-server that maintains all specified tasks. IoT-server should contain necessary amount of storage space to save statistical data for further analysis and processing. Retrieved data from sensors, statistics on the previous parameters and payments, smart meters data are used to form control actions for the whole system in general and for each element. That implies necessity of appropriate computational resources in hardware part of IoT-server. Data from sensors arrive at random time and the system must be ready to process several requests simultaneously. Structure of the network in IoT is changeable and tends to constant switch of configuration. Addition or removal of the modules, their substitution suppose that the system must have reserve for scalability. By default, it should not run on its maximum parameters and should accept this kind of changes without notable drawbacks in performance or stability.

Harvesting of energy is a commonly used notion for the process of accumulating and storing energy in appropriate storage as the backup source of energy. It has different scales from microcontroller-based systems [12] with minimal requirements for energy to large systems like local SEG. Local SEG has peculiarities of its own, as the main objective is to minimize payment for energy bills. It is an ordinary situation when building is equipped with energy generators that work on renewable energy. These generators not powerful enough to guarantee stable electricity supply for the entire household. Therefore,

consumption of generated energy and energy obtained from electrical plants have to be balanced regarding resources of generators and storage devices.

33.2 Hardware components for local SEG (sensors, measurement units, control units – Raspberry Pi, STM32 boards, ESP8266, PLC, Phoenix, etc.)

33.2.1 Sensors, measurement units. Energy measurement systems using PLC technology (IEEE 1901)

In IoT sensors play the major role in IoT-environment. In the most common sense, sensors provide compulsory mechanisms for measuring and evaluating state of IoT-system. Each sensor requires device that reads data from sensors (sensors can be grouped) as well as device that transfers data over the network to the destination application (often both functions are integrated in a single module). As wired connections require organization of connection by physical parts, wireless connection has become de-facto standard for sensor integration into the network. Wireless Sensor Network (WSN) is one of the fundamental concepts of IoT.

Investigations of sensors applications for SEG state that sensors organize basic level for intellectual management of energy resources. They provide necessary information about system (temperature, humidity, pressure, presence of objects, etc.) so control devices can react to changes in parameters.

AMI is one of the most important parts of local SEG tightly coupled with sensors. AMI has direct access to the data about consumption and provides access to the data to customers. Collection of data from AMI in the control device is basis for analysis and forming consumption plan for user equipment. The result statistics is used for selection of appropriate consumption plan to reduce overall consumption [11].

The main component of AMI is a set of smart meters. They send information to both customers and energy generating and distributing companies. Customers get data about consumption and can react to shorten uses of energy. Companies receive data to form monthly bill.

Installation of smart meters is negotiated between customers and companies.

AMI spreads its responsibilities over HAN, NAN, and even Wide-Area Network (WAN). It is one of the cornerstones of local SEG and to deliver data to the destination AMI utilizes different technologies. The most widespread communication technique for smart meters is wireless technologies (Wi-Fi, ZigBee, etc.). However, there is also possibility to send data directly over electrical wires. Power-Line Communication (PLC) technologies release solution for the market of smart meters that does not require installation of additional wired equipment. In this case, data transmission is performed using existing electrical wires. Only one additional PLC-device is required to support this method of smart metering. It is connected into power socket (serves as gateway between PLC and WAN-accessing technology) and can send data to other information network nodes.

IEEE 1901 standard is a standard of high-speed communication over power lines with maximum possible speed up to 500 Mbit/s. However, smart metering information exchange does not require such high speed. Even transmission with speed of order of dozens kbit/s is sufficient to pursue main objectives of metering technology. To support both high-speed communications and smart metering new standard has emerged. IEEE 1901.2 [7] identifies narrow-band PLC technology that is able to provide low-speed data transfer for devices like smart meters. It specifies MAC and PHY layer for communications. Higher levels can be defined by producer of the units. This standard sets data rate 234 kbit/s as maximum and formulates additional data protection from external influences in form of error-correction coding.

33.2.2 IoT control solutions based on STM32 boards, ESP8266

Microcontrollers are extensively used in the construction of IoT-systems. Previously, microcontrollers were considered to be the basis of embedded systems and all control functions were responsibilities of single microcontroller or group of microcontroller. With emergence of IoT-concept, embedded systems can be considered as the lowest level of the entire global IoT-system. In their origins, embedded systems were oriented on performing strictly prescribed functions and providing

necessary functionality with as low expenses as it is possible. And it can be stated that embedded systems have kept their main destination in the new digital eco-system. However, extended connectivity with higher layers is an obligatory for basic devices of embedded systems nowadays. They have to be able to provide information on request from higher level devices as well as communicate in their own network. This peculiarity determines current development line for microcontrollers. First of all, modern microcontrollers can have a lot of peripheral connections (for sensors, actuators, mechanical parts, etc.). Secondly, they provide extended connectivity with wireless devices. Though, specific device usually supports only single technology to transfer data over the air, it has become a great step forward in development of IoT-systems. Built-in resources for wireless communication (e.g. Wi-Fi, Bluetooth, ZigBee) guarantees connection to high-level devices and, thus, even simple system can connect to other devices [5].

Low energy consumption constraint combined with adequate computation abilities is required from microcontroller-based control systems. The microcontroller as a control device is responsible for setting up and reading data from sensors, collecting and analyzing data, sending control impulses to connected devices, and further transfer to the higher tier of the system. Contemporary microcontrollers are devices with quite powerful computation core. At the same time, they provide scalability of energy consumption by working in different low-power modes. Low-power modes are operation modes in microcontrollers that suppose lower consumption of energy at the expense of reducing full functionality of device (unavailable peripheral devices, lower internal frequency, temporary halt in code execution process, etc.). As the result, consumption can achieve values of dozens of nAh in some cases. This fact provides numerous benefits because the devices can function fully autonomously without necessity to connect them to power supply network as they can function from autonomous energy source. Such energy source does not require substitution or recharging for periods of up to several months (depends on peculiar device type).

It is obligatory for control devices not to consume extended amount of energy to perform their functions, especially in IoT-segment that is connected to local SEG. Cost-effective solutions that can

frugally utilize energy resources are necessary for this kind of application. In general, they have to use as little energy as it is possible and, moreover, bring additional benefits from intellectual control of other devices. The intellectual control of other devices can decrease total amount of spent energy.

Producers of microcontrollers nowadays follow the scheme when they use ready architecture and adopt it for the specific task which results in different series of devices. Some of them are computation-centric and others are oriented on low energy consumption. But the general idea is common or similar core for miscellaneous devices. In case of 32-bit microcontrollers, the niche of architecture provider is occupied by ARM Company. Their architectures are utilized by ST Microelectronics, NXP, Nuvoton, Microchip, and other companies. The statement about similarities in architecture supposes that devices produced by different vendors have a lot of similarities both in hardware and software. However, the software is not directly interchangeable between devices because of peculiarities in hardware part. Moreover, each company provides their own recommended set of software libraries to develop firmware for microcontrollers. These libraries are incompatible and bonded to be used with specific microcontroller. As there are no benefits of interoperability among devices, the preference of usage specific microcontroller depends on the following factors:

- quality of the software libraries;
- support in the development tools (project generation, initial configuration of peripherals, support of debug, etc.).

Both mentioned factors depend strictly on producing company. ST Microelectronics delivers ready-to-use libraries as well as development software to simplify design process. The set of tools they offer to the developer contains integrated development environment (and support from other environments), configuration manager, programming utility, and software with capabilities of logic analyzer used specifically for debugging purposes to obtain values of variable in real-time. The extended set of means identifies determination of the company to be on the leading edge of technologies and explains leading position of the company on microcontroller market and dissemination of their devices all over the world. In the second half of the previous decade,

ST Microelectronics started producing modern 32-bit microcontroller and sold them at low cost. This fact shifted the market from dominated at that time 8-bit microcontrollers to more powerful and advanced microcontrollers with support of 32-bit operations.

As for an instance, we consider typical scenario when microcontroller's core runs in default mode only to perform readings from sensors and then checks overall state of the system and goes into low-power modes afterwards. The aforementioned cycle is supposed to be constantly recurring with fixed sequence of transitions between states. Actually, the last state among them is the state that device spends most time for. As a consequence, total consumption on the period of cycle is quite small value. Modern software tools grant user an option to make preliminary assumption about power consumption. Configuration manager STM32CubeMX contains this type of tools as one of the tabs in user interface of the software. In Fig. 33.3 the example visualization of consumption profile is shown. Single-cycle takes about 10 minutes with only 2 seconds when device performs processing tasks.

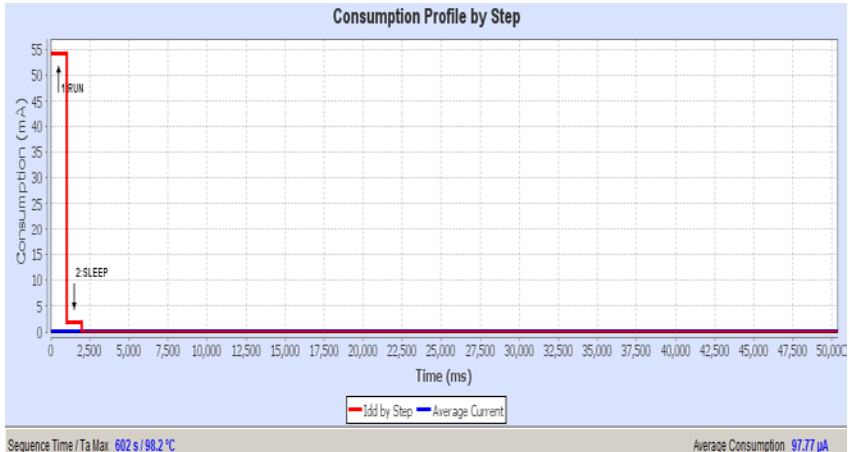


Fig. 33.3 – Consumption plan for microcontroller with predetermined activity cycles

Moreover, only one second is designated to be in active (RUN) mode. During active mode several interface units are active (ADC, SPI,

UART) alongside with core that runs at the maximum frequency. Following sleep step is considered to be transitional step to ensure correct state of the peripherals and core itself before going into STEADY state. This state lasts for 10 minutes and then the cycle begins from the start. From the hardware point of view, restart of the cycle is provided by watchdog timer but it can also be some other peripherals.

Regarding aforesaid use case, it can be concluded that outer influence (reading sensors) is applied to microcontroller only in periods of time according to schedule. Microcontroller wakes up from the STEADY state in predetermined moments. Therefore, according to the analysis result from the tool, it is possible to attain average consumption 97, 77 μ A during this period. This outcome means that this part of the system can be easily supplied with autonomous power source only.

Another scenario, that is more relevant to changeable and continuously running IoT-infrastructure, is the option when several external interrupts happen during single time frame. UART-message, GPIO-interrupt, timer wake-up signal can be considered as interrupt signal in this case. Previous condition limits possible transition between the low-power modes as this time STEADY state is not available. Usage of mentioned interrupts makes transition to this state impossible. This fact has implication that average consumption rises significantly. Despite both STEADY and SLEEP are low-power states, consumption indicator is rather different for them. The SLEEP state allows interruption from different external sources while the STEADY state assumes disabling almost all peripherals and computation core itself. In Fig. 33.4 another sample has been depicted.

Average consumption rises to 7.14 mA on the considered time interval. There are also three active periods when processor is actually working and performing computations. The number selected for demonstration purpose only and total number of peaks during period of time may vary. In opposite of the previous case, there is also no transition into STEADY state. Absence of this transition affects average consumption on the interval. In general, it entails in substitution of autonomous power source with more energy storage and, as a result, increased cost of the system. However, this very scenario is the one that is more probable to occur.

Among a big number of modern microcontrollers we consider ESP8266 as one that is worth special emphasizing. This is a product of Espressif company that conquered great popularity not only among embedded developers but also among scientists who are interested in IoT-related researches. The reason for such popularity is a combination of Wi-Fi connectivity, diverse peripheral interfaces, computational facilities, and low price. Separate unit costs approximately 3 USD. It provides outstanding resources for computation as it is able to run at clock frequency 160 MHz. There are various application fields where ESP8266 is applied. But the common idea is connection to WLAN with the following data transfer to remote nodes or local nodes with appropriate interfaces.

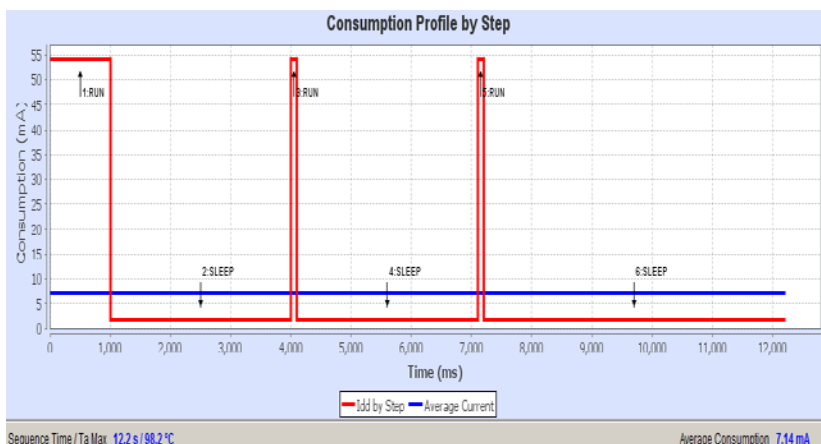


Fig. 33.4 – Consumption profile for interrupt-based case

One of the main peculiarities of ESP8266 is its energy consumption parameters. Connection to Wi-Fi network and data transmission/receiving consumes a lot of energy and equals to hundreds of mA during this intervals. It is notably higher than consumption of microcontroller. Another obstacle concerned with consumption of the module is limitations of low-power modes. The module supports them but transition into low-power mode implies closing network connection. Thus, the device goes out of the network and cannot receive data from user devices or send data into the network. This fact

presumes the device's workflow with constant switching between active state and low-power state. This approach is valid for autonomous power supply. In case of direct power supply, it is not necessary to enter into low-power mode and device can be constantly available.

Another aspect that is worth mentioning about ESP8266 is development of software. There are three different options for writing programs for ESP8266:

1. Hardware Abstract Library (HAL).
2. Arduino-based software libraries.
3. Interpreter-based firmware (Lua, Python).

The first one offers access to the lowest level of hardware and benefits of better performance. However, the development process requires full understanding of device architecture. Even small inaccuracy may (e.g. wrong sequence of function calls) result in wrong behavior of the system. This approach requires expert-level knowledge and experience. The second approach assumes usage of well-known Arduino IDE and adopted libraries. The libraries simplify development process by offering Arduino-style set of functions (GPIO control, connection control, interface data management, etc.) that is familiar to all developers who have experience with Arduino platform. The code of the libraries is not optimized to maximum level and, in general, decreases productivity. Nevertheless, the output is still a compiled binary file (C++ programming language is used) and loss in performance can be considered as neglectable. Interpreter-based firmware is a compromising variant between performance and convenience of development process. Practically, the firmware is an interpreter of corresponding language (NodeMCU for Lua and MicroPython for Python are the most commonly used). In other words, user software in this case may be considered as a program that runs inside another program (interpreter). The firmware also contains restricted set of libraries used in general version of language. The main reason of this is device's memory limitation. As interpreter runs, user can add his/her own program in form of script. Interpreter runs specific version of file system and offers user to keep programs as files in file system. Additionally, the firmware offers user built-in libraries that are optimized exactly for IoT. First of all, they provide support for main communication protocols (MQTT, CoAP). There is also support of the

networking (TCP, UDP) out of the box. It implies that ESP8266 can act both as a server (with limited number of incoming connections) and as a client. As an advanced feature the firmware has set of calls that can be used to access remote web-services. This rich set of networking accessories makes this module suitable for majority of IoT-applications even with quite big complexity. The main drawbacks of interpreter-based firmware are weaker performance and extensive memory usage. However, usually IoT-applications do not need complex calculations and massive storage of data, so ESP8266 running interpreter-based firmware is balanced choice for IoT in local SEG.

33.2.3 PLC in SEG architecture. Mini-computers for local SEG

Power-Line Communication (PLC) is technology of information transmission over the electrical power lines. Appearance of the PLC technology was caused by necessity of data transmission in premises with no possibility to place new equipment. The basic principle of data transmission via PLC is modulation on information signal with carrier frequency that exists in electrical wiring. Modulation frequency is much higher than carrier frequency, which makes possible to achieve high transmission speed (it is claimed to achieve throughput of order hundreds of Mbit/s). PLC-enabled devices are the part of local network infrastructure as their main purpose is to guarantee data transmission and reception.

In the context of IoT for local SEG, PLC is very promising technology because PLC-devices are plugged directly into power sockets. It allows measuring and monitoring, controlling, and sending data about power consumption over the local network (additional devices are required for these operations in case they are not included). In fact, IoT, SEG, and PLC converge at one point with plenty of obtained advantages for information and electrical spheres.

PLC technology in IoT for local SEG is blurring borderlines among power lines, networking, and measurement of energy consumption. In common sense, place of PLC technology in this segment is displayed in Fig. 33.5 (based on Fig. 33.1 from [8]).

PLC devices connect into power sockets inside the building. Exchange of information is performed through house access points that get data from PLC and higher levels of SEG.

Microcontrollers and wireless modules are conceivable solutions for implementing nodes in IoT-network for local SEG. However, their calculation performance is not enough to gather all the data from the network, support multiple connections, perform control over the whole system. More powerful device is required for these types of tasks. All of them are responsibilities of main information controller. Mini-computers are the perfect contenders for occupying this place among other devices. Comparing to microcontrollers, they have more powerful computing cores which run on higher operational clock frequency, contain more advanced interfaces to connect other devices, run operating system, and capable of connecting storage devices.

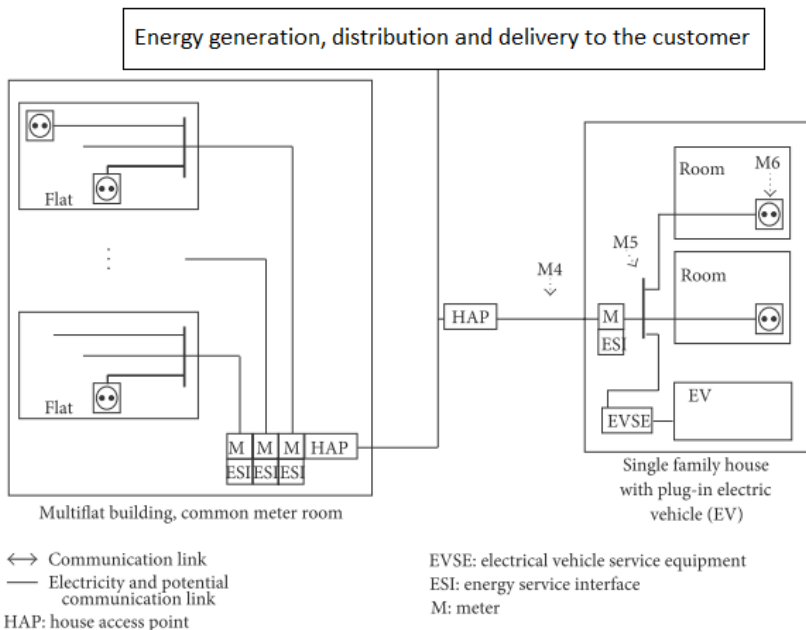


Fig. 33.5 – PLC in IoT-enabled local SEG

Taking into consideration peculiarities of IoT-system in local SEG, mini-computers are the best choice for the role of main control unit. They consume not as much power as ordinary personal computer, but still mini-computers harness necessary computational power for processing multiple request from nodes in IoT-network.

The list of famous mini-computers includes

- Raspberry Pi (most wide-spread device);
- Orange Pi (proposes miscellaneous devices for various application fields);

- Nano Pi (concentrates on minimalism in device's size);

- Cubieboard (one of the most powerful alternatives);

- UpBoard (supports Windows 10 operating system);

- Odroid (supports Android operating system) and many others.

Mini-computers play server role in architecture of local SEG based on IoT. They perform the following assignments in the system:

1. Collect data from all nodes inside network.

2. Analysis of all actions performed by control devices in the network.

3. Observe state of the nodes and make appropriate stimuli to keep each node and system in general in stable state.

4. Handle faults in separate node and recover it to the workable state.

Practically, it means that mini-computer, as control server in local SEG is aware of almost every important action that happens. It holds the whole system running. Moreover, it is interface point for user device to access information about the system.

33.3 Software components of SEG

33.3.1 Protocols for device communication

Establishing network connection among devices does not suppose that they are ready to communicate. Physical connection (wired or wireless) is a basement for information communication that is the cornerstone of IoT. Broad set of information protocols is available specifically for IoT. However, support of exact protocols depends on used device. There is still inconsistency that there is no single protocol

which is accepted as a standard and compulsory for IoT-devices support. Designers of IoT-solutions are free to choose either ready-to-use protocol or to develop their own one.

Considering protocols for device communication, it is necessary to mention that in IoT for local SEG mainly uses short messages with relatively long period between two consecutive messages from the same device. Therefore, there is no need for high-speed communications among IoT-devices in local SEG. Moreover, event-based scheduling is preferable for logical connections among the devices as it serves for lower power consumption of the modules [6]. Thus, preferable feature of the protocol for IoT in local SEG is support of event-based communication model. In the following section we highlight two protocols that are mostly utilized in IoT associated with resource constraints.

Message Queue Transport Telemetry (MQTT) protocol is a lightweight protocol for IoT. MQTT works on the top of TCP/IP stack and relies on TCP-protocol for data transmission. MQTT is based on client-server model and modifies it into publish-subscribe model. Three types of devices exist in the network. Broker device coordinates data streams among publishers and subscribers. Publisher is the device that provides some sort of information for subscribers by providing necessary information to broker. Subscribers receive updates from publishers via broker. Subscribers are notified only on the updates they are interested in. Although name of the protocol contains part “message queue” in its name, MQTT does not implement message queueing technique. Main attention is devoted to publish-subscribe mechanism that suits for event-based communications for IoT in local SEG. MQTT has a binary format so it does not contain even minimal overhead that features in XML or JSON-based protocols.

Constrained Application Protocol (CoAP) protocol is the protocol specially designed for devices with limitations in memory, computational power, lack of ready-to-use preinstalled software. CoAP works on the top of UDP-protocol which implies some peculiarities of its usage. First of all, it means that CoAP-message it not guaranteed to be delivered. However, it is strictly concerned with communication environment in local SEG where communications demand additional verification on the application layer. As for the second point, CoAP

works as transfer means for devices with limited resources that makes situations when they cannot process request even more probable. CoAP in many ways resembles HTTP-protocol which means it is easier for understanding for those who are familiar with web-development. CoAP was designed with the idea in mind to follow widespread web-based model of communication. However, in opposite to HTML, CoAP harnesses binary message format for frugal usage of resources.

Regarding communication protocols, communication technologies cannot be left unmentioned in this consideration. Wireless technologies are dominating in modern IoT-solutions and provide either their own protocols for device communication or serve as a basis for application protocols.

Wi-Fi technology is a connection between devices in local network and global network. Wi-Fi occupied the place of main wireless standard due to combinations of its features. High throughput, ease of configuration, sufficient transmission distance for local networks, simultaneous connection of all local devices (support of device quantity that is typical for local network) allow considering Wi-Fi as obligatory item in network layer of local SEG based on IoT. At the same time, IoT-devices also support data transfer over Wi-Fi. However, transmission using Wi-Fi requires high energy usage. Thus, this technology should be used cautiously as it increases consumption and jeopardies autonomous power supply resources.

Another prevalent wireless technology is ZigBee. It is based on mesh network architecture and oriented on extremely low consumption by node devices. Data transmission rate is fixed at level of dozens kbyte/s (most typical value). Thus, it is slow communication with hard limitations on the maximum transition speed. However, short information messages are the most common case for IoT in local SEG and it is not an obligatory to pass them over network with maximum speed. In most cases, system can tolerate small delays that happens during transmission. More important is reliability of the network that is one of the benefits of mesh architecture in ZigBee network. Malfunction of separate module can be overcome by rerouting data via another node that still works. ZigBee requires deployment of its own network that includes three types of devices. ZigBee End Device is responsible for communication with physical objects and sensors.

ZigBee Coordinator plays role of the link for End Devices. ZigBee Router connects different networks with each other. Thus, it is common scenario to organize multiple networks for separate type of equipment and manage multiple networks through router. It provides simple division on domain of responsibilities. One of the most substantial drawbacks of ZigBee technology is transition from ZigBee-network to IP-network. It requires separate gateway that converts internal data into data comprehensible for other devices.

Another technology for local wireless communication is Bluetooth. Latest version of Bluetooth standards claim movement towards low energy expenses and exchange of information in format of short messages. Bluetooth-compatible devices are characterized by low consumption and support of complex network structure that resembles ZigBee. However, network abilities of Bluetooth are almost never employed in their full potential.

Last but not least wireless technology that we consider in this review is 6LoWPAN. 6LoWPAN stands for IPv6 over Low-Power Wireless Personal Network. It brings IPv6 protocol into the deal with almost unlimited address space to assign. In spite of many similarities between 6LoWPAN and ZigBee, they are quite different technologies and vary especially on intermediate level of OSI Model. ZigBee is protocol that is more proprietary and uses custom technologies for communication organization. Open standards of 6LoWPAN make this technology much more attractive for beginner developer and new projects consider it as network basis for moving ahead.

33.3.2 Cloud infrastructure used by local SEG

Nowadays, cloud infrastructure is gaining an outstanding popularity for almost any information services. Permanent access to the Internet with high speed of data transmission allows sending data to the remote system for further processing, analysis, and replying to the clients. Enormous resource availability in the cloud is intended to make even toughest computation task possible. The cloud is extremely scalable so user can harness computation resources that match his/her requirements.

Regarding cloud infrastructure in context of IoT for local SEG, first of all, this is a mean of remote control for the user. It introduces concept of being all time available for electrical equipment in house area.

Another common use case of the cloud is data analysis. Several services implement interface to send data into web-service and process it using analysis functions.

The main concern about mixture of IoT in local SEG and cloud technologies is security. As an external service, cloud infrastructure is vulnerable to malware attacks and threats. Errors in general service configuration may entail data corruption if it is not encrypted properly. Thus, end user is responsible for cautious selection of the data from local network to be sent to the cloud servers. For instance, images received from the surveillance camera inside the house can be easily used by intruders if they have access to them.

Cryptographic means for IoT should match following criteria:

1. Reliability in security sense, i.e. guarantee necessary security level.
2. Conceivable computational time to compute cryptographic functions.

Researchers and developers provide different cloud services to integrate IoT with security tools. In order to fulfill requirements of the second mention item, cloud services offload devices with weak computational abilities and most computations and verifications are performed on powerful servers in cloud.

Interaction between cloud infrastructure and infrastructure of local SEG (microcontrollers and microcomputers) now can be organized in a fluent way. As has been mentioned previously, even wireless modules are able to perform remote web-requests, while microcomputers can deal with more complicated tasks.

33.3.3 Local software for SEG. Software platform named “mbed” for local infrastructure IoT solution

In the preceding part of the course materials main attention is paid to hardware parts and their connection with firmware. However, the topic of software that runs in local SEG deserves separate deliberation.

We can distinguish different types of software in local SEG according to device that it runs on:

1. Firmware (embedded devices).
2. Software for microcomputers.
3. Software for user devices (smart phones, PC, etc.).

Cloud applications software stands out of these types but still it can directly communicate with all abovementioned software types. Firmware has an access to the hardware on the lowest level. Firmware mainly is responsible for reading and writing data from and to external devices. At the same time, business logic functions appear rarely on this level of software due to the device limitations. Considering the whole scope of the IoT for SEG, firmware includes the least amount of business logic. Although, it is still important part of the system and all the other levels rely on the firmware.

Development of firmware is performed in specialized integrated development environments (IDE) like Keil, SystemWorkbench for STM32, etc. Such environments contain rich toolset and they make many helpful functions to speed up development process (e.g. library connection, simple build procedure). Usually, they contain all necessary files or are aware how to download them to target machine automatically. However, among well-known IDEs, there is one that worth mentioning. It is online-IDE mbed. Actually, it is more than just IDE, it is fully featured development platform. It provides access to the code editor with all connected libraries according to the selected device. The set of supported device is impressive in mbed. mbed offers Arduino-like approach for the beginners. However, at the same time, experienced developers retrieve full control over design process and can rely on both high-level classes and libraries for specific devices. Beyond the software that is intended to be used directly for microcontrollers, mbed proposes great amount of classes that represent external objects connected to microcontrollers (sensors, mechanical parts, electrical parts, etc.). They can be easily imported into any project without reference to board or microcontroller that project is configured for. mbed employs separate layer of hardware abstraction that unifies access to the resources for every supported device.

Mbed supports unobtrusive workflow for developer when minimal set of software is installed directly on developer's machine. Cloud

infrastructure maintains all the software that is needed for development. Compilation of project in mbed results in binary output file that represents program for microcontroller. Browser download file to the developer machine. Boards that contains mbed-enabled bootloader can be programmed using simple copy-and-paste procedure as during their connection to PC they are identified as mass-storage device with appropriate amount of memory that matches amount of Flash-memory in the device. Modules that do not support this technology are programmed by separate programming utility that usually consumes much less disk space than whole IDE.

33.4 Work related analysis

IoT infrastructure for Smart Energy Grid based on Embedded Systems devices are considered in different university-partners, besides University of Coimbra, Leeds Beckett University, Consiglio Nazionale delle Recerche - Istituto di Scienza e Technologie dell' Informazione "A.Faedo" (ISTI-CNR), Royal Institute of Technology (KTH) and Newcastle University. So, let's consider the following projects.

Cyber-physical system (CPS) is a notion for the advanced information system where objects of physical world obtain intellectual properties by leveraging modern computation means that integrated into the objects. CPS and IoT are closely related and emerged in scientific researches almost at the same time. However, CPS is mentioned as more complex model that can use IoT as fundament for further development.

Speaking in general, CPS is more specific and problem-oriented than IoT. CPS development is dedicated to peculiar context (social processes, health, energy consumption, technological processes, etc.). Context groups several problems and its own domain in case of CPS. Context-Awareness of CPS leads it to possibility of automation of much larger problem area than IoT. Physical world is characterized by its complexity, numerous interdependencies in each natural or social scope. Even the most progressive CPSs with closest mapping to real world assume some simplifications to cover single problem. However, the future of IoT supposes movements towards integration with CPSs. The aim of this convergence is to solve tasks that are more complex for

IoT and to combine several contexts with intention to form new powerful intellectual system that spreads across multiple domains problem. Integration of CPSs into SEG scope allows increasing complexity of the system and automate more functions of SEG. Presumably, all control, measurement, analysis, reaction assignments might be performed automatically in the future [13].

Gradual penetration of CPSs in all fields of human activity and more and more applications found for their components. In the final stage of development, CPSs will be the main mechanism for automating production sphere. For now, we can observe appliance of their components in specific production assets management [14]. In the mentioned work, WSN has been complemented by modern wireless technologies (SmartMesh). Consequently, existing production infrastructure has been updated to the requirements of continuous information supply and online assets monitoring.

In the context of IoT for local SEG, CPSs have extremely wide sphere of employment. Customers' demands for quality of service are constantly getting higher and ordinary control and observation over the energy commodities in premises are not enough. Even though, Smart Building systems propose additionally automation according to customer preferences (personal schedule, historical analysis of previous actions, etc.) with different automation modes of work for the system, customers want to obtain more from their energy infrastructure. Harvesting energy from the renewable and clean resources, frugal consumption of energy, longevity of local energy assets will be in focus of production companies and researches with further development of IoT, CPS, and their structural elements.

As IoT, CPS, and cloud technologies are getting more and more popular, borders among different information systems become more and vaguer. Customer can get access to almost any service online. Online-services retrieve personal data of customers and they are granted access to control their assets. That raises problems of security of private data and premises in case of a breach in one of the system layers. IoT-devices with low computation resources are the first candidate for possible attacks. Additionally, attacks on wireless modules are one of the simplest, as they even do not require direct physical intrusion into the system. Modern IoT-devices contain basic

security functions that are necessary to activate and configure properly during deployment of the system. Despite the fact that it can affect productivity of the system, security gains worth shortage of some computational power. As communications in local SEG are performed mainly with short messages with long period, actual effect of this configuration will not be significant. Moreover, as it is shown in the paper [15], modules with hardware support of security functions cope with additional computations with low time expenses. For the mentioned purpose, all communications among network devices in local SEG should be performed only with encrypted messages (plain-text information should be avoided). Some devices support it automatically, other ones should be configured appropriately. Configuration is usually set in firmware and several control bits should be set. In some cases, configuration may be fully programmable. This type of configuration must be thoroughly verified to prevent possible negative consequences.

Conclusions and questions

In this section, the materials for module ITMM 1.2 of MSc course “IoT for Smart Energy Grid” are presented. They can be used for preparation to lectures and self-learning. Analysis of local SEG, its components, architecture, and hardware backbone of the local SEG are the main topics of this section. The local SEG part of the bigger grid has its own peculiarities and, thus, requires considerations of issues concerned with its work. Local SEG has quite complex architecture that is comprised of devices integrated into single network. Network technologies are tightly cohensed in this segment of grid and suppose sophisticated communication among devices inside the network. All of them are thoroughly reviewed in this section as well as network nodes (sensor, control) inside the network.

In order to better understand and assimilate the educational material that is presented in this section, we invite you to answer the following questions.

1. What does PLC stand for?
 - a) Power-Line Communication
 - b) Proto-Layer Controller
- c) Photo-Liquid Compound
- d) Public Local Consumption
2. What is the name of described cloud developed platform?
 - a) CDP
 - b) mbed
 - c) dev-cloud
 - d) seg-dev
3. MQTT protocol has ... format.
 - a) XML
 - b) JSON
 - c) binary
 - d) encoded
4. CoAP is ...-based protocol.
 - a) TCP
 - b) ICMP
 - c) IGMP
 - d) UDP
5. WiFi-module considered in this section is entitled ...
 - a) ESP8266
 - b) BT345
 - c) Murata
 - d) Huawei
6. The most wide-spread mini-computer is ...
 - a) Odroid
 - b) Raspberry Pi
 - c) Cubieboard
 - d) Orange Pi
7. Configuration manager for STM microcontrollers is
 - a) Visual Studio
 - b) CodeBlocks
 - c) STM32CubeMX
 - d) mbed
8. What consumption mode does not exist for microcontroller?
 - a) RUN
 - b) SLEEP
 - c) STEADY
 - d) REPAIR
9. What order of magnitude of consumption is typical for STEADY state?
 - a) uA
 - b) dozens of uA
 - c) hundreds of uA
 - d) mA
10. 6LoWPAN technology uses address scheme that is based on ... protocol.
 - a) IPv4
 - b) IPv6
 - c) TCP
 - d) UDP
11. The main concern of cloud platforms for local SEG is ...
 - a) Accessibility
 - b) Cost
 - c) Security
 - d) Availability
12. What is not an option for writing programs for ESP8266?
 - a) HAL
 - b) Arduino
 - c) Interpreter-based
 - d) Enterprise Java
13. What state of STM microcontroller provides the lowest energy consumption?
 - a) STEADY
 - b) RUN
 - c) SLEEP
 - d) LOW RUN
14. AMI stands for ...
 - a) Application Meter Interface
 - b) Advanced Metering Infrastructure
 - c) Ascending Measurement of Internet
 - d) Access Mocking Instability
15. CoAP has ... format.
 - a) XML
 - b) JSON
 - c) binary
 - d) encoded

References

1. Y. Saleem, N. Crespi, M. H. Rehmani, and R. Copeland, "Internet of Things-aided Smart Grid: Technologies, Architectures, Applications, Prototypes, and Future Research Directions," *IEEE Access*, 2019, pp. 62962-63003. DOI: 10.1109/ACCESS.2019.2913984
2. J. Pan, R. Jain, S. Paul, T. Vu, A. Saifullah, and M. Sha, "An Internet of Things Framework for Smart Energy in Buildings: Designs, Prototype, and Experiments," in *IEEE Internet of Things Journal*, no. 2, 2015, pp. 527-537.
3. G. Fortino, C. Savaglio, C. E. Palau, J. S. de Puga, M. Ganzha, M. Paprzycki, M. Montesinos, A. Liotta, and M. Llop, "Towards Multi-layer Interoperability of Heterogeneous IoT Platforms: The INTER-IoT Approach," in *Integration, Interconnection, and Interoperability of IoT Systems*, 2018, pp. 199-232.
4. N. M. Masoodhu Banu and C. Sujatha, "IoT Architecture a Comparative Study," in *International Journal of Pure and Applied Mathematics*, vol. 107, no. 8, 2017, pp. 45-49.
5. L. R. Hua, Z. Junguo, and L. Fantao, "Internet of Things Technology and its Applications in Smart Grid," in *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 12, no. 2, 2013, pp. 940-946.
6. V. Tiwari, A. Keskar, and N. C. Shivaprakash, "A Reconfigurable IoT Architecture with Energy Efficient Event-Based Data Traffic Reduction Scheme," in *International Journal of Online Engineering*, vol. 13, no. 2, 2017, pp. 34-52.
7. S. Galli and L. Thierry, *Next Generation Narrowband (Under 500 kHz) Power Line Communications (PLC) Standards*, G3-PLC Alliance, 2015.
8. L. Berger, S. Andreas, and E. Joaquin, "Power Line Communications for Smart Grid Applications," in *Journal of Electrical and Computer Engineering*, vol. 2013, 2013, pp. 1-16.
9. L. Schibuola, M. Scarpa, and C. Tambani, "Intelligent Buildings Connected To Future Smart Energy Grids," in *WIT Transactions on The Built Environment*, vol. 142, 2014, pp. 255-266.
10. N. Angelis, N. Archontos, D. Vouyioukas, N. Nomikos, and C. Skianis, "An integrated NAN architecture for smart energy grid," *IEEE International Energy Conference (ENERGYCON)*, pp. 123-128, June 2018.
11. U.S. Department of Energy, "Advanced Metering Infrastructure and Customer Systems", 2016.
12. D. Ma, G. Lan, W. Xu, M. Hassan, and W. Hu, "SEHS: Simultaneous Energy Harvesting and Sensing Using Piezoelectric Energy Harvester," *2018 IEEE/ACM Third International Conference on Internet-of-Things Design and Implementation (IoTDI)*, pp. 201-212, April 2018.

13. J. Leitaó, P. Gil, B. Ribeiro, and A. Cardoso, "Adaptive Supervisory Framework for Cyber-Physical Systems," in *CISUC TECHNICAL REPORT*, 2018, pp. 1-9.

14. N. Huynh, V. Robu, D. Flynn, S. Rowland, and G. Coapes, "Design and demonstration of a wireless sensor network platform for substation asset management," in *CIREN - Open Access Proceedings Journal*, vol. 2017, no. 1, 2017, pp. 105-108.

15. S. Raza, T. Helgason, P. Papadimitratos, and T. Voigt, "SecureSense: End-to-end secure communication architecture for the cloud-connected Internet of Things," in *Future Generation Computer Systems*, vol. 77, 2017, pp. 40-51.

34. AVAILABILITY ASSESSMENT OF IOT BASED IT INFRASTRUCTURE OF POWER GRIDS

Prof., DrS E.V. Brezhniev,
Assoc. Prof., Dr. M. O. Kolisnyk (KhAI)

Contents

Abbreviations	84
34.1 Reliability assessment of IoT based IT infrastructure	85
34.1.1 Smart grid and I&C development trend's analysis	85
34.1.2 Analysis of failures	86
34.1.3 Models of reliability	92
34.2 IoT based predictive diagnostics and maintenance of power grid equipment	100
34.2.1 Principles of IoT based predictive analytics, diagnostics and maintenance	101
34.2.2 Tools for predictive diagnostics and maintenance for predictive diagnostics	107
34.2.3 Reliability and cyber-security issues for predictive analytics software based systems. Cases	109
34.3 Availability assessment of IoT based IT infrastructure	111
34.3.1 Availability models	111
34.3.2 Research of models	113
34.3.3 Tools and techniques	118
34.3.4 Assessment cases	120
34.4 Work related analysis	123
Conclusions and questions	124
References	125

Abbreviations

AI – Artificial Intelligence
ATHENA – Technique for Human Event Analysis
BBN - Bayesian Networks
BEMS – Building Energy Management System
CMF – Common Mode Failure
CCF – Common Cause Failure
CF – Cascading Failure
CMMS – Computerized Maintenance Management Systems
CPT – Conditional Probability Table
CREAM – Cognitive Reliability and Error Analysis Method
CRM – Customer Relations Management
DBBN – Dynamic Bayesian Networks
DNNs – Deep Learning Neural Networks
ERP – Enterprise Resource Planning
FMECA – Failure Mode, Effects and Criticality Analysis
GERT – Graphic Evaluation and Review Technique
HAZOP - Hazard and Operability
HCR – Human Cognitive Reliability
HEART – Human Error Assessment and Reduction Technique
LV – Linguistic Values
MPP – Massively Parallel Programming
MRO – Maintenance, Repair and Operations
NPTA – Non-Productive Time Availability
OATS – Operators Action Trees
ORE – Operators Reliability Experiments
PdM – Predictive Maintenance
ROI – Return on Investment
PIM – Processing in Memory
SBC – Smart Business Centre
SG – Smart Grid
SLIM – Success Likelihood Index Method
SMART – Self Monitoring Analysis and Reporting Technology
TESEO – Empirical Technique to Estimate Operator Errors
THERP - Technique for Human Error Rate and Prediction

34.1 Reliability assessment of IoT based IT infrastructure

34.1.1 Smart grid and I&C development trend's analysis

The Smart Grid (SG) is a movement to bring the electrical power grid up to date so it can meet current and future requirements to fit customer needs. Updating the electrical power grid could introduce new security vulnerabilities into the system. The SG is an upgrade to the current electrical power system, so it has all the functionality of our current power system plus several new functionalities such as: self-healing, motivating and including the consumer, attack resistance, power quality increase, all generation and storage options accommodation, electrical markets enabling, assets optimization and efficiently operating.

This is already being realized in the real world through the Internet of Things (IoT) technology. IoT is a network of physical objects or things connected to the Internet. Such objects are equipped with embedded technology to interact with their internal and external environments. These objects sense, analyze, control and decide individually or in collaboration with other objects through high speed and two-way digital communications in a distributed, autonomous and ubiquitous manner. IoT technology can help SGs by supporting various network functions throughout the power generation, storage, transmission, distribution and consumption by incorporating IoT devices (such as sensors, actuators and smart meters), as well as by providing connectivity, automation and tracking for such devices.

Information from [1-10] was analyzed. There are following development trends in SG and I&C that are supported by IoT such as:

- ***Implementation of Open Protocols***: Open industry standard protocols are replacing vendor-specific proprietary communication protocols.

- ***Interconnected to Other Systems***: Connections to business and administrative networks to obtain productivity improvements and mandated open access information sharing.

- ***Reliance on Public Information Systems***: Increasing use of internet and public telecommunication systems the for portions of the control system, etc.

The SG always needs to be available, and locking the system during an emergency could cause safety issues and security issues.

The SG security objectives are confidentiality, integrity and availability. In most industries confidentiality and integrity have higher precedence over availability. In the electrical power system, electricity must always be available, so this is the most important security objective. Integrity is the next important security objective followed by confidentiality. Availability is the most important security objective.

Integrity is the next important security objective in the SG. The SG uses data collected by various sensors and agents. This data is used to monitor the current state of the electrical power system. Unauthorized modification of the data, or insertion of data from unknown sources can cause failures or damage in the electrical power system. The electricity in the power grid not only needs to always be available, but it also has to have quality. The quality of the electrical power will be dependent on the quality of the current state estimation in the power system.

One of the main concerns for SG is the connectivity, automation and tracking of large number of devices, which requires distributing monitoring, analysis and control through high speed, ubiquitous and two-way digital communications. It requires distributing automation of SG for such devices or “things”.

34.1.2 Analysis of failures

NPP is part of sustainable energy so this is also the future part of SG. The Instrumentation and Control (I&C) systems play a crucial role in the operation of NPP and other SG power generation plants. The main objective of I&C systems is to ensure safety, availability and performance of the generation plant. The SG safety means the achievement of proper operating conditions, prevention of accidents or mitigation of accident consequences, resulting in protection public and environment from undue radiation hazards.

The I&C's failures data analysis proves that multiple failures (MFs) are significant contributors to the I&C incidents. The multiple failures cause the diesel-generator's trip, the malfunctions of the reactor trip breakers, the motor-operated valves, the pumps, etc.

The MFs of the I&C combined with operator's errors could cause the significant accident in the nuclear power generating industry, resulting in the release of radioactive gases. The MFs might be classified on dependent and independent failures. The independent multiple failures are simultaneous (or in short time interval) failures caused by different specified reasons. The multiple dependent failures consist of common cause and cascading failures. The common mode failures (CMFs) are a subset of common cause failures (CCFs). The cascading failures (CFs) are considered as a sequence of dependent failures of individual components that successively weakens the I&C. The cascading failures occur when the I&C's basic design principles are violated. The cascading of component states is normally due to functional dependencies. Such functional dependencies are modeled in systems models without the need for common cause events models. The component failure caused by other component failure isn't attached to common cause failures. The multiple failures classification is shown in Fig.34.1.

Common cause failures (CCFs)

The SG power plants' operational experience proves CCFs are a subset of multiple failures and main contributors to the accident risk's increase. The CCFs are an important class of dependent events with respect to their contribution to the I&C unavailability. This is important for redundant or diverse systems. The failure of multiple components due to a common cause represents one of the most important issues in evaluation of the I&C reliability or unavailability. The frequency of such events has relatively low expectancy compared to random failures, which affect individual components. But in many cases the consequence of CCFs is a direct loss of safety or mitigation safety function.

The I&C failure statistics demonstrates that CCF contributes up to 29% of total amount of dependent failures. The CCFs are difficult to quantify correctly, i.e. it is difficult to know if a component fails due to a common root cause that affects several components, or if it fails because it is old and worn out.

In general, I&C CCFs are characterized by the following features:

1. Two or more similar components have failed or are degraded. The failures occurred on demand, during testing.

2. The failures share a single cause and are linked by a coupling factor. The condition or mechanism through which failures of multiple components are coupled is termed as the coupling factor. The coupling factor is a characteristic of a group of components that identifies them as susceptible to the same causal mechanism of failures.

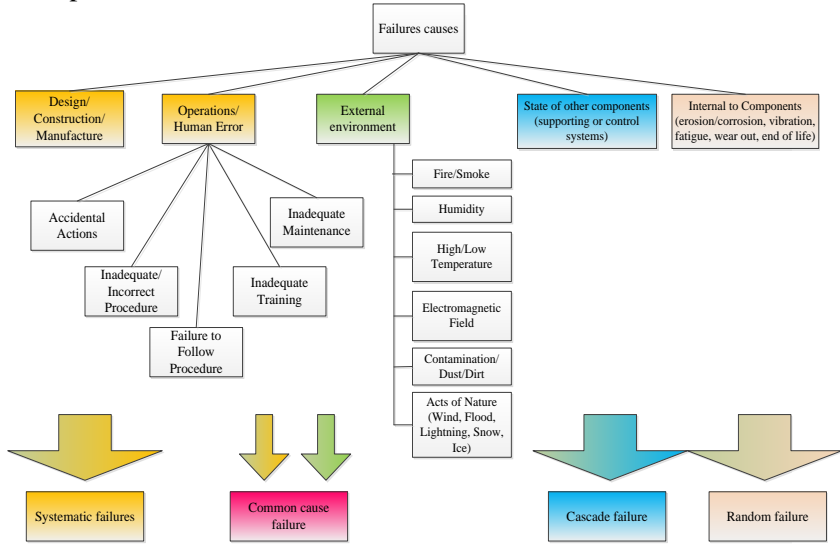


Fig. 34.1 - The Failure Causes

3. The equipment failures are not caused by the failure of equipment outside the established component boundary. These failures are dependent but are not CCF events.

4. The conditions which cause CCF have to affect multiple components simultaneously. Simultaneity, in this context, refers to failures that occur close enough in time to lead to the inability of multiple components to perform their intended function.

Classification of coupling factors stipulating CCFs in I&C

As described earlier, for failures to originate from the same cause and be classified as a CCF, the conditions for the trigger or conditioning events have to affect multiple components simultaneously. Simultaneity, in this context refers to failures that occur close enough in time to lead

to the inability of multiple components to perform their intended safety function for a PRA mission. As mentioned, the condition or mechanism through which failures of multiple components are coupled is termed the coupling factor.

During all of its life cycle the I&C system is affected by set of factors which stipulate the couplings among its components and subsystems. The coupling factors classification consists of five major classes:

- Design based;
- Manufactory (quality) based;
- Operation based;
- Maintenance based;
- Environment based.

A. Design based factors

The design coupling factors result from common characteristics among components determined at the hardware design level. There are two groups of design-related hardware couplings: system level and component level. System-level coupling factors include features of the system or groups of components external to the components that can cause propagation of failures to multiple components. Component level coupling factors represent features within the boundary of each component.

The following are coupling factors in the design category:

- ***System Layout/Configuration***. Refers to the arrangement of components to form a system;
- ***Component Internal Parts***. Refers to characteristics that could lead to several components failing because of the failure of similar internal parts or subcomponents. This category is used when investigating the root cause of component failures and when the investigation is limited to identifying the sub-components or piece-part at fault, rather than the root cause of failure of the piece- part.

B. Manufactory (quality) based factors

The quality coupling factors refer to characteristics introduced as common elements for the quality of the hardware and include the following:

- ***Manufacturing Attributes***. Refers to the same manufacturing staff, quality control procedure, manufacturing method, and material;

– **Construction/Installation Attributes** (both initial and later modifications). Refers to the same construction/installation staff construction/installation procedure, construction/installation testing/verification procedure, and construction/installation schedule. Inadequacy of procedures mentioned might result to multiple failures in I&C system.

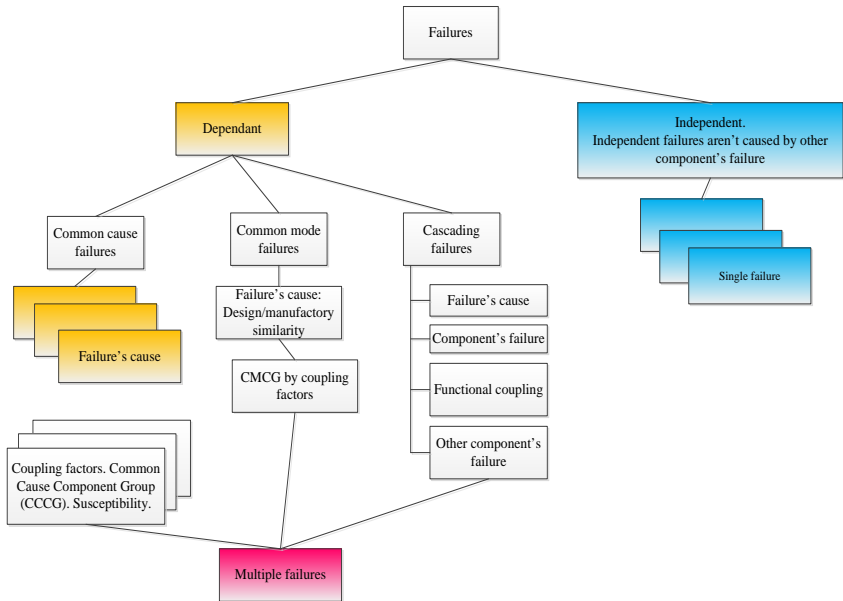


Fig. 34.2 - The Failure Classification

C. Maintenance based factors

The maintenance based coupling factors propagate a failure mechanism from identical maintenance program characteristics among several components. The categories of maintenance based coupling factors are:

– **Maintenance/Test/Calibration Schedule.** Refers to the maintenance/test/calibration activities on multiple components being performed simultaneously or sequentially during the same event. Thus, a number of breakers in the AC power system failed to close due to dirt and foreign material accumulation in breaker relays. Existing

maintenance and testing requirements allowed the relays to be inoperable and not detected as inoperable until the breakers were called on to operate. The maintenance requirements or cleaning schedules had not been established or identified as being necessary;

– **Maintenance/Test/Calibration Procedures.** Refers to propagation of errors through procedural errors and operator interpretation of procedural steps. It is recognized that for non-diverse equipment, it is impractical to develop and implement diverse procedures;

– **Maintenance/Test/Calibration Staff.** Refers to the same maintenance/test/calibration team being in charge of maintaining multiple systems/components.

D. Operation based factors

The operation based coupling factors propagate a failure mechanism from identical operational characteristics among several components. The categories of operation based coupling factors are:

– **Operating Procedure.** It refers to the cases when operation of all (functionally or physically) identical components is governed by the same operating procedures. Consequently, any deficiency in the procedures could affect these components as shown in the first example. Sometimes, a set of procedures or a combination of procedure and human action act as the proximate cause and coupling factor, as seen in the second example. In other cases, a common procedure results in failure or multiple failures of multiple trains as demonstrated by the third example. For example, two pumps failed to develop the proper flow output. It was determined that the manual governor speed control knobs had been placed in the wrong position because of an error in the procedure.

– **Operating Staff.** Refers to the events that result if the same operator (team of operators) is assigned to operate all trains of a system, increasing the probability that operator errors will affect multiple components simultaneously.

Example: All the emergency service water pumps were found in the tripped condition. The trips were the result of an emergency engine shutdown device being tripped. The operations personnel did not recognize that the trip devices had to be reset following testing. The

procedures were enhanced to include information that is more detailed and the operator training was enhanced on operating the trip devices.

E. Environment based factors

The environment based coupling factors propagate a failure mechanism via identical external or internal environmental characteristic. These coupling factors are:

- **External environment.** Refers to all redundant systems (components) exposed to the same external environmental stresses (flood, fire, high humidity and earthquake);

- **Internal environment.** Refers to commonality of multiple components in terms of the medium of their operation such as internal fluids (water, lube oil, gas, etc.) As example, three water pumps failed because of high pump vibration. The ocean is the suction source for pumps, and the failures were caused by excessive quantities of abrasive particles in the water.

Hereby the I&C systems are affected by the set of coupling factors during all life cycle. The factors' impacts can't be avoided because of factors' permanency. They are inherent part of evolutionary progress of any complex system. The only approach here is to control them in purpose to reduce their influence on the I&C. The multiple failures' risk is right along. So we need to develop and implement the strategies of failure management and models for I&C reliability assessment to make the I&C system capable to provide the services, though possibly alternated or degraded in the face of various type of failures and disruption.

34.1.3 Models of reliability

SG reliability describes the overall ability of the SG to perform its function.

In general, reliability analysis can be performed either analytically or numerically, while this overview only treats analytical methods. In analytical methods, the system is represented by mathematical models, which are typically based on reliability models (as an example, Markov). The expectation values of reliability indices are calculated by solving an equation system. The most common numerical method is the Monte Carlo simulation method. In this method, random behavior of the

system is analyzed through simulation of physical relationships. The outcome of a Monte Carlo simulation is the expectation value probability distributions of reliability indices, i.e. not only the average values as in analytical methods. The method offers the possibility to apply more sophisticated component models, e.g. including effects of component aging. However, this leads to increased computation time, why Markov models are also often used here.

Reliability studies are conducted for two purposes. First, long-term evaluations are performed to assist in system planning. Secondly, short-term evaluations assist in day to day operating decisions.

The SG reliability is the complex property that determines the ability to perform power supply to consumers by performing functions in the production, transmission and distribution of electrical energy under a single technological interaction between generating installations, electrical networks and electrical installations of consumers at any given time, the demand for power and electricity (adequacy, balance component of system reliability) to withstand perturbations caused by failures from the grid elements (safety, system reliability, operational component).

Particular reliability indicators include:

- **Failure flow parameter**: ratio of the number of unrecorded elements of time to the total number of test items of the same type, provided that the failed elements are replaced by new ones;
- **Failure rate**: average value of time between successive failures;
- **Recovery time**: ratio of the total time of recovery of the technical device for the selected calendar time to the number of its failures for the same calendar period;
- **Readiness ratio**: ratio of the failure time of the technical device to the total time of its failure-free operation and forced downtime due to failures.

Typical reliability indices used in SG systems evaluation are the following:

- **Load interruption indices**: average load interrupted per period.
- **Loss of load probability**: probability of load exceeding available generation.
- **Frequency and duration indices**: average number of occurrences and duration of interruptions per time period.

Application of Markov Model for reliability assessment

If a large system is subject to assessment, the applied model easily can become impossible to handle if components are modelled in detail. The Markov model gives a simple description of a component, which can be handled well with mathematical methods. In order to be able to utilize the techniques the components of the system must be able to be described as a Markov model. This means that the system should be represented as a system lacking memory of previous states with identifiable system states. Markov models can be represented either as discrete or continuous models, both in time and space. In power system reliability assessment it is common to use stationary Markov models which are discrete in space while continuous in time. Implying that the components are modelled in steady state in a continuous time space, where transitions between discrete states occur at constant transition rates.

The Markov process method considers the functioning of a CI as a random process. It takes into account both the impact of independent component failures and the intensity of the transition between states under the influence of various factors that cannot be taken into account in analytical models for simple systems. For this reason, the Markov method is used to assess the reliability of functionally complex systems with complex repair and maintenance strategies.

Application of Bayesian Networks (BBN) for SG reliability assessment

A classical BBN is a pair $N = \{V, E, P\}$ where V and E are the nodes and the edges of a Directed Acyclic Graph (DAG), respectively, and P is a probability distribution over V . Discrete random variables $V = \{X_1, X_2, \dots, X_n\}$ are assigned to the nodes while the edges E represent the causal probabilistic relationship among the nodes. Each node in the network is annotated with a Conditional Probability Table (CPT) that represents the conditional probability of the variable given the values of its parents in the graph. The CPT contains, for each possible value of the variable associated to a node, all the conditional probabilities with respect to all the combinations of values of the variables associated with the parent nodes. For nodes that have no parents, the corresponding table will simply contain the prior probabilities for that variable.

The principles behind BBN are Bayesian statistics and concentrate on how probabilities are affected by both prior and posterior knowledge. In order to extend the classic BBN into fuzzy BBN which is capable of dealing with linguistic variables, fuzzy numbers and their operations must be used.

Fragment of linguistic CPT is shown in the table 34.1.

Table 34.1 - Fragment of CPT

S ₁			S ₂			S ₃	
Criticality			Criticality			Criticality	
H	M	L	H	M	L	H	...
+			+			P(Crt(S ₃)=H/Crt(S ₁)=H, Crt(S ₂)=H)= <i>High</i>	...
+				+		P(Crt(S ₃)=H/Crt(S ₁)=H, Crt(S ₂)=M)= <i>Low</i>	...
					
	+		+			P(Crt(S ₃)=H/Crt(S ₁)=M, Crt(S ₂)=H)= <i>Low</i>	...

The probability of S₃, being at one of the established state Ω_{S3} depending on the states of parents nodes, could be determined as:

$$P(S_3^{(k)}) = \sum_i \sum_j P(S_3^{(k)} / S_1^{(i)}, S_2^{(j)}) * P(S_1^{(i)}) * P(S_2^{(j)}),$$

where P(S₃^(k)) – a probability for S₃ being at k-th state; P(S₃^(k) / S₁⁽ⁱ⁾, S₂^(j)) – a conditional probability for SG system S₃ to be at k-th state, provided system S₁ being at i th state and system S₂ being at j – th state; P(S₁⁽ⁱ⁾) – probability for S₁ being at i-th state determined by expert, taking into account value (34.1); P(S₂^(j)) – probability for S₂ being at j-th state determined by expert, taking into account value (34.1).

Empirical frequencies, subjective estimates of “expectations” and theoretical ideas about the mathematical probabilities of various consequences of a priori information can be used in BBN. This is an important practical advantage and distinguishes the BBN from other approaches in assessing the safety and reliability of SGs.

Analysis of publications shows a tendency to increase the use of BBN for solving evaluating safety and reliability problems. According to the journal (Reliability Engineering and System Safety) for the period 1999-2015, there has been an increase of 100% of publications based on the use of BBN for the reliability and safety assessment tasks analysis.

The percentage of BBN application for the reliability, assurance and risk analysis is shown in Fig.34.3.

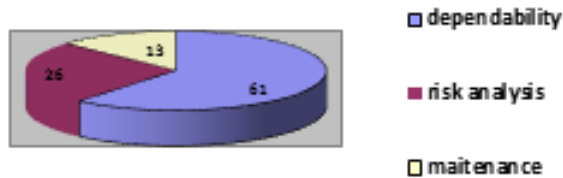


Fig. 34.3 - Percentage ratio of BBN usage for the tasks of reliability analysis, dependability and risk analysis

Any SG can be represented as a graph, where the nodes are systems and the edges describe the existing interaction between them. The idea of the nature of interdependencies, cause-effect relationships between nodes lays in fact that systems are not static. In the tasks of evaluating the safety and reliability of SG, it is necessary to take into account the state of all systems, external environment, the influence of the human factor. This leads to the fact that not only technical and software components, the human operator, but also various external factors (of natural and man-made nature) become nodes of the BBN.

Conducting a periodic safety and reliability analysis of the SG allows determining the existence of hazardous conditions that could significantly reduce system safety and reliability margins. In this case it is recommended to conduct a comprehensive verification of the possibility of consequences of high severity levels.

Static (classical) BBNs do not allow to model dynamic of SG systems. The disadvantages of static BBN include:

- the CPT invariance. CPT represents an estimate of the interaction between the systems degree. The influence between the states of systems degree varies during their performance. This leads to

the needs of specifying the BBN parameters in the safety and reliability of SG analysis;

- taking into account large number of interference types between the SG systems, the same node can be either a node parent or a node descendant;

- arcs representing the interaction between nodes can also be dynamic, that is, they can appear, disappear and change directions.

The advantages of Dynamical BBN (DBBN) for SG safety and reliability assessment are:

- Nonlinearity. Through a tabular representation of conditional probabilities, Dynamical BBN is able to describe any nonlinear phenomenon (problem);

- Interpretability. Each network variable represents a specific physical phenomenon for the process being described;

- Factorization. Using a joint probability distribution leads to statistical efficiency – fewer parameters are required.

- Computational efficiency – DBBN allows to reduce the number of model parameters without reducing its accuracy;

- DBBN has clear probabilistic semantics.

In general, DBBN can be represented as $D=(X, U, Y)$, where X , U and Y are sets of stochastic random variables that respectively determine system state variables, input (control) effects for the system and system response to them.

Another feature of DBBN is that the values of a number of variables can be obtained indirectly through the values of other variables, the calculation or observation of which is a simpler task.

Dynamic BBNs are an extension of the classic BBNs allowing to model the behavior of dynamic systems. DBBN is the composition of several static BBN defined at each time interval (cut), t_i .

To simplify the reliability modeling using DBBN allowed:

- DBBN has the Markov property of the first order. In other words, the state of nodes in the network at time t is determined only by the previous state of nodes at time $t-1$;

- the structure (nodes and relations), as well as parameters (conditional and a priori probabilities), is unchanged.

Thus, for DBBN, the state of the system in a given time interval can be determined by the state of this or other systems from the previous interval.

DBBN can be defined as a pair (B_1, B_{\rightarrow}) , where B_1 is BBN, which defines a priori network $P(Z_1)$; B_{\rightarrow} - a two-interval temporary BBN (2TBN) which determines $P(Z_t / Z_{t-1})$ by means of a directed acyclic graph of the form, i.e. state change model

$$P(Z_t / Z_{t-1}) = \prod_{i=1}^N P(Z_t^i / Pa(Z_t^i))$$

where Z_t^i is the i -th node at time t , $Pa(Z_t^i)$ is the set of parents of the Z_t^i node. Nodes in the first time interval 2TBN do not have parameters associated with them; each node in the second interval is described by a conditional probabilities table (CPT), which defines $P(Z_t^i / Pa(Z_t^i))$ for all $t > 1$.

DBBN can be described using the probability distribution function on a sequence of T variables with hidden states $Y = \{y_0, y_1, \dots, y_{T-1}\}$ and a sequence T of observed variables $X = \{x_0, x_1, \dots, x_{T-1}\}$ where T is the time interval (slice) for evaluation. The time interval changes when a new certificate enters the network.

$$P(Z_{1:T}^{1:N}) = \prod_{i=1}^N P_{B_1}(Z_1^{(i)} / Pa(Z_1^{(i)})) \times \prod_{t=2}^T \prod_{i=2}^N P_{B_{\rightarrow}}(Z_t^{(i)} / Pa(Z_t^{(i)}))$$

The model of state changes and observations can be represented as a product of the distribution of conditional probabilities of the form

$$P(X_t / X_{t-1}) = \prod_{i=1}^N P(X_t^{(i)} / Pa(X_t^{(i)})).$$

DBBN can be represented as

$$P(X, Y) = \prod_{t=1}^{T-1} P(x_t | x_{t-1}) \prod_{t=0}^{T-1} P(y_t | x_t) P(x_0)$$

In order to fully describe DBBN, one must specify the following parameters:

- probability distribution function describing the change of states. Describes the time dependencies between the states $P(Q_t|Q_{t-1})$ or $P(Q_t|Q_{t-1}, U_{t-1})$ (taking into account the U_t control signals).

- the probability distribution function $P(Y_t|Q_t)$ of observations (observation model), which determines the dependencies between the observed parameters and the rest of the network parameters in a given time interval.

- probability distribution of the initial state of the nodes $P(x_0)$.

The joint distribution of values at the vertices (observable and hidden) shown in the figure has the form:

$$\begin{aligned}
 P(S_1^{1:T}, S_2^{1:T}, S_3^{1:T}, y_{i,j}^{1:T}) &= P(S_1^1) \times P(S_2^1) \times P(S_3^1 / S_1^1, S_2^1) \times \\
 &P(y_{1,1}^1 / S_1^1) \times P(y_{1,2}^1 / S_2^1) \times \\
 &\times P(y_{1,3}^1 / S_3^1) \times \prod_{j=2}^N P(S_1^j / S_1^{j-1}) \times P(S_2^j / S_2^{j-1}) \times \\
 &\times P(S_3^j / S_1^j, S_2^j, S_3^{j-1}) \times \prod_{i=2}^K P(y_{j,i}^j / S_i^j)
 \end{aligned}$$

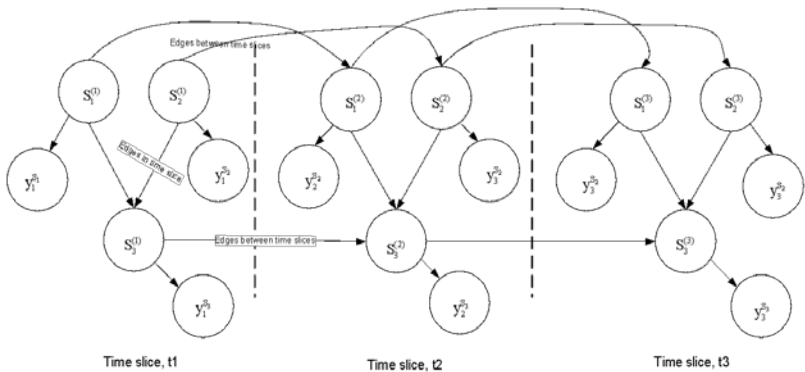


Fig. 34.4 – The DBBN generic

Examples of application of these models (techniques, tools and cases) are described in the practicum book.

34.2 IoT based predictive diagnostics and maintenance of power grid equipment

Predictive maintenance (PdM) is maintenance that monitors the performance and condition of equipment during normal operation to reduce the likelihood of failures. Also known as condition-based maintenance, predictive maintenance has been utilized in the industrial world since the 1990s. In information technology (IT), a neural network is a system of hardware and/or software patterned after the operation of neurons in the human brain. Neural networks - also called *artificial neural networks* - are a variety of deep learning technology, which also falls under the umbrella of artificial intelligence, or AI [11].

Predicting when equipment or individual components will fail benefits asset insurers, as well as manufacturers. In predictive maintenance, sensors and smart cameras gather a continuous stream of data from machines, like temperature and pressure. The quantity and varied formats of real-time data generated make machine learning an inseparable component of IIoT. Over time, the algorithms can predict a failure before it occurs. Dropping costs of industrial sensors, advances in machine learning algorithms, and a push towards edge computing have made predictive maintenance more widely available.

Deals to AI companies focused on industrials and energy, which includes ML-as-a-service platforms for IIoT, are rising. Predictive maintenance (PdM) does not just pertain to the manufacturing, rail, and oil and gas industries. In other applications, PdM is used to:

- help prevent utility outages with the help of drones and sensors that map utility networks;
- detect a temperature decline in a steam pipeline, indicating a potential pressure leak; capture increased temperatures in electrical panels to prevent component failures;
- measure supply-side and demand-side power at a common coupling point for monitoring power consumption;
- locate overloads in electrical panels;

- identify motor amperage spikes or overheating from bad bearings or insulation breakdowns;
- find three-phase power imbalances from harmonic distortion, overloads, degradation or failure of one or more phases.

34.2.1 Principles of IoT based predictive analytics, diagnostics and maintenance

Implementing predictive maintenance requires a significant investment in money, personnel and education. While these initial investments might seem daunting to an organization, predictive maintenance's return on investment (ROI) far outweighs any upfront costs. The software is basically an event-driven data pool, which pools data from various sources through databases and ERP systems to facilitate integrated processing and management, thereby enabling digital images of different physical or logical objects to interact. The result: simplified troubleshooting and the option of integrating predictive maintenance solutions from different providers.

Predictive analytics draws its power from a wide range of methods and technologies, including big data, data mining, statistical modeling, machine learning and assorted mathematical processes. Organizations use predictive analytics to sift through current and historical data to detect trends and forecast events and conditions that should occur at a specific time, based on supplied parameters.

Digital Twins. By definition, a "Digital Twin" is a continuously learning system of digital copies of assets, systems and processes that can be queried automatically, or even by voice, for specific outcomes. A digital twin can predict asset behavior and capacity to deliver on specific outcomes within given parameters and cost constraints. The machine doesn't sleep and the digital twin informs what you need to do with the assets on the physical twin in order to achieve the targeted outcome.

The **digital twin** is a *system of systems* based on a virtual digital copy of all the infrastructure assets as represented by Deep Learning Neural Networks (DNNs). DNNs are a Machine Learning technique that brings us a new paradigm of "software that writes software" and acts as

a compiler for your data to deliver the desired outcome. Virtual twins accompany a physical product from the initial conceptualization and the design process right through production and updates - helping digital machine construction run better.

3D models instead of prototypes. Digital Twins are digital representations of physical machines. In industry, they are used to optimize product design and ensure error-free operation. They are formed on the basis of a high-precision 3D CAD model that has been assigned all the properties and functions of the planned product - from its materials and sensing systems to the movement and dynamics of the real machine.

Constant exchange of data. The twins are constantly in connection with one another - even after production and sale of the physical product. The real machine is outfitted with sensors that send status data to its virtual reproduction on a constant basis. A requirement management system functions as a digital requirements library, gathering the incoming data and comparing it against the specifications by which the product was created. If a discrepancy is detected, engineers can work on potential solutions directly on the digital twin - after which the real machine can then be updated to resolve the problem as quickly as possibly.

IT security for digital twins. To ensure the security of the Digital Twins, a variety of enhanced security measures from the IT realm are needed in industry. Digital industry systems are an especially common target for malicious software, spread through the internet, corporate intranets or external hardware. The concept of "industrial security" is thus not just focused on physical securing of devices through alarm systems and access codes, but also the use of firewalls in corporate networks and walling off of external electronic interfaces.

Predictive maintenance is a popular application of predictive analytics that can help businesses in several industries achieve high asset utilization and savings in operational costs. This guide brings together the business and analytical guidelines and best practices to successfully develop and deploy PdM solutions using the Microsoft Azure AI platform technology.

Prerequisite knowledge. The BDM content does not expect the reader to have any prior data science knowledge. For the TDM content,

basic knowledge of statistics and data science is helpful. Knowledge of Azure Data and AI services, Python, R, XML, and JSON is recommended. AI techniques are implemented in Python and R packages. Solution templates are implemented using Azure services, development tools, and SDKs.

Business problems in PdM. Businesses face high operational risk due to unexpected failures and have limited insight into the root cause of problems in complex systems. Some of the key business questions are: detect anomalies in equipment or system performance or functionality; predict whether an asset may fail in the near future; estimate the remaining useful life of an asset; identify the main causes of asset failure; identify what maintenance actions need to be done, by when, on an asset.

Typical goal statements from PdM are: reduce operational risk of mission critical equipment; increase rate of return on assets by predicting failures before they occur; control cost of maintenance by enabling just-in-time maintenance operations; lower customer attrition, improve brand image, and lost sales; lower inventory costs by reducing inventory levels by predicting the reorder point; discover patterns connected to various maintenance problems; provide KPIs (key performance indicators) such as health scores for asset conditions; estimate remaining lifespan of assets; recommend timely maintenance activities; enable just in time inventory by estimating order dates for replacement of parts.

These goal statements are the starting points for: *data scientists* to analyze and solve specific predictive problems; *cloud architects and developers* to put together an end to end solution.

Data affinity by association. Association rule mining is another analytics method that looks for relationships among different data attributes. For doing predictive customer analytics, it produces rules that support market basket analysis aimed at finding products that frequently coexist in online shopping carts in order to identify purchase patterns that can trigger recommendations to shoppers.

Applications of real-time analytics. In CRM (customer relations management), real-time analytics can provide up-to-the-minute information about an enterprise's customers and present it so that better and quicker business decisions can be made - perhaps even within the

time span of a customer interaction. Real-time analytics can support instant refreshes to corporate dashboards to reflect business changes throughout the day. In a data warehouse context, real-time analytics supports unpredictable, ad hoc queries against large data sets. Another application is in scientific analysis such as the tracking of a hurricane's path, intensity, and wind field, with the intent of predicting these parameters hours or days in advance.

How deep learning works. Computer programs that use deep learning go through much the same process. Each algorithm in the hierarchy applies a nonlinear transformation on its input and uses what it learns to create a statistical model as output. Iterations continue until the output has reached an acceptable level of accuracy. The number of processing layers through which data must pass is what inspired the label *deep*.

Use cases today for deep learning include all types of big data analytics applications, especially those focused on natural language processing (NLP), language translation, medical diagnosis, stock market trading signals, network security and image identification.

Using neural networks. A type of advanced machine learning algorithm, known as neural networks, underpins most deep learning models. Neural networks come in several different forms, including recurrent neural networks, convolutional neural networks, artificial neural networks and feed forward neural networks, and each has their benefit for specific use cases.

Neural networks involve a trial-and-error process, so they need massive amounts of data to train on. It's no coincidence that neural networks became popular only after most enterprises embraced big data analytics and accumulated large stores of data.

Examples of deep learning applications. Because deep learning models process information in ways similar to the human brain, models can be applied to many tasks people do. Deep learning is currently used in most common image recognition tools, NLP processing and speech recognition software. These tools are starting to appear in applications as diverse as self-driving cars and language translation services.

Limitations of deep learning. The biggest limitation of deep learning models is that they learn through observations. This means they only know what was in the data they trained on. If a

user has a small amount of data or it comes from one specific source that is not necessarily representative of the broader functional area, the models will not learn in a way that is generalizable.

Computer programs that use deep learning go through much the same process. Each algorithm in the hierarchy applies a nonlinear transformation on its input and uses what it learns to create a statistical model as output. Iterations continue until the output has reached an acceptable level of accuracy. The number of processing layers through which data must pass is what inspired the label *deep*.

A neural network usually involves a large number of processors operating in parallel and arranged in tiers. The first tier receives the raw input information - analogous to optic nerves in human visual processing. Each successive tier receives the output from the tier preceding it, rather than from the raw input - in the same way neurons further from the optic nerve receive signals from those closer to it. The last tier produces the output of the system.

Each processing node has its own small sphere of knowledge, including what it has seen and any rules it was originally programmed with or developed for itself. The tiers are highly interconnected, which means each node in tier n will be connected to many nodes in tier $n-1$ - its inputs - and in tier $n+1$, which provides input for those nodes. There may be one or multiple nodes in the output layer, from which the answer it produces can be read.

Neural networks are notable for being adaptive, which means they modify themselves as they learn from initial training and subsequent runs provide more information about the world. The most basic learning model is centered on weighting the input streams, which is how each node weights the importance of input from each of its predecessors. Inputs that contribute to getting right answers are weighted higher (Fig. 34.5) [12].

The assumptions people make when training algorithms causes neural networks to amplify cultural biases. Biased data sets are an ongoing challenge in training systems that find answers on their own by recognizing patterns in data. If the data feeding the algorithm isn't neutral - and almost no data is - the machine propagates bias.

Types of neural networks. Neural networks are sometimes described in terms of their depth, including how many layers they have between input and output, or the model's so-called hidden layers.

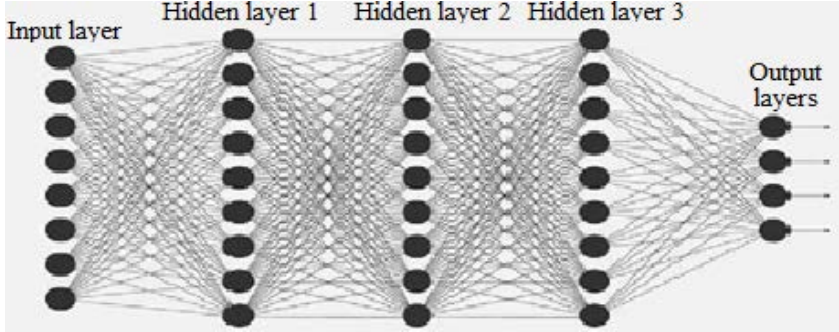


Fig. 34.5 - Deep learning neural network [12]

This is why the term *neural network* is used almost synonymously with deep learning. They can also be described by the number of hidden nodes the model has or in terms of how many inputs and outputs each node has. Variations on the classic neural network design allow various forms of forward and backward propagation of information among tiers.

The simplest variant is the feed-forward neural network. This type of artificial neural network algorithm passes information straight through from input to processing nodes to outputs. It may or may not have hidden node layers, making their functioning more interpretable.

More complex are recurrent neural networks. These deep learning algorithms save the output of processing nodes and feed the result back into the model. This is how the model is said to learn.

Convolutional neural networks are popular today, particularly in the realm of image recognition. This specific type of neural network algorithm has been used in many of the most advanced applications of AI including facial recognition, text digitization and natural language processing.

Applications of artificial neural networks. Image recognition was one of the first areas to which neural networks were successfully applied, but the technology uses have expanded to many more areas, including: chatbots; natural language processing, translation and

language generation; stock market prediction; delivery driver route planning and optimization; drug discovery and development.

34.2.2 Tools for predictive diagnostics and maintenance for predictive diagnostics

Predictive analytics can be used to predict important events in a customer's life cycle and increase their revenue during those times. Predictive maintenance involves the deployment of sensor-based diagnostic monitoring in real-time for assets and sub-systems that provide enough time to act - based on the recorded condition parameters [12-14]. Predictive analytics is the use of data, statistical algorithms and AI techniques to identify possible future outcomes. This can help you stay ahead of the curve and assess the future of your marketing. Here are a few ways that you can use AI and predictive analytics in the marketing. Predictive analytics use science to predict what will happen in the future - everything from what customers will want to how the market will perform and the biggest trends. Brands can use this information to target the right customers and provide personalized service and recommendations.

Data visualization tools go beyond the standard charts and graphs used in Microsoft Excel spreadsheets, displaying data in more sophisticated ways such as infographics, dials and gauges, geographic maps, sparklines, heat maps, and detailed bar, pie and fever charts.

A predictive maintenance application with a data repository based on the Hadoop distribution from MapR Technologies. The data goes into an Amazon Simple Storage Service (Amazon S3) repository for processing and analysis on a pair of cloud-based clusters running Databricks' version of Spark [14,15].

Automated neural networks (ANN) are advancing robotics both as a source for improvements in computer vision and with collaborative computing. The ability of ANNs to learn complex tasks and interactions has meant the rapid advancement in vision skills seen in the last decade. In addition, collaborative computer requires the adaptive ability that that ANNs can provide.

Recent advances in natural language processing (NLP), as seen with Amazon Alexa and Apple Siri, and natural language generation

(NLG) as found in companies such as Narrative Science and Automated Insights, have advanced to the point where robots can understand humans and respond in human-like speech. While that is being adopted faster in other areas, the ability of a regular line worker or manager to get information from and give information to manufacturing robots without requiring skills in programming is beginning to see this move from academics into field robotics, but of the four AI points it is the one in the earliest stage.

Predictive Maintenance Tools. Successful predictive maintenance programs all rely on a set of tools to make them function.

1. **Small Early Pilot Programs.** Before you invest in an entire predictive maintenance program, do pilots. Pilots will help you determine whether the value is there in your organization. Find a partner that has a SaaS service you can pilot your predictive maintenance program with. Start small and see what predictive maintenance can do for your organization and then iterate and grow from there.

2. **A Technology Suite for Aggregating Data.** Data is the engine of any predictive maintenance program. Therefore, there must be technology in place to collect, process, prepare and structure massive amounts of device data which will be stored in the organization's ecosystem. This system must be able to understand what each piece of data represents so that it can be monitored as a part of the entire maintenance feedback landscape.

3. **Algorithms to Monitor Patterns and Events in Real Time.** Once there is data streaming in and being collected from your industrial equipment, data science and machine learning come into play. By monitoring patterns in real time and looking at historical data, the machines themselves can identify repeat scenarios which they can then create rules for moving forward. This process is an adaptive learning process, meaning that the machines learn over time. The more data and scenarios they collect and encounter, the more they learn.

4. **Effective Workflows.** Once your machines have collected enough data and have begun predicting events, your organization will need to ensure it has the tools in place to integrate your predictive maintenance data with your existing technology.

5. **Service Management.** With workflows in place, deep analysis can be performed to improve and refine processes over time.

6. A Change Management Agreement. Ensure there is commitment and buy in from management. In order for any organizational or technological change to be effective, there needs to be company wide adoption. This is true of any large change to the way a business operates, and implementing a predictive maintenance program is no exception.

34.2.3 Reliability and cyber-security issues for predictive analytics software based systems. Cases

The architecture of the predictive analytics can be divided into 3 parts:

Knowledge View. Here the data collection part is done by the user and sensor. The data collected is stored in the form of representation maps and the knowledge cycle. The cycle is segregated with the help of artificial intelligence.

B. Technique View. In this view pre discovered techniques are applied which are properly scrutinized so that the result obtained is of high quality. Machine learning is used to optimize the technique so that the knowledge is consistent and the outliers are minimum.

C. Application View. In this view try to inculcate the applications or the task that has to be performed on the database [16].

The process of predictive analytics consists of various steps as mentioned in Fig. 34.6:

1) Data gathering: The data is gathered from the sensors and IoT appliances in order to make the things easier for the analytics process which requires a proper dataset.

2) Data Cluster analysis: The data is then formed into clusters to group the similar values as one unit. The cluster is then used for further processing [17].

3) Association rule mining: Association rule mining is performed on the attribute values to conclude which kind of values occur together.

4) Outlier Analysis: Outliers are analyzed to derive a conclusion for their exact position. The decision about whether the values gathered can be accommodated to the current data cluster or a new cluster is taken by following certain predefined steps [18].

5) Conclusive Statement gathering: This is the last step of the process in which the data after processing forms an if-else ladder for easy derivation of conclusions [19].



Fig. 34.6 - Flow chart on predictive analytics process A

The diagram depicting the complete process is mentioned in the fig. 34.7. The process is must for all systems offering support for predictive analytics.



Fig. 34.7 - Process of Conclusive Statement gathering

Architecture. The architecture of the predictive analytics on IoT is divided into 4 stages on the basis of the function performed at each level and the kind of job performed as shown in the fig. 34.7. The process revolves around 4 level architecture.

1) Sensor level – the sensors are used along with the internet connected appliances to help in the building of the database [20].

2) Controller level – in this level the controller helps in reporting the values to the database which can be local as well as in cloud.

3) Database level –the values gathered as the dataset are reported to the central database where the values are altered as per the user [21].

4) Application level – the altered values are put into application as per the application requirement [22].

The predictive analytics on IoT is the branch of predictive analytics dealing with the prediction involved with the setting of IoT appliances. The predictive analytics on IoT works with the help of data gathered by various specialized sensors implanted at places where IoT devices have to function and helps in creating the data set which act as an input to the predictor. The process of predictive analytics on IoT helps us in achieving the goal of home automation and makes the things lot easier to implement, it offers the flexibility of implementing the latest hardware by making certain changes to the dataset created by the

previous generation hardware. Apart from the data generated by the IoT one should make separate table to store the data generated by the sensors which act as the catalyst to the process of predictive analytics. Along with the feedback to rely upon we will also have the sensor to supplement the existing information. Predictive analytics makes use of various statistical and analytical technique to predict the setting used by the IOT devices. It makes use of machine learning to make the process of prediction lot easier.

34.3 Availability assessment of IoT based IT infrastructure

34.3.1 Availability models

The example of IoT based IT infrastructure is smart business center (SBC). The structure of the SBC network includes devices: a router with Ethernet ports, a soft switch, a firewall, a power network, a server with management software, an IP camera, sensors, cables. In the operational system of the server and the router there are several power consumption modes of operation. When creating SBC, it is advisable to take into account the security, reliability of software and hardware subsystems, the choice of energy saving modes [23,24]. Fig.34.8 shows a Markov graph of functioning of the main subsystems SBC, λ - the failure rate or attack, μ - the recovery rate.

A Markov model of SBC subsystems functioning, represented in fig.34.8, considering DDoS attacks and energy modes of server and router, which has the following states: Good-working state (1); State when the server is fully used with high power consumption S0 (2); State when the server is fully used, the hardware, that are not used, can enter the low-power mode S1 (3); State of the server sleep mode with low power consumption, a computer can wake up from a keyboard input, a local access network or universal serial bus device S2 (4); State when power consumption of server is reduced to the lowest level S3 (5); State of server failure (6); State of switching to the backup server device after the server failure (7); State of restarting the server software after the software fault (8); Successful DDoS-attack on the server after the firewall failure (9); State of firewall software or hardware failure (10); Attack on the power supply system after the firewall failure, that lead

the failure of general power system of IoT system (11); State of switching from the general power system after its failure on the alternative energy sources (solar, diesel generator, wind turbine) (12); Router Status Active - sending packages with high power consumption (13); successful DDoS-attack on the router (14); Good-working state of the router without transmitting packets - Normal Idle (15); Good-working state of the router without packet transmission Low-Power Idle (16); Router software or hardware failure (17); State of server software or hardware fault (18); State when router hardware or software fault (20); State of switching to the backup router device after the router failure (19); State of restarting the router software after its fault (22).

The availability factor is an important indicator of SBC reliability under the influence of different kinds of DDoS-attacks, so as an index of its reliability we choose availability function $AC(t)$, that is defined as the sum of the probabilities of staying the system in an up-states.

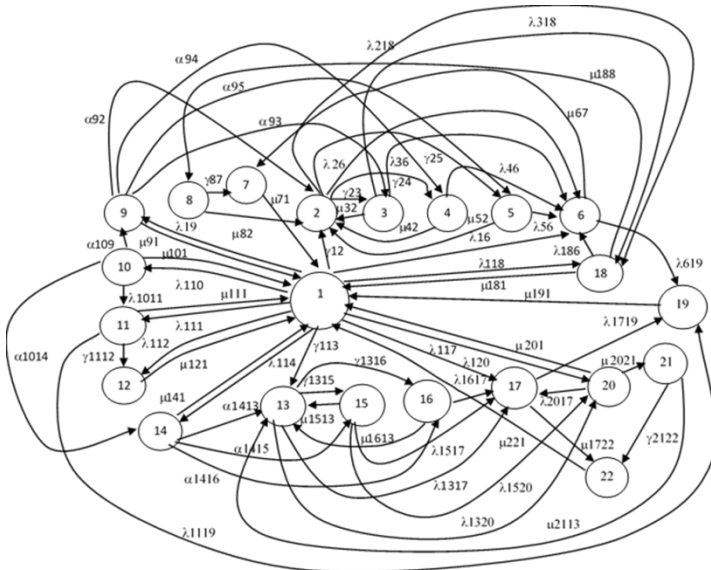


Fig. 34.8 - A graph of a Markov model of SBC subsystems functioning

For the developed model, the following assumptions were chosen:
 - the flow of failures that occurs in the SBC system is a process without aftereffects, each time in the future the system's behavior

depends only on the state of the system at this time and does not depend on how the system has passed to this state. The flow of failures and failures of both software and hardware is the simplest and obeys the law of exponential distribution. The failures flow in the SBC system has the Markov property;

- the structure of the network include the reservation of the server and router, time of transition to the reserve in the event of a failure of the main device is minimal;

- the number of DDoS attacks and the number of primary defects in the software are constant;

- the monitoring and diagnostics tools are in good working order and determine the technical state of the system with a high degree of authenticity.

For rebuilt model (different options for patching or lack of patching on the vulnerability of firewalls), the system of differential linear Kolmogorov-Chapman equations was presented and researched, the availability function (AC) value calculated and analyzed if normalization conditions:

$$\sum_{i=1}^{22} P_i(t) = 1, P_i(0) = 1, i=1...22 \quad (34.1)$$

The AC is an important indicator of the reliability of SBC when exposed to various types of DDoS attacks, so AC was chosen as the SBC availability indicator, which is defined as the sum of the probabilities of the system staying in well-operating states.

For the model, shown in Fig. 34.8, the AC is determined from the equation:

$$AC=P1(t)+P2(t)+P3(t)+P4(t)+P5(t)+P12(t)+P13(t)+P15(t)+P16(t)+P21(t). \quad (34.2)$$

$P_i(t)$ – probabilities of SBC components states.

34.3.2 Research of models

Basing on the analysis of statistical data, an indicator of the AC can be found. The graphical dependencies of the system AC on the

transition rates to different states (λ_{ij} - failure rates, α_{ij} - attack rates, γ_{ij} - transition rates in different modes power consumption of the router and server, where $i = 1...22, j = 1...22$) have been received for the various technical states of the SBC components shown in Fig. 34.9 - 34.14. In the values of failure rates, factors influencing the reliability of the IoT subsystems during operation (climatic factors, load, vibrations) are taken into account. Initial data for the calculation of AC, the values of which are based on the analysis of statistical data, are: $\lambda_{1317}=5,7 \cdot 10^{-4}$ 1/h; $\lambda_{1517}=1 \cdot 10^{-5}$ 1/h; $\lambda_{1617}=1 \cdot 10^{-6}$ 1/h; $\lambda_{218}=1 \cdot 10^{-5}$ 1/h; $\lambda_{318}=1 \cdot 10^{-5}$ 1/h; $\lambda_{1320}=1 \cdot 10^{-6}$ 1/h; $\lambda_{1520}=1 \cdot 10^{-6}$ 1/h; $\lambda_{2017}=1,14 \cdot 10^{-3}$ 1/h; $\lambda_{120}=1 \cdot 10^{-6}$ 1/h; $\mu_{67}=60$ 1/h; $\mu_{141}=0,125$ 1/h; $\mu_{111}=0,5$ 1/h; $\mu_{32}=40$ 1/h; $\mu_{42}=30$ 1/h; $\mu_{52}=30$ 1/h; $\mu_{1513}=50$ 1/h; $\mu_{1613}=60$ 1/h; $\mu_{71}=0,02$ 1/h; $\mu_{87}=2$ 1/h; $\mu_{81}=30$ 1/h; $\mu_{101}=1$ 1/h; $\mu_{121}=5$ 1/h; $\mu_{181}=1$ 1/h; $\mu_{191}=0,02$ 1/h; $\mu_{91}=1$ 1/h; $\mu_{171}=1$ 1/h; $\mu_{188}=60$ 1/h; $\mu_{61}=0,02$ 1/h; $\mu_{2021}=60$ 1/h; $\mu_{221}=20$ 1/h; $\mu_{211}=30$ 1/h; $\mu_{1722}=60$ 1/h; $\mu_{201}=40$ 1/h; $\mu_{2113}=20$ 1/h.

The graphical dependencies (Fig. 34.8 - 34.13) show the change in the AC values from the change in the transition rates from one state to another in the Markov models with fixes for software vulnerabilities: the server firewall (AC 9); firewall (AC 10); the firewall of the server and the router (AC 9_14) and without patches (AC).

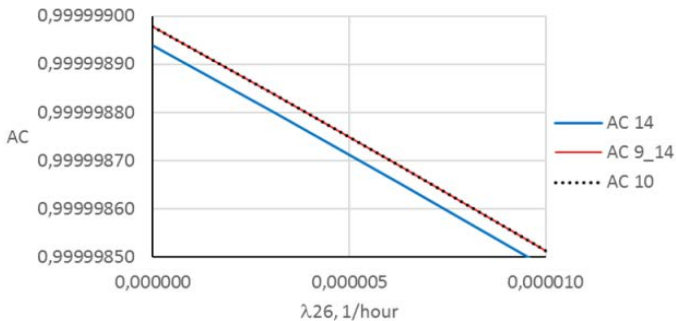


Fig. 34.9 - Graphics of AC SBC dependence on the transition rate λ_{26} from active-power state of the server 2 to a state of the server failure 6 for models with patches on vulnerabilities of: server firewall (AC 9) and router firewall (AC 14) and without patches (AC) if λ_{26} change values in range $0...1 \cdot 10^{-5}$ 1/h

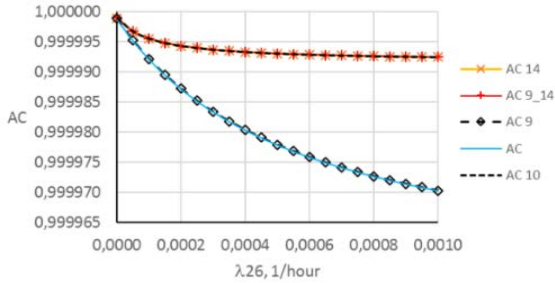


Fig. 34.10 - Graphics of AC SBC dependence on the transition rate λ_{26} from active-power state of the server 2 to a state of the server failure 6 for models with patches on vulnerabilities of: router firewall (AC 14); server firewall (AC 9); firewall (AC 10); server and router firewall (AC 9_14) and without patches (AC) if λ_{26} change values in range $0 \dots 1 \cdot 10^{-3}$ 1/h

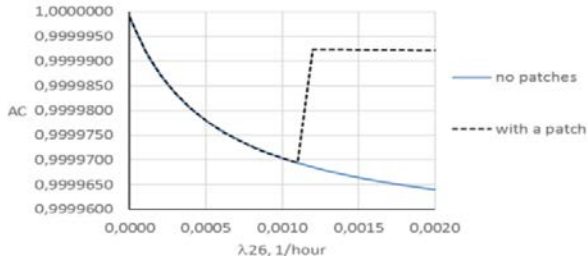


Fig. 34.11 - Graphics of AC SBC dependence on the transition rate λ_{26} from active-power state of the server 2 to a state of the server failure 6 for models with patches on vulnerabilities of: firewall (AC 10) and server and router firewall (AC 9_14) if λ_{26} change values in range $0 \dots 2 \cdot 10^{-3}$ 1/h

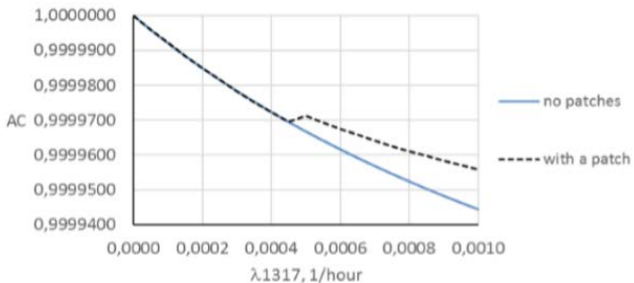


Fig. 34.12 - Graphics of AC SBC dependence on the transition rate λ_{1317} from active-power state of the router 13 to a state of the router failure 17 for models with and without patches on firewall if λ_{1317} change values in range $0 \dots 1 \cdot 10^{-3}$ 1/h

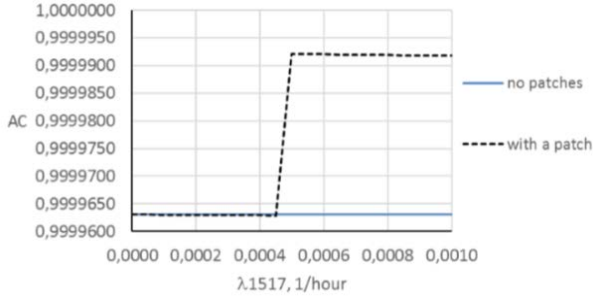


Fig. 34.13 - Graphics of AC SBC dependence on the transition rate λ_{1517} from low-power state of the router 15 to a state of the router 17 for models with and without patches on firewall if λ_{1517} change values in range $0 \dots 1 \cdot 10^{-3}$ 1/h

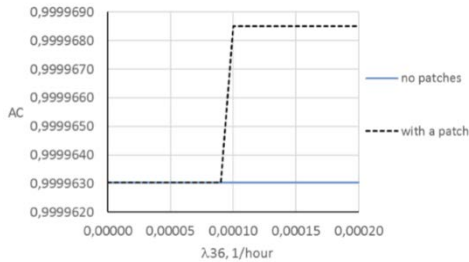


Fig. 34.14 - Graphics of AC SBC dependence on the transition rate λ_{36} from not active-power state of the server 3 to a state of the server failure 6 for models with patches on vulnerabilities of firewall (AC 10) and without patches if λ_{36} change values in range $0 \dots 2 \cdot 10^{-4}$ 1/h

When DDoS attacks affect the SBC server and router, the power consumption of these devices increases, because they can't switch to a low-power mode, because they constantly process requests for data transmission and processing. The analysis of the Markov model simulation results showed that by increasing the rate of the transition to a state of denial firewall λ_{19} decreases the value of SBC availability function. In case of refusal the firewall different kinds of attacks can

freely influence the vulnerability of the server software, router, switch. Increase the rate of the transition from a state to a state of denial firewall Brute-force attack - λ_{920} , Phishing-attacks - λ_{921} , DDoS-attacks - λ_{916} reduces the value of availability function of SBC.

Analysis of the constructed Markov model showed that the studied system is stable, the availability function quite high and not much changing with an increase in the intensities of the attacks. Recently, however, increasing number of malicious attacks and their types, that will lead to a sharp decrease in system reliability and security of SBC. It is therefore necessary to look for more advanced security techniques researched systems that suppose purpose of further research.

Fig. 34.8 shows the graph of AC SBC from λ_{26} - the transition rate from a good working state in the active mode (2) to the server failure state (6) without patches in the attack conditions (AC) and patches on vulnerabilities of the firewall software of the router (14), router and server simultaneously (9 and 14), server (9), firewall at SBC (10) input. As can be seen from the figure, with increasing λ_{26} , installing a patch on the firewall software of the server at $\lambda_{26} = 1 \cdot 10^{-3}$ 1/hour gives the value of AC = 0.99997 and slightly affecting the availability of the system, since with the selected source data it differs from the system's AC without patches on 10^{-9} .

At the same time, when the patches are installed on the vulnerabilities of the firewall software, the firewall server and the router, the firewall of the router (states 10, 9_14, 14) the system readiness is increased and at $\lambda_{26} = 1 \cdot 10^{-3}$ 1/h is AC = 0.999925. Fig. 34.9 shows the graph of AC dependency, taking into account patching, on the vulnerability of the firewall software, the server firewall and the router, the router's firewall with a higher sampling rate than Fig. 34.8. Analysis of graphs (Fig. 34.9, Fig. 34.10) showed that the greatest increase in AC occurs when patching the vulnerabilities of the router and the server simultaneously (9_14) or the vulnerabilities of the entire system's firewall (10). The research data are valid for a given set of input data, which must be periodically refined.

The developed models allows take into account the change in the transition rates from one state to another state under attack conditions and the installation of patches for various vulnerabilities. The calculations took into account the average statistical data - the critical

number of data packets for DDoS attacks, which leads to possible fails and failures of various SBC devices or failure of the entire system. The beginning of the attack can't always be determined. An indirect sign of the beginning of the attack can serve as an increase in the requests flow to a critical level. Under the influence of an attack, an increase in the transitions rates from one state to another leads to a decrease in the value of AC. After installing the patch, when the critical level of the transitions rates is reached, AC increases. According to the average statistical data, critical values were adopted for the rates of transitions under attack conditions: $\lambda_{36} \leq 1 \cdot 10^{-4}$ 1/h, $\lambda_{26} \leq 1.2 \cdot 10^{-3}$ 1/h, $\lambda_{1317} \leq 5 \cdot 10^{-4}$ 1/h, $\lambda_{1517} \leq 1 \cdot 10^{-5}$ 1/h. When specifying conditions for determining attacks based on later statistics and installing patches, can get updated graphs of the AC dependence on the system transitions rates from one state to another.

The graphical dependences shown in Fig. 34.9-34.14, reflect the change in the value of AC, when the transition rates λ_{26} , λ_{1517} , λ_{36} change values in the range $0 \dots 2 \cdot 10^{-4}$ 1/h in two cases: when the model does not take into account the installation of a patch on the vulnerabilities of the firewall software and when in the model it is considered that fixing the vulnerabilities of the firewall software will be immediately as soon as the attack shows itself.

The use of patches on software vulnerabilities of devices after detection of the attack process immediately significantly increases the value of AC SBC: AC (λ_{26}) to about 0.9999925, AC (λ_{1317}) to about 0.99997, AC (λ_{1517}) to about 0.99999, AC (λ_{36}) to about 0.99990.

34.3.3 Tools and techniques

1) **SAP Business Objects:** Being one powerful Business Intelligence platform, SAP Business Objects definitely makes to the top of our list. The tool promises to offer agile and informed business decision-making techniques. Hence giving the business an entirely new perspective to incorporate robust and scalable solutions. SAP Business Object allows businesses to analyze large volumes of data and find insights that are capable of inspiring actions in real time, to visualize data on a self-service basis and thereby provides a decent time for both users and organizations to focus on creating more business value.

2) **IBM Predictive Analytics:** IBM provides easy to use predictive analysis products and solutions to meet the need of different businesses. IBM SPSS Modeler and IBM SPSS Analytics are two major software that enables users of all skill levels to deploy predictive analytics to improve the businesses. The platform helps the organization to transform the irrelevant data into predictive insights to guide major enterprise decisions and thereby help in the prevention of frauds and maximization of profitability. With capabilities of text analytics and geospatial analysis, it is easily extendable to open source technologies with optional coding. The platform even enables organizations to adapt quickly to changing business requirements without compromising on security and privacy when using the cloud.

3) **QlikView:** one of the most flexible yet simple business intelligence platforms is QlikView. Designed by QlikTech for business intelligence data recovery it helps organizations to extract relevant information from a given set of data. The interpreted data thereafter help the users in creating guided analytics applications. The platform utilizes a user-driven approach to business intelligence and the interface is extremely simple to work with when it building charts and generating custom made dashboards reflecting upon the business challenges. QlikView is ascertained to bring the fastest and smooth implementation in a short span of time. Even BARC' BI Survey 10 acknowledged QlikView for its 'Agile BI' ability and rendered it as the highest scorer.

4) **Halo:** an end to end supply chain management system that helps in business forecasting and planning then Halo must be your pick. It is an essentially smart platform that provides a reliably established data repository where scenarios can be run and repeated over time to match predictions with the result. Easily available for hosted or cloud and accessible from any browser, Halo supply chain analytics passes information directly into the hands of the decision makers. With self-service supply chain management and data planning, Halo enables organizations to gain competitive advantage and help increase customer satisfaction.

5) **Dataiku DSS.** Based out of Collaborative Data Science development platform, Dataiku offers to turn raw data into predictions. Dataiku DSS enables users to apply analytics appropriate algorithms in order to uncover patterns and predict trends. Users can easily leverage

existing libraries or even use custom codes in R, Python or can even integrate external libraries through code API's. It helps users to interact, explore and clean raw data form. Another incentive associated with the platform is that it is quite quick when it comes to preparing and processing data. With a simplified spreadsheet interface that runs in conjunction to contextual transformations, makes working on bulk data a painless process altogether.

6) **RapidMiner Studio:** RapidMiner Studio is a data science workflow designer that access, load and analyze any type of data to extract statistics and a key piece of information. The platform also cleanses data efficiently for predictive analytics and on the basis of the extracted data, it delivers faster models.

The platform comes with an unparalleled set of modeling capabilities and machine learning algorithms for supervised and unsupervised learning. RapidMiner Studio also means to estimate accurate model performances. It employs a modular approach which prevents data leak and there is no overestimation of prediction performances occurrence.

7) **Knime Analytics:** Knime or Konstanz Inforation Miner is an open source platform for data analytics, reporting, and integration. The platform employs Apache Hadoop and Apache Spark and integrates with several machine learning libraries such as H2O, Keras, Scikit-Learn for offering advanced predictive analytics. Knime makes the use of native nodes, community contributions, and various tool integrations and therefore emerges as a strong and powerful analytics tool for data scientists.

The platform has easy to learn interface which means the coding becomes an optional and the work is visually documented. Apart from that simple text files, databases, images, and even Hadoop based data can be combined with the same visual flow.

34.3.4 Assessment cases

There are some predictive analytics cases for industry:

1. **Churn Prevention.** When a business loses customers, it needs to bring new customers in to replace the loss in revenue. And that can get very expensive, because the costs of new customer acquisition is usually

much more expensive than existing customer retention. Key Industries: Automotive, Banking, Insurance, Retail, Telecommunications.

2. Customer Lifetime Value. One of the more difficult things to do in marketing is to identify those customers that are going to spend the most money, in the most consistent way and over the longest period of time. This kind of insight allows companies to optimize their marketing to increase their share of that segment of the business, and gain those customers that will have the greatest lifetime value to your company. Key Industries: Banking, Insurance, Retail, Telecommunications, Utilities.

3. Customer Segmentation. Different companies define their markets differently, and segment their markets according to those aspects that offer the most value to their particular industry, products and services. Key Industries: Automotive, Banking, Life Sciences/Pharmaceutical, Insurance, Retail, Telecommunications, Utilities.

4. Next Best Action. Defining your primary market segments and customers is a critical use case for predictive analytics. But that only provides an incomplete picture of what your marketing approach should be. Key Industries: Banking, Education, Insurance, Telecommunications.

5. Predictive Maintenance. In many industries, containing costs is as valuable a strategy and increasing revenue. And for companies with a major investment in infrastructure and equipment, the ability to manage that capital outlay is critical. By analyzing metrics and data related to the lifecycle maintenance of technical equipment, companies can predict both timelines for probable maintenance events and upcoming capital expenditure requirements, allowing them to streamline their maintenance costs and avoid critical downtime. Key Industries: Automotive, Manufacturing, Logistics & Transportation, Oil & Gas, Utilities.

6. Product Propensity. Product propensity analytics combine data on purchasing activities and behavior with online behavior metrics from things like social media and e-commerce, and performs correlations of that data to provide insight into the effectiveness of different campaigns and social media channels when it comes to your company's products and services. Key Industries: Banking, Insurance, Retail.

7. **Quality Assurance.** Quality control is key to not just the customer experience, but also to your bottom line and operational expenses as well. Over time, inefficient quality control will affect your customer satisfaction, buying behaviors, and ultimately impact revenues and market share. And the costs don't stop there. Poorer quality control leads to more customer support costs, warranty issues and repairs, and less efficient manufacturing. Good predictive analytics can provide insight into potential quality issues and trends before they become truly critical issues. Key Industries: Automotive, Life Sciences/Pharmaceutical, Manufacturing, Logistics & Transportation, Oil & Gas, Utilities.

8. **Risk Modeling.** Risk comes in a number of forms, and can originate from a variety of sources. Predictive analytics can glean potential areas of risk from the massive number of data points collected by most organizations, and sorting through them to identify potential areas of risk, and trends in the data that suggest the development of situations that can affect the business and bottom line. By combining these analytics with a cogent risk management approach, companies can capture and quantify risk issues, evaluate them, and decide on a course of action to mitigate those risk factors deemed most critical. Key Industries: Automotive, Banking, Manufacturing, Logistics & Transportation, Oil & Gas, Utilities.

9. **Sentiment Analysis.** It's very difficult to be everywhere at all times, especially in the online world. Likewise, capturing and reviewing everything that's said about your company or organization is virtually impossible. However, by combining web search and crawling tools with customer feedback and posts, you can create analytics that give you a picture of your organization's reputation within your key markets and demographics, and provide you with proactive recommendations as to the best ways to enhance that reputation. Key Industries: Life Sciences/Pharmaceutical, Education, Insurance, Retail, Telecommunications.

10. **Up- and Cross-Selling.** Predictive analytics can provide suggestions on which products might be combined to appeal to which market segments. Key Industries: Banking, Insurance, Retail, Telecommunications.

34.4 Work related analysis

The project PRORETA [25] is a research in the area of the cooperative HMIs. The research object is the prototype of the cooperative automobile HMI that implements the scenarios of preventing collisions at the cross-roads. The PRORETA HMI system implements a huge number of use scenarios, it does not complicate or irritate and ensures the multimode support.

The HMI provides 4 support levels – information messages, warnings, actions recommendations, automatic intervention.

This project is focused on the measurement accuracy performance and role of smart meters as distributed end-node sensors in the distribution grid, providing leadership for an ANSI standard for meter upgradeability, and creating a testbed for testing the best commercially-available smart meters, expected to have 0.05% measurement accuracy [26].

Smart Grid Projects Outlook 2014 presents the latest analyses and insights from the most comprehensive database of smart grid projects for electricity across the European Union (EU) Member States. This rolling review, carried out on a periodical basis by the European Commission Joint Research Centre (JRC) in tight cooperation with the European Commission Directorate-General for Energy (ENER) [27].

The NIST wide Smart Grid Program develops and demonstrates smart grid measurement science advances to improve the efficiency, reliability, resilience, and sustainability of the nation's electric grid. This program is housed in the Engineering Laboratory and draws on the expertise of the Information Technology and Physical Measurement Laboratories [28].

Smart Grid Communication Networks project will focus on identifying opportunities to tailor communication protocols that have been designed for network traffic control to provide quality of service (QoS) to smart grid applications and to manage power flows in the smart grid between traditional and renewable generation sources and between utility-owned and customer-owned assets [29].

- KTH University, Sweden: three MSc programs including:

- a) IoT related topics in Information and Network Engineering [30],
- b) Communication Systems [31],

- c) Embedded Systems [32];
 - Newcastle University, United Kingdom: MSc Program on Embedded Systems and Internet of Things (ES-IoT) MSc [33].

Conclusions and questions

SMART (Self Monitoring Analysis and Reporting Technology) is the technology of self-diagnostics, analysis and report - was created to increase the reliability of the equipment, to ensure its remote control.

Smart Grid is a system that optimizes energy consumption, allowing the redistribution of electricity. "Intelligent" networks - a set of technical tools that allows you to quickly change the characteristics of the electrical network. At the technological level, electric networks, consumers and producers of electricity are combined into a single automated system that allows real-time monitoring and control of the operation modes of all participants in the process.

At the same time, the widespread introduction of IoT creates additional security deficiencies for the SG as a whole, due to the inadequate assessment of their impact on the functional and information security of the I&C in SG.

This Section presents a comprehensive information in regards to reliability assessment of IoT based IT infrastructure, I&C failures classification, highlights on models of reliability and techniques of its assessment and assurance. Method of safety assessment taking into account the reliability of systems (subsystems) is considered in this section.

The section presents the features of the implementation of machine and deep learning of neural networks, predictive analytics for the Internet of things systems are considered. Markov models of functioning of the Internet of things systems are proposed and investigated. The research showed that the IoT system, even with the required high AC value, is highly dependent on the correct failure-free operation of the firewalls. Analysis of the graphical dependencies obtained for the developed models, taking into account the rearrangement in case of appearance and installation of the patch on the vulnerability of the firewall software, showed that AC is most sensitive to patching the firewall software of the router and the network firewall.

With the purposes of understanding of material presented in this section, the readers are supposed to answer the following questions.

1. What are the main difference between Smart grid and power grid?
2. Why is smart grid safety important?
3. What are the main trends in the development of smart grid technologies at the present stage?
4. Give examples of the SG information technologies.
5. What are the main methods of SG reliability analysis?
6. What are the main differences between the Markov and BBN reliability models?
7. What role of IoT in SG?
8. Please describe the features of using machine learning for Internet of Things.
9. What is the difference between machine learning and deep learning of a neural network?
10. Explain what the term predictive maintenance means.
11. What are the features of the use of predictive analytics for the Internet of things systems? Please give examples.
12. How can you apply the mathematical apparatus of Markov models to assess the readiness of the Internet of things systems?
13. What are the main categories of the main applications of the Internet of things?
14. What are the main stages of the predictive analytics process for the Internet of Things systems?
15. What are the challenges for cybersecurity of the Internet of things systems using predictive analytics?
16. What are the main tools for the implementation of predictive analytics?

References

1. T. Basso, J. Hambrick, D. DeBlasio (2012) Update and review of IEEE P2030 Smart Grid Interoperability and IEEE 1547 interconnection standards. 2012 IEEE PES Innovative Smart Grid Technologies (ISGT).
2. NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0. NIST Special Publication 1108r3. – September 2014.

3. V. Gunes, S. Peter, T. Givargis, and F. Vahid, (2015) A survey on concepts, applications, challenges in cyber-physical systems, *KSII Trans. Internet Inf. Syst.*, 2015, doi:10.3837/tiis.0000.00.000.

4. Al-Omar, B., Al-Ali, A.R., Ahmed, R. and Landolsi, T. (2012) Role of Information and Communication Technologies in the Smart Grid. *Journal of Emerging Trends in Computing and Information Sciences*, 3, 707-716.

5. Gungor, V.C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C. and Hancke, G.P. (2013) A Survey on Smart Grid Potential Applications and Communication Requirements. *IEEE Transactions on Industrial Informatics*, 9, 28-42. <http://dx.doi.org/10.1109/TII.2012.2218253>

6. L. Bittencourt, R. Immich, R. Sakellariou, N. Fonseca, E. Madeira, M. Curado, L. Villas, L. DaSilva, C. Lee, and O. Rana, (2018) The internet of things, fog and cloud continuum: Integration and challenges, *Internet of Things*, 2018, vol. 3-4, pp.134-155.

7. K. Velasquez, D. P. Abreu, M. R. M. Assis, C. Senna, D. F. Aranha, L. F. Bittencourt, N. Laranjeiro, M. Curado, M. Vieira, E. Monteiro, E. Madeira, (2018) Fog orchestration for the internet of everything: state-of-the-art and research challenges, *Journal of Internet Services and Applications*, 2018, 9 (1).

8. Nunes D., Sá Silva J., Boavida F. (2017) *A Practical Introduction to Human-in-the-loop Cyber-physical Systems*. – John Wiley & Sons Ltd., 2017. – 320 p.

9. Nunes D.S., Pei Z., Sá Silva J. (2015) A survey on human-in-the-loop applications towards an internet of all. *IEEE Communications Surveys & Tutorials*. Vol.17, Issue 2, P.944-965.

10. Newcastle University. Science Central Smart Energy Labs. – <https://www.ncl.ac.uk/media/wwwnclacuk/instituteforsustainability/files/Smart-Energy-Labs-Online.pdf>

11. Margaret Rouse. Data sampling. <https://searchbusinessanalytics.techtarget.com/definition/data-sampling..>

12. Everything about data analytics. [https://datawarrior.wordpress.com/2017/10/31/interpretability-of-neural-networks/..](https://datawarrior.wordpress.com/2017/10/31/interpretability-of-neural-networks/)

13. Shivam Gupta. Transforming Railroad Asset Management: Going Smart with Predictive Maintenance. 2018. <https://www.tcs.com/content/dam/tcs/pdf/Industries/travel-and-hospitality/Transforming-Railroad-Asset-Management.pdf..>

14. Mit Predictive Analytics die Qualität von Fertigungsprodukten vorhersagen. Realtime Scoring bei der Felss Systems GmbH. https://x-integrate.com/mit-predictive-analytics-die-qualitat-von-fertigungsprodukten-vorhersagen/?fbclid=IwAR1F1UsGb_n1sv4uFqgO4z6nATsJmjc9H_51YWUvpeCKU-PwgY7p09jJ1g4..

15. Craig Stedman. IoT data analytics spurred on by big data's expansion. <https://internetofthingsagenda.techtarget.com/feature/IoT-data-analytics-spurred-on-by-big-datas-expansion..>

16. <https://searchbusinessanalytics.techtarget.com/feature/BI-data-dashboards-help-businesses-focus-on-analytics-ROI..>

17. Naveen Joshi. Can AI Become Our New Cybersecurity Sheriff? Contributor Cognitive World. Contributor Group. <https://www.forbes.com/sites/cognitiveworld/2019/02/04/can-ai-become-our-new-cybersecurity-sheriff/#2b89b5c836a8..>

18. IEC. IoT 2020: Smart and secure IoT platform. White paper. <http://www.iec.ch/whitepaper/pdf/iecWP-IoT2020-LR.pdf..> 193 p.

19. Architecture and Protocols for the Internet of Things: A Case Study/ Angelo P. Castellani, Nicola Bui, Paolo Casari, Michele Rossi, Zach Shelby, Michele Zorzi. 679-683 p. Available at: <https://www.ieeexplore.ieee.org/document/5470520..>

20. Sriram Parthasarathy. Top Use Cases for Real-Time Predictive Analytics. Sept., 2018. <https://www.logianalytics.com/predictive-analytics/top-use-cases-for-real-time-predictive-analytics/..>

21. Andrei Babulevich. The Importance of Quality Assurance Testing for the Internet of Things/ Andrei Babulevich, Ron Mader, Dan Myers, Sudha Sundaresan/Ayla Networks. 12 p. Available at: <https://www.aylanetworks.com..>

22. Ovidiu Vermesan, Peter Friess. Internet of Things – From Research and Innovation to Market Deployment/ River Publishers Series in Communication. 2014. 451 p.

23. Maryna Kolisnyk, Vyacheslav Kharchenko, Iryna Piskachova, Nikolaos Bardis. A Markov model of IoT system availability considering DDoS attacks and energy modes of server and router. ICTERI 2017. 14 p. <http://ceur-ws.org/Vol-1844/10000699.pdf..>

24. Kharchenko Vyacheslav, Kolisnyk Maryna, Piskachova Iryna. Reliability and Security Issues for IoT-Based Smart Business Center: Architecture and Markov Model. IEEE; Computer of science, MCSI 2016, Greece, Chania, 2016. Paper ID: 4564699.

25. Bauer, E. PRORETA 3: An Integrated Approach to Collision Avoidance and Vehicle Automation Text./E. Bauer, F. Lotz, M. Pfromm//At – Automatisierungs technik. – 2012. – № 12. – pp. 755-765.

26. Internet of Things Course - Immersive Program Master in City and Technology <https://apps.uc.pt/search?q=Internet+of+Things..>

27. Advanced metering smart distribution grids. NIST. <https://www.nist.gov/programs-projects/advanced-metering-smart-distribution-grids..>

28. Smart Grid Communication Networks. NIST.
<https://www.nist.gov/programs-projects/smart-grid-communication-networks..>

29. Smart Grid Testing and Certification. NIST.
<https://www.nist.gov/programs-projects/smart-grid-testing-and-certification..>

30. Master's program in Information and Network Engineering
<https://www.kth.se/en/studies/master/information-and-network-engineering/master-s-programme-in-information-and-network-engineering-1.673817..>

31. Master's program in Communication Systems
<https://www.kth.se/en/studies/master/communication-systems/description-1.25691>.

32. Master's program in Embedded Systems
[https://www.kth.se/en/studies/master/embedded-systems/description-1.70455/..](https://www.kth.se/en/studies/master/embedded-systems/description-1.70455/)

33. Related Programs to Embedded Systems and Internet of Things (ES-IoT) MSc <https://www.ncl.ac.uk/postgraduate/courses/degrees/embedded-systems-internet-of-things-msc/relateddegrees.html..>

PART X. IOT FOR SMART BUILDING AND CITY

35. IOT FOR SMART GRID SAFETY AND SECURITY MANAGEMENT

Prof., DrS E. V. Brezhniev (KhAI)

Contents

Abbreviations	130
35.1 Introduction into smart grid safety and security	131
35.1.1 Challenges in smart grid safety and security in context IoT	131
35.1.2 Analysis of IoT based smart grid and I&C safety factors	134
35.1.3 Nuclear energy's cyber safety and security	138
35.1.4 Selection of smart grid model	144
35.1.5 Features of IoT based smart grid safety and security assessment and assurance	152
35.2 Analysis of smart grid safety and security	154
35.3 IoT based smart grid safety and security management system	156
35.3.1 Structure and goals of IoT based smart grid safety and security management system	156
35.3.2 IoT based smart grid safety and security strategies	159
35.3.3 Safety strategies: redeployment of resources in smart grid	160
35.3.4 Strategy of redistribution with the mandatory allocation of sufficient resources	162
35.3.5 Strategy of redistribution with the possible (but insufficient) resource allocation	165
35.3.6 Cases	169
35.4 Resilience-oriented measurement of quality of IoT based smart grid service assess	171
35.4.1 Method for IoT based smart grid resilience assessment	171
35.4.2 SDOE-based development of resilient digital substation	180
35.5 Work related analysis	184
Conclusions and questions	189
References	192

Abbreviations

ASARP - As Safe As Reasonably Practical
ATHENA - Technique for Human Event Analysis
CCFs - Common Cause Failures
CCCE - Cyber common cause events
CEI – Critical Energy Infrastructure
CRR - Cyber Resilience Review
DO – Degree of Openness
DC – Direct Current
ER – Emergent Risk
FMECA - Failure Mode, Effects and Criticality Analysis
HF – Human Factor
HEP - Human Error Probability
HPP – Hydro Power Plant
IP – Internet protocol
I&C – Information and Control
LR – Local Risk
LC – Life Cycle
LLM – Logic Linguistic Model
NPP – Nuclear Power Plant
OVI - Overall Vulnerability Index
QMS – Quality Management Systems
RVI - Resource Vulnerability Index
RG – Regulatory Guide
SG - Smart Grid
SMS - Safety Management System
SI – Safety Index
SSMS - Safety and Security Sanagement System
SDOE – Secure Development and Operational Environment
SCADA - Supervisory Control and Data Acquisition
TPP – Thermo Power Plant
THERP - Technique for Human Error Rate and Prediction

35.1 Introduction into smart grid safety and security

35.1.1 Challenges in smart grid safety and security in context IoT

IoT is a network of physical objects or things connected to the Internet. Such objects are equipped with embedded technology to interact with their internal and external environments. These objects sense, analyze, control and decide individually or in collaboration with other objects through high speed and two-way digital communications in a distributed, autonomous and ubiquitous manner. This is exactly what is required for the SG.

Hence, IoT technology can help SGs by supporting various network functions throughout the power generation, storage, transmission, distribution and consumption by incorporating IoT devices (such as sensors, actuators and smart meters), as well as by providing connectivity, automation and tracking for such devices [1].

The application of the IoT in SGs can be classified into three types. Firstly, IoT is applied for deploying various IoT smart devices for the monitoring of equipment states. Secondly, IoT is applied for information collection from equipment with the help of its connected IoT smart devices through various communication technologies. Thirdly, IoT is applied for controlling the SG through application interfaces. A SG is comprised of four main subsystems (see Fig.35.1), power generation, power transmission, power distribution and power utilization.

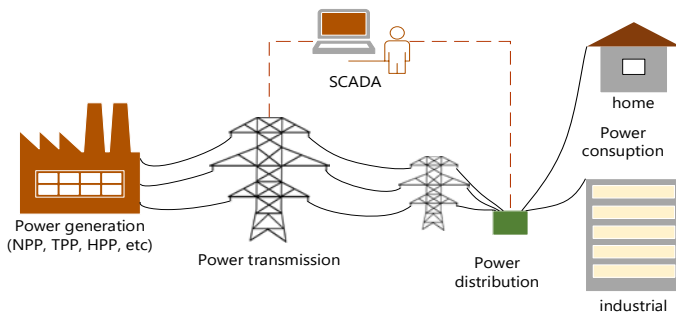


Fig. 35.1 - Four main subsystems of smart grid

IoT can be applied to all these subsystems and appears as a promising solution for enhancing them, making IoT a key element for SG. In the power generation area, IoT can be used for the monitoring and controlling of energy consumption, units, equipment, gas emissions and pollutants discharge, power use/production prediction, energy storage and power connection, as well as for managing distributed power plants, pumped storage, wind power, biomass power and photo-voltaic power plants [2]. In the power transmission area, IoT can be used for the monitoring and control of transmission lines and substations, as well as for transmission tower protection [3], [4]. In the power distribution area, IoT can be used for distributed automation, as well as in the operations and equipment management. In the power utilization area, IoT can be used for smart homes, automatic meter reading, electric vehicle charging and discharging, for collecting information about home appliances energy consumption, power load controlling, energy efficiency monitoring and management, etc.

There are many IoT technologies that are already implemented in the SG, but some are still being on the way. Examples of potential and existing IoT applications in smart grid is given on Fig.35.2 [1].

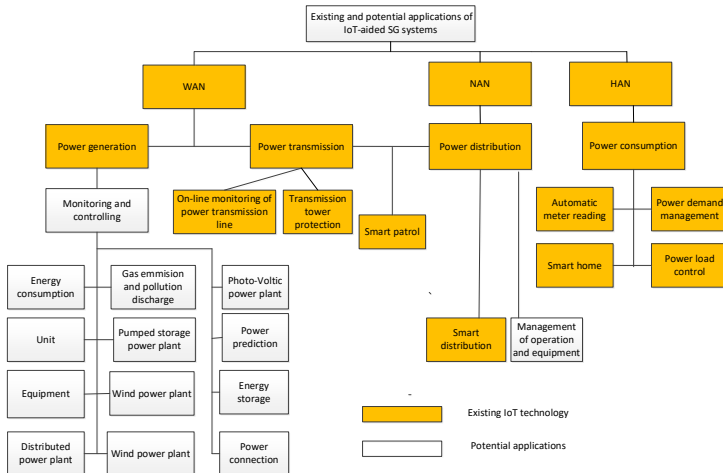


Fig. 35.2 - Examples of potential and existing IoT applications in smart grid

With the dawn of the IoT, the utilities industry and SG systems are poised to enjoy unprecedented benefits. Increased efficiency, reliability, proactive maintenance, and visibility into how energy is consumed are just a few of the promised advantages that IoT will bring to a leveled-up smart grid.

But SG will also face new, complex challenges. There are several challenges that the SG might face, including:

- **Security challenges.** Security is the most important aspect of the SG's IoT future. As more connected devices get added to the grid, it will become increasingly important to make sure they are secure, as each and every device will offer a new avenue for hackers to maliciously exploit;

- **Interoperability.** Ensuring interoperability for connected devices is a must. Effective communication between devices ensures SG resiliency, reliability, and power management and provides greater visibility into grid operations; As embedded devices, IoT technologies are being introduced into SG architecture and this process might lead to new risks to safety of SG;

- **Logistics and scalability.** To increase the efficiency of a SG, the utilities industry needs scalability at the forefront [5].

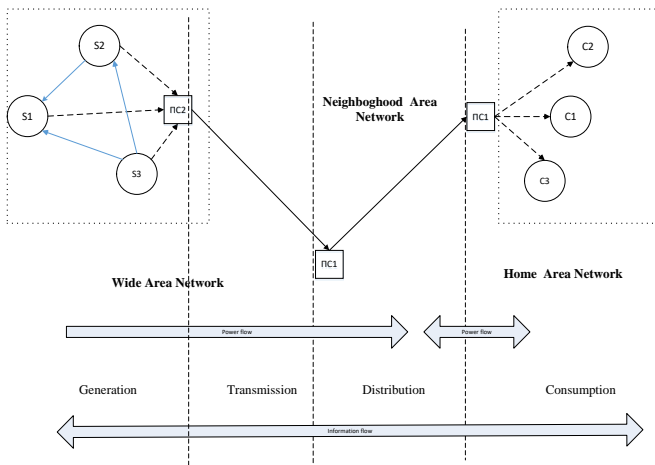


Fig. 35.3 - Information and material flows in IoT based SG

Cyber threats to the SG can also emerge from attacks directed via IoT devices connected to networks. IoT devices have been increasingly targeted by botnet malware (whereby the hacker takes over the operation of a large number of infected devices) to launch denial-of-service or other cyberattacks.

If such IoT cyberattacks were able to access electric utility operational or industrial control systems, they could potentially impair these systems or cause electric power networks to operate based on manipulated conditions or false information.

35.1.2 Analysis of IoT based smart grid and I&C safety factors

SG safety is affected by many factors regarding its design, manufacturing, installation, commissioning, operation and maintenance. Consequently, it may be extremely difficult to construct a complete mathematical model in order to assess the safety because of inadequate knowledge about the basic failure events.

This leads inevitably to problems of uncertainty in SG safety assessment.

The SG is a very complex system. It is characterized by huge number of nodes and links between nodes with increasing structural complexity; links between nodes could change over time, have different weights, directions, etc.

There are a lot of risks as the inherited essences of SG life cycle. Due to high complexity, its dynamic nature these risks are not static. Moreover, SG life cycle is characterized by complicated risk flow when safety and reliability issues might endanger the cyber security and vice versa.

The risk associated with SG weakest link could compromise the safety and reliability of SG as a whole.

Main safety factors of IoT based Smart Grid and their relationship are shown in Fig.35.4.

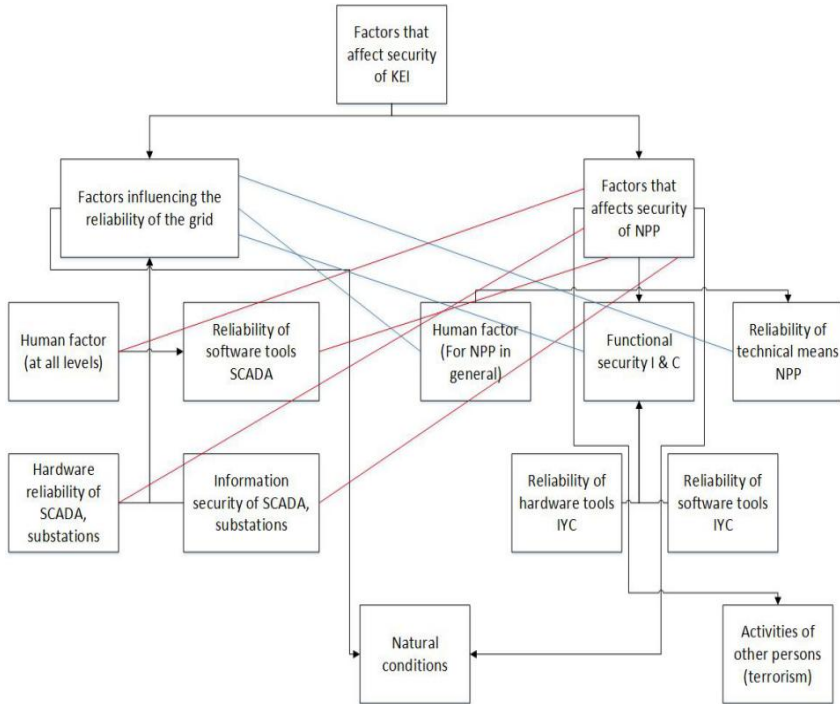


Fig. 35.4 - Main safety factors of IoT based SG and their relationship

A. Natural factors influence analysis

Analysis of the IoT based SG's accidents and failures causes confirms the vulnerability of its assets to the effects of natural factors (earthquakes, volcanic eruptions, landslides, etc.) due to:

- centralized architecture,
- geographic distribution,
- balancing between generation and demand, and
- the complexity of integrating alternative sources, etc.

Fig.35.5 shows main causes of accidents and failures in the IoT based SG work that occurred over the past 10 years.

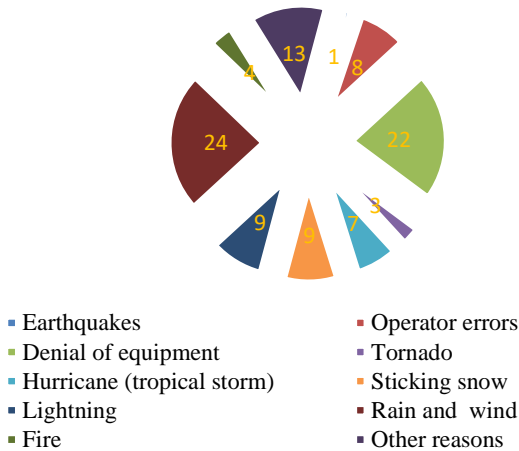


Fig. 35.5 - Main causes of the IoT based Smart Grid major crashes

The main methods that take into account the natural factors influence include: risks indexation method, environmental impact assessment, geospatial analysis, hazard mapping, historical analysis, etc.

Risks indexation method is a qualitative approach that allows monitoring the risks for the public at the national level. The disadvantage of the method is simplification and usage of averaged data, which prevents a specific assessment for a specific region.

Environmental impact assessment is a mean of supporting decisions to assess the impact of companies on the infrastructure vulnerability to natural disasters. The disadvantage of the method is the focus on post-event analysis of the natural disasters consequences. The approach is not integrated into the disaster management planning process.

There are also approaches to mapping hazards. The advantage of the method is the visualization of information for decision-making. A disadvantage is a large amount of necessary information, which leads to the need to use computing support.

Geospatial analysis is used to compile a map of hazards at different levels: local (less than 100000 km², regional - 100000 - 10000000 km², and continental (10000000 - 100000000 km²). In

addition, different predisposition to risk levels are considered. The disadvantage of the method is the possibility of using it only for predefined geographical areas.

Historical analysis is based on the use of historical information about the natural disasters area. The method is based on weighing different aspects of vulnerabilities. The disadvantage is the high requirements for the database of historical events, which also needs support (filling, evaluation of reliability, etc.)

All approaches make it possible to identify the risks nature and assess their impact on the IoT based Smart Grid security. At the same time, safety assessment is a complex task which solution must be based on the general consideration of the whole safety factors set, including the human factor (HF).

B. Human factor influence analysis

IoT based SG consists of sophisticated human-machine systems, in which the impact of HR on reliability and security is determinational at any level of its hierarchy.

There are many approaches to human-operator reliability assessment in many areas of their activities, primarily related to security. The main approaches to incorporating HF [6-9] into IoT based Smart Grid security analysis include:

- Human Error Probability (HEP) quantitative methods;
- holistic and decomposition methods.

Holistic models are used to assess the human operator's overall performance without breaking them into small sub-actions, as suggested by using the Technique for Human Error Rate and Prediction (THERP) and Technique for Human Event Analysis (ATHENA). Decomposition methods consider the human functions quality as a combination of sub-actions.

Thus, the provided analysis allows us to make such conclusions:

1. HR is a major risk factor for IoT based SG and I&C security assessments. Its influence occurs not only during the life cycle, but also at all levels of the hierarchy, that means there is HF impact hierarchy on security.

2. HR can also be decomposed into an individual, collective, and organizational level.

3. In all methods of HF analysis, the main attention is paid to the negative human influence in the transitional and post-revolutionary periods. The HF impact occurs throughout the life cycle of the IoT based Smart Grid and I&C. Human reliability analysis methods are most developed for atomic energy.

35.1.3 Nuclear energy's cyber safety and security

Nuclear energy occupies a unique position in the debate over global climate change as the only carbon-free energy source. Nowadays it is already contributing to world energy supplies on a large scale, and has potential to be expanded if the challenges of:

- safety,
- nonproliferation,
- waste management and
- economic competitiveness

are addressed and technologically fully mature.

So it might be concluded that Nuclear Power Plants (NPP) are an intrinsic part of future IoT based SG. I&C NPP will be communicating with other I&Cs of SG power generation facilities.

Risk is an inevitable factor throughout the life cycle of the smart grid and I&C NPP. Risk $R(t)$ is estimated as follows

$$R(t) = P(t) \times S(t),$$

where $P(t)$ – adverse event (failure, accident) occurrence probability caused by negative interactions between SG systems (subsystems) of the I&C NPP;

$S(t)$ – adverse event (accident, failure) consequences severity in the I&C NPP measured in terms of damage (economic, health and people life, etc.).

Within the IoT based Smart Grid, risk decomposition can be done by the levels of its hierarchy (Fig.35.6). Let's highlight the main risk groups in the IoT based Smart Grid (table 35.1).

The risks on the IoT based Smart Grid are the sum of systems LR that were not reduced during the design process, as well as ER $R_{CI}^{emerg}(t)$, due to negative interactive systems when they are combined within the IoT based Smart Grid:

$$R_{CI}(t) = \sum_{h=1}^H \beta_h R_{CI}^h(t) + \sum_{i=1}^N \alpha_i R_i(t),$$

where $R_{CI}^h(t)$ – ER h-th type, $R_{CI}^{emerg}(t) = \sum_{h=1}^H \beta_h R_{CI}^h(t)$;

$R_i(t)$ – LR i-th asset SG system;

$$R_{S_i}^{Closed}(t) = \sum_{i=1}^N \alpha_i R_i(t); \alpha_i, \beta_h - \text{risk priorities } \alpha_i, \beta_h \in [0,1].$$

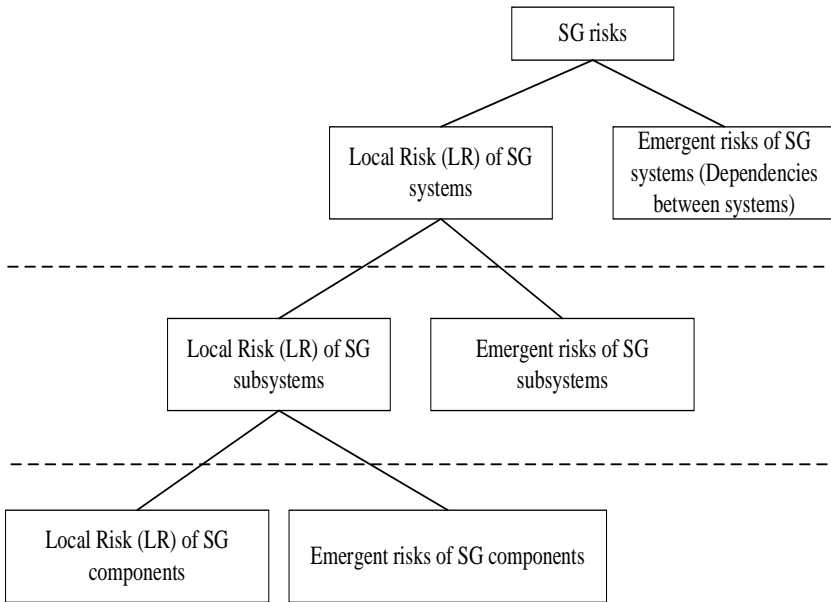


Fig. 35.6 - Hierarchical risk structure in IoT based Smart Grid

Table 35.1 - Major Risk Groups in the IoT based Smart Grid Hierarchy

Types of risks on IoT based Smart Grid	Notation
EP systems	
Risks due to the negative geographic impact between IoT based Smart Grid systems	$R_{CI}^{geogr}(t)$
Risks due to negative informational influence between IoT based Smart Grid systems	$R_{CI}^{inform}(t)$
Risks due to negative physical effects between IoT based Smart Grid systems	$R_{CI}^{physic}(t)$
Risks due to the negative organizational influence between IoT based Smart Grid systems	$R_{CI}^{organiz}(t)$
Risks due to negative logic influence between IoT based Smart Grid systems	$R_{CI}^{logic}(t)$
Risks of using inaccurate (inadequate) models	$R_{model}(CI)$
The risks of not accounting for uncertainties	$R_{uncertain}(CI)$
Type of Local Risks	
Risks related to physical assets (hardware): – hardware;	$R_{hard}(S_i)$
– electric cables; – peripheral measuring equipment (sensors);	$R_{ecabl}(S_i)$ $R_{sensor}(S_i)$
– substations and transformers, etc.	$R_{substr}(S_i)$
Risks associated with organizational assets of systems (Management, Organizational Risks): – culture of safety; – imperfect security policies.	$R_{organ}(S_i)$
Risks of multiple failures of IoT based Smart Grid assets:	$R_{MF}(S_i)$ $= R_{CFF}(S_i) \cup R_{casc}(S_i)$

Types of risks on IoT based Smart Grid	Notation
– Common Cause Failure (CCF) risks;	
– risks of cascading accidents.	$R_{\text{cascad}}(S_i)$
Risks of using non-accurate security models	$R_{\text{model}}(S_i)$
Risks not taking into account uncertainties	$R_{\text{uncertain}}(S_i)$
Emergent risks for systems due to the interplay between their subsystems	$R_{S_i}^{\text{emerg}}(t)$
Local risks for subsystem (I&C level)	
Risks associated with information assets (I&C software and hardware). Functional I&C safety risks	$R_{I\&C_q^i}(t) = R_{I\&C_q^i}^{\text{hard}}(S_i) \cup R_{I\&C_q^i}^{\text{soft}}(S_i)$
Risks caused by interfacing I&C subsystems (by Emergent risks)	$R_{I\&C_i}^{\text{emerg}}(t) = R_{I\&C_q^i}^{\text{inf}}(\bar{S}_i) \cup R_{I\&C_q^i}^{\text{geogra}}(\bar{S}_i) \cup R_{I\&C_q^i}^{\text{log}}(\bar{S}_i) \dots$
Risks associated with organizational assets (management, organizational risks)	$R_{\text{organ}}(I \& C_q^i)$
The risks of multiple I&C failures: – CCF risks, – risks of cascade failures of assets.	$R_{\text{MF}}(I \& C_q^i)$ $= R_{\text{CCF}}(I \& C_q^i)$ $R_{\text{casc}}(I \& C_q^i)$
Risks of using inaccurate I&C security models	$R_{\text{model}}(I \& C_q^i)$
The risks of not accounting for uncertainties	$R_{\text{uncertain}}(I \& C_q^i)$

The closed system risks set and its risks within the IoT based smart grid set differ from each other. This is due to the presence of ER in the IoT based SG, that is:

$$R_{CI}^{emerg}(t) = \sum (R_{CI}^{physic}(t) + R_{CI}^{inform}(t) + R_{CI}^{organiz}(t) + \dots + R_{CI}^{logic}(t)).$$

The dependencies between the safety and reliability levels on the IoT based Smart Grid is shown on Fig.35.7. IoT based Smart Grid security is determined by the security of the NPP and the SG reliability. The NPP's safety is determined by the functional safety and I&C cyber security. SG reliability is determined by its equipment reliability, as well as its smart devices and components information security.

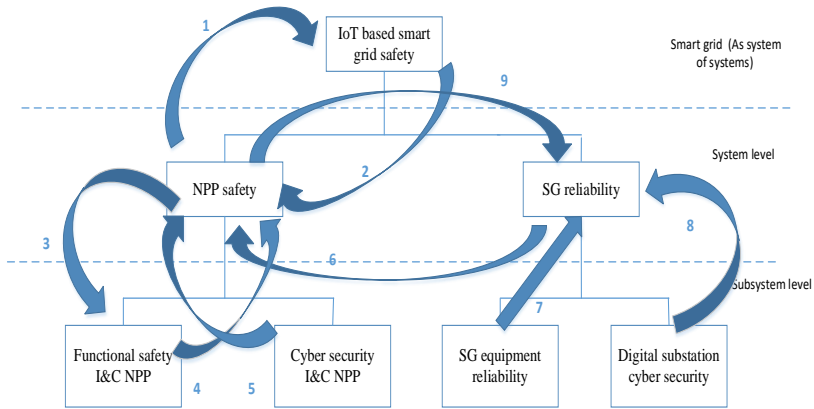


Fig. 35.7 - Dependencies between safety and reliability levels on IoT based Smart Grid

Table 35.2 - Interoperability description

Marking	Comment
$SI_{NPP}(t) \rightarrow SI_{CI}(t)$	Security of the NPP (System) determines the security of the IoT based Smart Grid
$SI_{CI}(t) \rightarrow SI_{NPP}(t)$	Security IoT based Smart Grid ensures the safety of the NPP
$SI_{NPP}(t) \rightarrow FSI_{I\&C^i}(t)$	Safety of NPPs determines functional safety of I&C NPP
$FSI_{I\&C^i}(t) \rightarrow SI_{NPP}(t)$	Functional safety I&C NPP determines safety NPP
$CSI_{I\&C^i}(t) \rightarrow SI_{NPP}(t)$	Information security I&C NPP determines safety NPP
$RI_{grid}(t) \rightarrow SI_{NPP}(t)$	The reliability of the grid (system) determines safety NPP (system)
$RI_{subst}(t) \rightarrow RI_{grid}(t)$	The reliability of the substation (subsystem) determines the reliability of the grid (system)
$CSI_{subst}(t) \rightarrow RI_{grid}(t)$	Information security of the substation (subsystem) determines the reliability of the grid (system)
$SI_{NPP}(t) \rightarrow RI_{grid}(t)$	NPP safety determines the reliability of grid (systems)

If risk management strategies do not ensure their reduction, it leads to their transfer to the level of the systems, in particular, for the NPP, $R_{S_i}^{emerg*}(t) \rightarrow R_{NPP}(t)$. Then ER, due to interconnected power supply and NPP, can be transferred to NPP: $R_{grid}(t) \rightarrow R_{NPP}(t)$, which causes a decrease in safety (for example, due to a loss of power supply).

I&C risks $R_{I\&C^i}(t)$ are formed by combining sets of NPP risks

$R_{NPP}(t)$ risks of functional I&C safety $R_{I\&C_i^i}(t)$, risks $R_{CI}^{emerg*}(t)$, which have not been reduced at the level of IoT based Smart Grid systems, as well as the risks inherent in I&C subsystems interacting $R_{I\&C_i}^{emerg*}(t)$:

$$R_{I\&C_i}(t) = R_{NPP}(t) \cup R_{I\&C_i}^*(t) \cup R_{I\&C_i}^{emerg*}(t) \cup R_{CI}^{emerg*}(t).$$

I&C risks can be transferred to other NPP systems, so $R_{I\&C} \rightarrow R_{NPP}$.

This results in an increase in all LR NPPs associated with its equipment failure. Thus, there are dependencies at all levels of the IoT based Smart Grid: the negative interaction of safety states causes the ER appearance; IoT based Smart Grid asset hierarchy allows you to depict a hierarchy of risks: ER IoT based Smart Grid – system risks – I&C risks; risk reduction is possible due to ER reduction.

35.1.4 Selection of smart grid model

Formalized IoT based SG can be represented as a hierarchy. The main levels include:

- **SG level** (first level), which contains different systems: systems generating (NPP, TPP, alternative generation sources, etc.) (S1), services delivery (S2), services distribution (S3), etc.;
- **subsystem level** (second level), for example, for NPP (as systems), subsystems are normal operation systems, subsystems of distribution and transmission, etc.

SG hierarchical representation is shown in Fig.35.8. If necessary, the levels of components and elements can be considered.

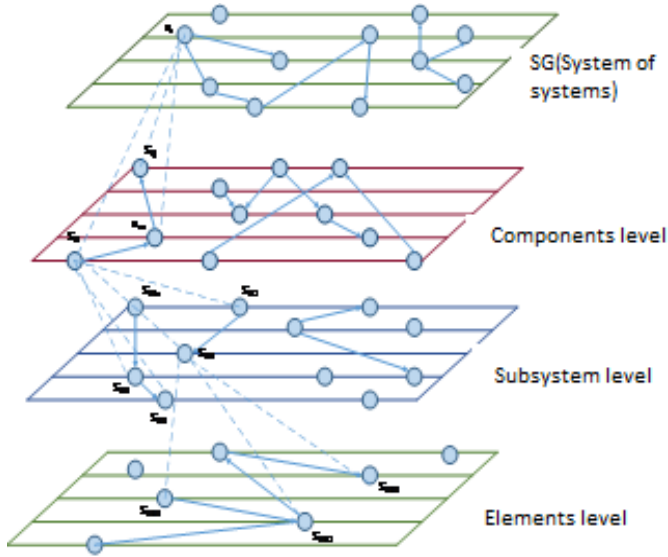


Fig. 35.8 - SG hierarchical representation

The nodes of each level of IoT based SG are interconnected by $I_{geo}^{NPP}(t)$ connections (influences) $I(t)_h^{CI}(S_i \rightarrow S_j)$ different types, namely:

$$I(t)_h^{CI}(S_i \rightarrow S_j) \in \{I(t)_{geo}^{CI}(S_i \rightarrow S_j), I_{geo}^{CI}(t)(S_i \rightarrow S_j), I_{phys}^{CI}(t)(S_i \rightarrow S_j), I_{org}^{CI}(t)(S_i \rightarrow S_j), I_{inf\ om}^{CI}(t)(S_i \rightarrow S_j), I_{log}^{CI}(t)(S_i \rightarrow S_j)\},$$

where $I_{geo}^{CI}(t)(S_i \rightarrow S_j)$ – geographic impact due to the spatial closeness SG systems, which leads to an increase in ER associated with the spread of the effects of accidents between systems;

$I_{phys}^{CI}(t)(S_i \rightarrow S_j)$ – physical impact due to flows of material resources (for example electricity) between systems; loss of which leads to an increase in ER associated with sources of supplies of resources, resources, energy;

$I_{org}^{CI}(t)(S_i \rightarrow S_j)$ – organizational impact due to the impact of staff errors of one system on the safety of another system on the IoT based

Smart Grid;

$I_{inform}^{CI}(t)(S_i \rightarrow S_j)$ – information interactions associated with the flows of information (data) between information assets IoT based Smart Grid;

$I_{icg}^{CI}(t)(S_i \rightarrow S_j)$ – logical influence associated with the logic of the functioning of systems.

The IoT based Smart Grid model has a graph like:

$$G = (X, V),$$

where X – set of systems $X = \{S_i\}_I$;

$V = \{I(t)_h^{CI}(t)(S_i \rightarrow S_j)\}_H$.

Thus, IoT based Smart Grid can be presented as a hierarchical graph, where each i -th node of the j -th level of the hierarchy can also be represented as a subgraph of the form:

$$G_{ij} = \{(X_{ijs})_{is}, (V_{kij})_{kj}\},$$

where $(X_{ijs})_{is}$ – s -th subsystem of the i -th system (node) of the j -th level of the hierarchy; $j = \overline{1, J}$, $s = \overline{1, S}$;

$(V_{kij})_{kij}$ – k -th rib of the i -th system of the j -th level of the hierarchy, $k = \overline{1, K}$, which is a kind of mutual influence.

Among the whole set of subsystems a subset is allocated I & C $\{I \& C_q^i\}_Q$, connected with other subsystems by information links $I(t)_{inform}^{CI}(S_i \rightarrow S_j)$.

The NPP as a part of SG interacts with other elements of SG. All influences (or relationships) existed in SG could be divided into several hierarchy's levels.

The influences between different systems of IoT based Smart Grid could be described (or formalized) by means of the Influence vector. The *Influence vector* is characterized by the value and direction. The direction points the initial influence source and systems being under influence. The value characterizes the strength of influence.

The influences between NPP and IoT based Smart Grid systems could be represented by a matrix of influence shown in the table 35.3:

Table 35.3 - Matrix of influence

	NPP	TPP	HPP
NPP	-	M	H
TPP	L	-	
HPP	M		-

The influence matrix shows how elements of the system influence each other and strength of their influence. As an example, NPP influences TPP with a strength – medium and HPP with high level of influence. Generally, influence is an ability of one system to determine the state, characteristics and behavior of other systems.

To evaluate the influences between NPP and SG systems we need to have the metrics by which this influence could be measured and compared. Two types of metrics are suggested: linguistic and numerical. The linguistic metric operates with the linguistic values used to evaluate the strength of influence.

The different values as high, medium and low are applied to consider and predict the smart grid's system state changing provided the accident in other SG systems occurred. Numerical values, as ranks, are used in the similar way, and the different ranks stand for the different strength of influence. Expert judgments are considered as the basis for taking the influence values. The influence database is completed for each NPP. These values are regularly updated.

NPP could influence the IoT based SG in the different ways, such as physical, geographical, organizational, by means of information, logical, societal, etc. Thus, we introduce the space of influence. Physical, geographical, organizational, informational, logical, societal is a particular influence.

Total influence might be represented as:

$$I_t^{NPP} \left(I_{geo}^{-NPP}(t), I_{phys}^{-NPP}, I_{org}^{-NPP}, I_{soc}^{-NPP}, I_{log}^{-NPP}(t) \right),$$

where $\bar{I}_{phys}^{-NPP}(t)$ – a physical reliance on materials flow between NPP and other SG systems;

$\bar{I}_{inf}^{-NPP}(t)$ – a reliance on information transfer between NPP and other elements of SG (via I&C systems);

$\bar{I}_{geo}^{-NPP}(t)$ – a local environmental event affects components of NPP-SG (usually the transmission lines) due to physical proximity;

$\bar{I}_{log}^{-NPP}(t)$ – an influence that exists between NPP - SG that does not fall into one of the about categories;

$\bar{I}_{org}^{-NPP}(t)$ – organizational influences through policy, regulation, markets;

$\bar{I}_{soc}^{-NPP}(t)$ – influences that SG components may have on public opinion, fear and confidence.

The total influence is a time dependable value. The changes of NPP states and characteristics stipulate the changes of the total influence value.

Formally, the geographical influence of NPP on other systems of SG might be written as:

$$\begin{aligned} \bar{I}_{geo}^{-NPP}(t) &= \{I_{geo}(NPP \rightarrow TPP), I_{geo}(NPP \rightarrow HPP), I_{geo}(NPP \rightarrow TG)\} = \\ &= \{\text{Medium}(M), \text{High}(H), \text{Low}(L)\}. \end{aligned}$$

The value of geographical influence could be calculated as:

$$I_{geo}^{-NPP} = \sum_{i=1}^l I_{geo}^i(NPP \rightarrow SPG_i) = H + M + L.$$

The value of organizational influence could be calculated as:

$$I_{org}^{-NPP} = \sum_{i=1}^l I_{org}^i(NPP \rightarrow SPG_i);$$

$$I_{org}^{-NPP} = \sum_{i=1}^l I_{org}^i(NPP \rightarrow SPG_i) = M + L + M.$$

The total influence value might be calculated as a sum of the particular influence values on all influence space existed for NPP-SG system.

The total influence value calculated as a sum of the particular influence values characterizes the absolute influence of NPP on other SG systems. For each systems of power grid could be evaluated their total influences. Their ranking might determine the most and least influential system.

In table 35.4 the different influences' factors are combined.

Table 35.4 - The combined matrix of influences

	Physical				Geographical				Informational			
	NPP	TPP	HPP	DG	NPP	TPP	HPP	DG	NPP	TPP	HPP	DG
NPP	0	M	L	H	0	H	M	L	0	M	H	M
TPP	M	0	M	L	H	0	M	L	H	0	H	H
HPP	L	H	0	H	H	L	0	H	H	L	0	H
DG	L	L	H	0	L	M	M	0	L	M	H	0

It helps to estimate the value of total influence, for instance, NPP on all of subsystems as:

$$I_t^{NPP} \left(I_{geo}^{-NPP}(t), I_{phys}^{-NPP}, I_{org}^{-NPP}, I_{soc}^{-NPP}, I_{log}^{-NPP}(t) \right).$$

$$I_{tot}^{NPP} \left(\bar{I}_{phys}^{-NPP}(t), \bar{I}_{geo}^{-NPP}(t), \bar{I}_{org}^{-NPP}(t), \bar{I}_{inf}^{-NPP}(t), \dots, \bar{I}_{soc}^{-NPP}(t) \right) - \text{total NPP's inf lueuce};$$

$$\bar{I}_{phys}^{-NPP}(t) = \sum_{i=1}^I I_{phys}^i(NPP \rightarrow SPG_i); \bar{I}_{geo}^{-NPP}(t) = \sum_{i=1}^I I_{geo}^i(NPP \rightarrow SPG_i), \dots;$$

$$I_{tot}^{NPP} = w_{phys}(H + M + L) + w_{geo}(M + L + H) + w_{org}(M + H + L) + \dots,$$

$SPG_i - S_i$ of smart grid.

We shall consider the relative influence value $I_{rel}(t)$. The relative influence value determines the influence of one system on another system, for example NPP on TPP. It might be calculated as:

$$I_{rel}(NPP \rightarrow TPP) = I_{geo}(NPP \rightarrow TPP) + I_{org}(NPP \rightarrow TPP) + \dots + I_{soc}(NPP \rightarrow TPP).$$

It is worth to note that:

$$I_{tot}^{NPP} = \sum_{i=1}^I I_{rel}(NPP \rightarrow SPG_i).$$

In the case when this value exceeds the certain value $I_{rel}^{lim}(S_1 \rightarrow S_2)$, it might lead to state changing of S_2 .

The IoT based Smart Grid could be characterized by some values shown in table 35.5.

Table 35.5 - The characteristics of influences

Relation	Current Influence	Influence limit
$TPP \rightarrow NPP$	$I_{rel}(TPP \rightarrow NPP)$	$I_{rel}^{lim}(TPP \rightarrow NPP)$
$TPP \rightarrow T \& D$	$I_{rel}(TPP \rightarrow T \& D)$	$I_{rel}^{lim}(TPP \rightarrow T \& D)$
$NPP \rightarrow T \& D$	$I_{rel}(NPP \rightarrow T \& D)$	$I_{rel}^{lim}(NPP \rightarrow T \& D)$
$NPP \rightarrow TPP$	$I_{rel}(NPP \rightarrow TPP)$	$I_{rel}^{lim}(NPP \rightarrow TPP)$

In this case the conditions of safety for NPP – IoT based Smart Grid based on the balance of influence might be written as:

$$I_{rel}(TPP \rightarrow NPP) \leq I_{rel}^{lim}(TPP \rightarrow NPP);$$

$$I_{rel}(TPP \rightarrow T \& D) \leq I_{rel}^{lim}(TPP \rightarrow T \& D) ;$$

$$I_{rel}(NPP \rightarrow T \& D) \leq I_{rel}^{lim}(NPP \rightarrow T \& D);$$

$$I_{rel}(NPP \rightarrow TPP) \leq I_{rel}^{lim}(NPP \rightarrow TPP) .$$

Then the current value of influence between infrastructures exceeds the acceptable value, it could result to the state changing of one of them. The Fukushima nuclear accident proved this principle of the balance influence.

FMECA might be very helpful technique for formalization of influences to help performing NPP safety analysis. Traditionally the criticality assessment is performed by calculating the failures criticality as a product of failure severity and frequency:

$$Crt(S_i) = Fr(S_i) \times Sev(S_i),$$

where S_i – NPP (smart grid) accident, $Fr(S_i)$ – accident frequency; $Sev(S_i)$ – severity of accident's consequences.

The traditional FMECA is two dimensional. In the case when $Crt(S_1) = Crt(S_2)$ we need to use additional information to differ possible accidents.

Therefore the total influence I_{tot}^S characterized by direction and strength might be used as third value to prioritize the possible accident. The criticality is assessed as

$$Crt(S_i) = Fr(S_i) \times Sev(S_i) \times I_{tot}^S.$$

Taking into consideration the mutual influences between NPP and power grid we assume the failure criticality of NPP (smart grid) might be changed as a result of the criticality changing of smart grid (NPP). We introduce the conditional criticality presented as

$$I(S_i^* \rightarrow S_j): Crt(S_i|S_j^*) = Fr(S_i|S_j^*) \times Sev(S_i|S_j^*)$$

where $Crt(S_i|S_j^*)$ – conditional criticality of S_i provided the failure of S_j^* ;

$Fr(S_i|S_j^*)$ – S_i frequency changing provided the failure of S_j^* ;

$Sev(S_i|S_j^*)$ S_i severity changing provided the failure of S_j^* .

Any accident or failure of smart grid system leads to the change of criticality of all related systems. When a failure of one system occurs, our approach recalculates the criticalities of all dependent systems. In case of criticalities growth, when it goes through the diagonal of criticality matrix and reaches its margin values, some actions should be taken to decrease criticality and improve the smart grid safety.

35.1.5 Features of IoT based smart grid safety and security assessment and assurance

IoT based Smart Grid is considered as a set of systems $\{S_i\}_I$, their I&C system (subsystems) $\{I \& C_q^i\}_Q$ and the h-type bonds (mutual influences) $I(t)_h^{CI}(S_i \rightarrow S_j)$ between the systems.

It is important to note that interactions occur at all levels of the IoT based Smart Grid, at the subsystem level, as well as at the system-subsystem level, that is $I(t)_h^{Si}(\bar{S}_{ik} \rightarrow \bar{S}_{lm}), I(t)_h^{Si}(S_i \rightarrow \bar{S}_{ik})$

The main means of monitoring system security is I&C $\{I \& C_q^i\}_Q$. Between security states I&C systems subsystems are also mutually influential $I(t)_h^{I\&Cq}(\bar{S}_{ik} \rightarrow \bar{S}_{jl})$.

IoT based Smart Grid is characterized by security (safety index, SI), $SI_{CI}(t)$, the cost of systems (subsystems) (C) (M, resources to boost SI and risk reduction), as well as reliability indicators $RI_{S_i}(t)$. I&C system is characterized by indicators functional safety $FSI_{I\&C}(t)$. There is an interconnection between the IoT based Smart Grid security features and the functional I&C system safety. Systems S_i (subsystems \bar{S}_{ij}) are characterized by a state of safety $\{St_1^{S_i}(t)\}_L (\{St_g^{S_j}(t)\}_G)$.

The value of the current SI of the IoT based Smart Grid does not match the required value $SI_{CI}^{req}(t), SI_{CI}(t) \notin \Omega_{SI_{CI}^{accept}}(t)$. The current risks of IoT based Smart Grid do not match their acceptable value, $R_{CI}(t) \notin \Upsilon_{R_{CI}^{accept}}$ where Υ - set of acceptable risks. IoT based Smart Grid SI

meets the required value only when the current IoT based Smart Grid risks $R_C(t)$ are acceptable, i.e.

$$SI_{CI}(t) = SI_{CI}^{Accept}(t) \Leftrightarrow R_{CI}(t) = R_{CI}^{accept}(t).$$

The risks of IoT based Smart Grid are determined by the local (own) system risks $R_{S_i}^{Closed}(t)$ and emergent risks $R_{CI}^{emerg}(t)$, caused by the negative impact between systems on the IoT based SG. The individual target function of the i -th system in the IoT based SG has the form:

$$f_{s_i}(x) \rightarrow \max, \varphi_i(x) \leq 0, i = \overline{1, m}, x \in X,$$

where X - set of alternatives to achieve the goal;

$f : X \rightarrow \mathbb{R}$ and $\varphi : X \rightarrow \mathbb{R}$ - specified functions.

Target independence between IoT based Smart Grid systems is recorded as:

$$\{f_{s_i}(X), f_{s_j}(Y), \mu(f_{s_i}(X)f_{s_j}(Y) = 0) \wedge \{X, Y, \mu(X, Y) = 0\}\}.$$

Safety dependence looks like:

$$\{St_g^{S_i}(t), St_g^{S_j}(t), \mu(St_g^{S_i}(t), St_g^{S_j}(t)) \neq 0\}.$$

The I&C system is characterized by risks that may be greater (less) than acceptable I&C system risks $R_{I\&C_q^i}(t) <> R_{I\&C_q^i}^{accept}(t)$.

Safety dependency between IoT based Smart Grid and I&C system looks like:

$$\{St_g^{S_i}(t), St_k^{I\&C_q^i}(t), \mu(St_g^{S_i}(t), St_k^{I\&C_q^i}(t)) \neq 0\}.$$

Between the risks $R_{I\&C_q^i}(t)$ and $R_{CI}(t)$ there is an interconnection, i.e.: $R_{I\&C_q^i}(t) \subseteq R_{CI}(t), R_{CI}(t) \subseteq R_{I\&C_q^i}(t)$.

So,

$$\begin{aligned}
 1) CI &= \{ \{S_i\}_I, \{I \& C_q\}_Q, \{\bar{S}_{ij}\}_J, I(t)_h^{CI} (S_i \rightarrow S_j), I(t)_h^{Sij} (\bar{S}_{ik} \rightarrow \bar{S}_{lm}), I(t)_h^{Si} (S_i \rightarrow \bar{S}_{ik}) \}, \\
 \exists SI_{CI}(t) &\notin \Omega_{SI_{CI}^{accept}(t)}, \exists R_{CI}(t) \notin \Upsilon_{R_{CI}^{accept}(t)}, \exists C_{CI}(M_{CI}) \in \Omega_{accept}; \\
 I \& C_q &= \{ \{\bar{S}_{ij}\}, I(t)_h^{I\&C_q} (\bar{S}_{ik} \rightarrow \bar{S}_{jl}) \}, \exists SI_{I\&C_q}(t) \notin \Omega_{SI_{I\&C_q}^{accept}(t)}, \exists R_{I\&C_q}(t) \notin \Upsilon_{R_{I\&C_q}^{accept}(t)}.
 \end{aligned}$$

It is necessary to ensure an acceptable level of SI IoT based Smart Grid by identifying, evaluating and reducing the ER by diversifying the systems (subsystems) on the IoT based Smart Grid and redistributing resources, which ensures that the ER is reduced to an acceptable level:

$$\begin{aligned}
 2) CI^* &= \{ \{S_i^*\}_I, \{\bar{S}_{ij}^*\}_J, I^*(t)_h^{CI} (S_i^* \rightarrow S_j^*), I^*(t)_h^{Sij^*} (\bar{S}_{ik}^* \rightarrow \bar{S}_{lm}^*), I^*(t)_h^{Si^*} (S_i^* \rightarrow \bar{S}_{ik}^*) \}, \\
 \exists SI_{CI^*}(t) &\in \Omega_{SI_{CI^*}^{accept}(t)}, \exists R_{CI}(t) \in \Upsilon_{R_{CI}^{accept}(t)}; \exists C_{CI^*}(M_{CI^*}) \in \Omega_{accept} \\
 I \& C_q^* &= \{ \{\bar{S}_{ij}^*\}, I^*(t)_h^{I\&C_q^*} (\bar{S}_{ik}^* \rightarrow \bar{S}_{jl}^*) \}, \exists SI_{I\&C_q^*}(t) \in \Omega_{SI_{I\&C_q^*}^{accept}(t)}, \exists R_{I\&C_q^*}(t) \in \Upsilon_{R_{I\&C_q^*}^{accept}(t)}.
 \end{aligned}$$

At the same time, the reduction of infrastructure risks should not increase the risk for I&C and reduce its functional safety.

The complex of risk reduction measures (diversification and redistribution) in IoT based Smart Grid is limited by resources $C_{CI}(M_{CI}) \in \Omega_{accept}$.

35.2 Analysis of smart grid safety and security

According to [10, 11] generic vulnerabilities of smart grid which might lead to emergency situation specific areas (safety and security) are the following:

1. **Increasing Dependence and Interdependence** between SG systems.

2. **Natural events and accidents.**

3. **Blunders, errors, and omissions.** By most accounts, incompetent, inquisitive, or unintentional human actions (or omissions) cause a large fraction of the system incidents that are not explained by natural events and accidents.

4. **Insiders.** Normal operation demands that a large number of people have authorized access to the facilities or to the associated information and communications systems. If motivated by a perception

of unfair treatment by management, or if suborned by an outsider, an "Insider" could use authorized access for unauthorized disruptive purposes.

5. **Recreational hackers.** For an unknown number of people, gaining unauthorized electronic access to information and communication systems is the most fascinating and challenging game.

6. **Criminal activity.** Some people are interested in personal financial gain through manipulation of financial or credit accounts or stealing services. In contrast to some hackers, these criminals typically hope their activities will never be noticed, much less attributed to them.

7. **Industrial espionage.** Some firms can find reasons to discover the proprietary activities of their competitors, by open means if possible or by criminal means if necessary. Often these are international activities conducted on a global scale.

8. **Terrorism.**

9. **National intelligence.** Most, if not all, nations have at least some interest in discovering what would otherwise be secrets of other nations for a variety of economic, political, or military purposes.

10. **Information warfare.** Both physical and cyber attacks on our infrastructures could be part of a broad, orchestrated attempt to disrupt a major US military operation or a significant economic activity.

Thus, IoT application stipulates an appearance of **specific smart grid vulnerabilities**, such as:

1. **Customer security:** Smart meters autonomously collect massive amounts of data and transport into the utility company, consumer, and service providers. This data includes private consumer information that might be used to infer consumer's activities, devices being used, and times when the home is vacant.

2. **Greater number of intelligent devices:** A smart grid has several intelligent devices that are involved in managing both the electricity supply and network demand. These intelligent devices may act as attack entry points into the network.

3. **Physical security:** Unlike the traditional power system, smart grid network includes many components and most of them are out of the utility's premises. This fact increases the number of insecure physical locations and makes them vulnerable to physical access.

4. **The lifetime of power systems:** Since power systems coexist with the relatively short lived IT systems, it is inevitable that outdated

equipments are still in service. This equipment might act as weak security points and might very well be incompatible with the current power system devices.

5. ***Implicit trust between traditional power devices***: Device-to-device communication in control systems is vulnerable to data spoofing at the points where the state of one device affects the actions of another. For instance, a device sending a false state makes other devices behave in an unwanted way.

6. ***Using Internet Protocol (IP) and commercial off-the-shelf hardware and software***: Using IP standards in smart grids offer a big advantage as it provides compatibility between the various components. However, devices using IP are inherently vulnerable to many IP-based network attacks such as IP spoofing, Tear Drop, Denial of Service, and others.

It is worth noting that the new challenge which is stipulated by IoT application is **cyber common cause events (CCCE)**.

CCCEs might be determined as events when:

- cyber assets' availability,
- confidentiality and
- integrity

(of one system or different systems with the same functionalities) are compromised within a specified (short) time interval.

The reasons are the common vulnerabilities, coupling within networks between equipment which might lead to security violation due to human errors, shared input data equipment, environmental events (flooding, storm and cyber attacks).

35.3 IoT based smart grid safety and security management system

35.3.1 Structure and goals of IoT based smart grid safety and security management system

According to [12] safety management system (SMS) is a systematic approach to managing safety, including the necessary organizational structures, accountabilities, policies and procedures.

SMS is a comprehensive management system designed to manage safety elements in the workplace. It includes policy, objectives, plans, procedures, organisation, responsibilities and other measures [12]. The SMS is used in industries that manage significant safety risks,

including aviation, petroleum, chemical, electricity generation and others.

Security management system is a set of policies and procedures for systematically organization's sensitive data management. The goal of such system is to minimize risk and ensure business continuity by pro-actively limiting the security breach impact. The security management is a planning, organisation and allocation of resources, humans and tasks with aim to reach demanded supply chain security level.

Considering the huge impact of IoT technologies on smart grid safety and cyber security it is worth introducing a new system for safety management which is complimented by cyber security management features.

The generic structure of IoT safety and security management system (SSMS) based smart grid is given on Fig. 35.9.

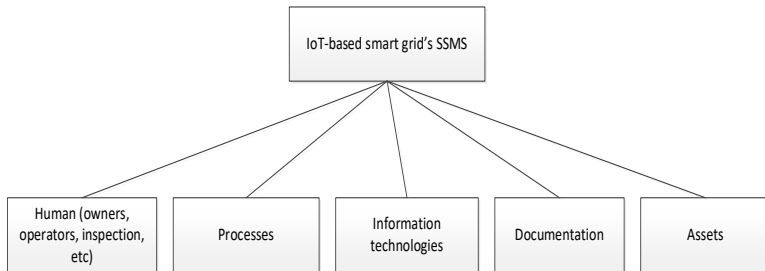


Fig. 35.9 - Generic structure of IoT SSMS based smart grid

SSMS includes the following main elements:

1. **Humans** (owners, operators, etc.) – those who are involved into decision making process in SG.

2. **Safety/security assessment and assurance processes** (safety processes) used by humans in SG.

3. **Information technologies** which support the safety/security processes in SG.

4. **Documentation** which is supposed to be filled during implementation of SG safety/security assessment and assurance processes.

5. **Assets** – facilities which are objects of safety/security processes implementation in SG.

SG safety/security management is a planning, organisation and allocation of resources, humans and tasks with aim to reach demanded safety level of infrastructure and its vicinity.

IoT based Smart Grid Safety and Security management system has two main goals:

1. Perform safety/security level assessment from all available data.
2. Perform measures to assure that safety/security levels meet the requirements.

Practical recommendations to establish IoT based SSMS:

1. **Roles and responsibilities identification** of safety/security personnel. Once general planning is underway, identifying roles and responsibilities of key safety/security personnel (safety/security manager) is an important step. This will ensure they have a good understanding of what the system aims to achieve are and what needs to be built or purchased.

2. **Managing safety/security data.** Another planning task could determine if it is required to procure external software to manage safety/security. Keeping accurate records throughout the life of SSMS is important as it will allow to effectively review safety issues and to be able to predict potential safety issues.

3. **Implementation plan** as a guide on how to setup SSMS and reflect SSMS changes and growth. The implementation plan should be established by organisations implementation team, e.g. the:

- Safety/Security Manager,
- Accountable Manager,
- Responsible Manager and
- staff representatives.

The following activities might be included into this plan: gap analysis, communications channels setup, emergency response plan development, etc.

4. **Preparing gap analysis.** Gap analysis provides valuable information about which parts of SSMS are in place and which parts should be added.

SSMS of IoT based SG could be represented as an ierarchy which includes the following levels (Fig. 35.10):

- SSMS goal, strategy;
- Management level;
- Process level;
- Application level;
- Assets level.

It is worth noting that SSMS is not static. One of its' main features is changing as SG evolves through its life cycle.

35.3.2 IoT based smart grid safety and security strategies

The interaction (informational, physical, geographical, etc.) between systems in SG leads to new (emergent, hereinafter ER) risks that cannot be identified in the early stages of LC.

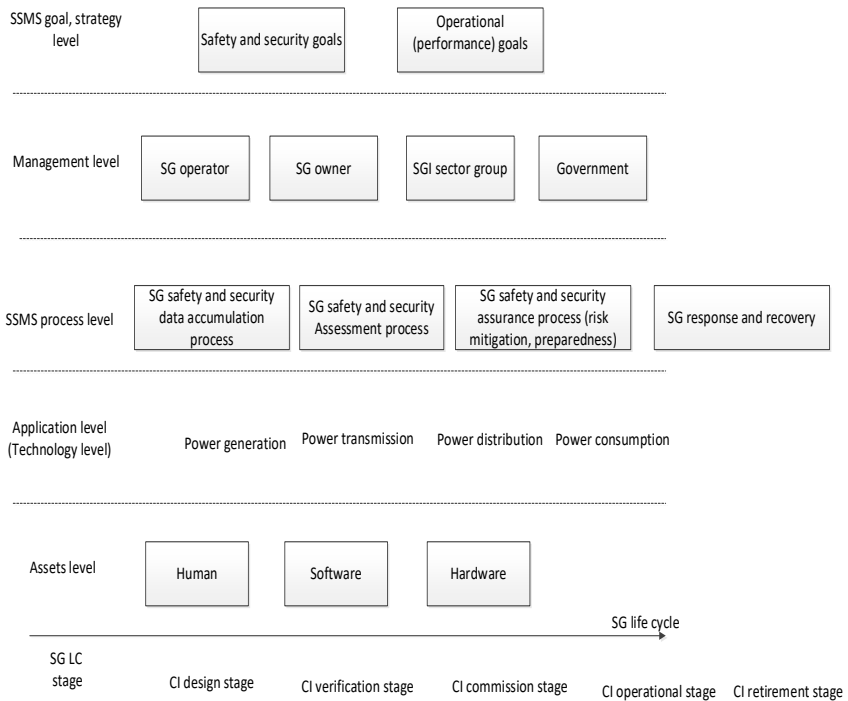


Fig. 35.10 - Main SSMS levels of IoT based SG

If the local risk (LR) is measured and reduced at the design stage of the system, the uncertainty in the estimation of ER remains one of the main danger sources to SG and its safety. Thus, increasing the SG safety can be achieved by identifying and reducing ER.

Since each of the SG systems has some resources (ability to load-sharing), then one of the possible strategies is to reduce ER is the redistribution aimed (see Fig.35.11) at the one system excess resources use to reduce another system ER, due to the interaction.

35.3.3 Safety strategies: redeployment of resources in smart grid

All systems in SG are open, i.e. systems which exchange resources (power loadable reserve, etc.) and information with other systems during their LC. The degree of openness (DO) is characterized by many parameters: number of ties with other systems type, period of interaction.

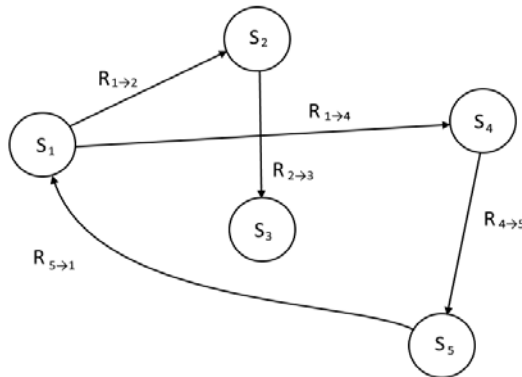


Fig. 35.11 - General view of SG S_0 and the interaction between its systems

DO of any SG system changes as all the parameters of the interaction change. Open systems are subject to the negative influence of other systems in SG. The more the system is, the greater its vulnerability to negative influence is.

The results of SG risk analysis depend on the adopted (under studies)

system DO. It is quite difficult to reliably determine DO, especially at the project analysis stage. The underestimation of interaction makes the system conservatively “closed” in some sense. This leads to the fact that risk analysis becomes inaccurate, deterministic, which reduces the reliability of the results and effectiveness of countermeasures aimed at reducing ER. Please do not include section counters in the numbering.

SG can be represented as a set of interacting systems (see Fig.35.14), linked by bonds of different nature (electricity flow, information, logical, etc.).

In the general case SG (S_0) can be represented as a set of the interacting systems.

Risks in open and closed (without interaction) systems are different. In the general case, the total amount of LR for a closed system S_1 (without taking into account the interference from other systems in SG) at time t can be represented by the additive convolution of the form:

$$R_{S_1}^{\text{Closed}}(t) = \sum_{i=1}^N \alpha_i R_i(t),$$

where $R_{S_1}^{\text{Closed}}(t)$ – cumulative LR for the closed-loop S_1 at time t ;

$R_i(t)$ – specific LR for S_1 at time t ;

α_i – coefficient describing the priority of LR for the system.

We can assume that for system S_1 , some SG component part of S_0 in the presence of interference between S_1 and S_2 , the magnitude of the resulting risk to system S_1 is related to the S_2 system will be greater than the magnitude of the risk for S_1 closed the effect of the system S_2 .

In other words, the cumulative LR for the closed-loop system S_1 is less than its total risk as part of a system S_0 , containing systems S_1 and S_2 .

The difference between the total risk of a closed and open system can be represented as:

$$R_{S_1}^{\text{emerg}}(t) = R_{S_1}^{S_0}(t) - R_{S_1}^{\text{Closed}}(t),$$

where $R_{S_1}^{\text{emerg}}(t)$ – the value of ER that occurs in the system S_1 as a result of interaction with S_2 in the system S_0 ;

$R_{S_1}^{S_0}(t)$ – the risk of system S_1 to the system SG (S_0).

Thus, at any point in time, the system S_j is characterized by the value of LR and ER due to the negative influence of h-type (informational, physical, etc.) from another system S_i . Assume that each system S_i has a resource (reactive power) which can be used to reduce LR.

In the general case, the task of resources redistribution within the SG to reduce ER caused by interference between the systems can be formed. A shared SG resource is an additive amount of system resources, which is a limitation in redistribution.

Condition. The system may not transfer the resources if the current safety index (SI) and the ER value do not match the required values.

Assumption. These resources are only used to reduce ER.

In general, the task of reallocating resources in SG can be formulated as:

– there is some system S_i in SG, with resources M_{S_i} . Safety Index and ER do not meet the required values, i.e. $SG = \{\{S_i\}_I, \{M_{S_i}\}, \{SI_{S_i}(t) \notin \Omega_{SI_{S_i}^{accept}(t)}\}, \{R_{S_i}^{emerg}(t) \notin Y_{R_{S_i}^{accept}(t)}\}\}$.

– it is necessary to provide an acceptable level of LS and ER system by redistributing resources within SG, i.e. $SG = \{\{S_i\}_I, \{M_{S_i}^*\}, \{SI_{S_i}(t) \in \Omega_{SI_{S_i}^{accept}(t)}\}, \{R_{S_i}^{emerg}(t) \in Y_{R_{S_i}^{accept}(t)}\}\}$ subject to the restrictions that $M_{CEI} = \sum_i^I M_{S_i}$.

Within SG there are various strategies of resources redistribution to reduce ER.

35.3.4 Strategy of redistribution with the mandatory allocation of sufficient resources

The system (a subject of influence, donor system) transfers to another system (object of influence) the amount of resources necessary to reduce ER that it creates. In this case, the donor system must allocate the number of resources sufficient to maintain SI of another system (As Safe As Reasonably Practical, ASARP).

This approach may not be rational for the donor system, because there are risks of situations in which it will not be able to reduce its ER due to the influence of other systems.

Condition. The donor system S_i can allocate resources to reduce ER just in case when the current SI and the level of ER are acceptable,

$$SI_{S_i}(t) \notin \Omega_{SI_{S_i}^{accept}(t)}, R_{S_i}^{emerg}(t) \in Y_{R_{S_i}^{accept}(t)}.$$

The critical system condition $Crt(S_i)$ is considered as SI.

Assumption. The current resource system provides a reduction of its LR, i.e. the system must have sufficient resources to reduce the LR.

We introduce an indicator which characterizes the vulnerability of the resource (resource vulnerability index, RVI) systems in SG:

$$RVI_{S_i} = \frac{N_{S_i \rightarrow S_j}}{N_{S_j \rightarrow S_i}},$$

where $N_{S_i \rightarrow S_j}$ – the number of outgoing ties (the system S_i is the subject of influence); $N_{S_j \rightarrow S_i}$ – the number of incoming ties (the S_i system is the object of influence). The higher the value of RVI is, the more resource insecurity system in SG risks there are.

We introduce an additional indicator – the ratio of the current LS $Crt(S_i)$ to the value of RVI – overall vulnerability index (OVI) of the system. The smaller OVI is, the more vulnerable the system is (low safety and high risks of resource insecurity).

The resources reallocation within the framework of the first strategy includes the following steps:

1. Evaluation of $ER R_{S_i}^{emerg}(t)$, current SI $Crt(S_i)$ of systems and resource vulnerability index Li , OVI.

2. Ranking of SG systems to a minimum of OVI with the purpose to select the system for the redistribution initialization. Note that the resources distribution between systems in SG begins with systems with a minimum OVI value. This means that the system has low safety and high risks of resource insecurity. Thus, from the ranked series we take the vulnerable system, from which the improved safety is begun.

3. Systems-subjects possibilities determination (associated with the affected system) for the resources transfer to reduce ER system with a minimum OVI. If you have multiple subjects of influence, the resources transfer for the object of influence begins from the “strong” system (the highest of OVI). Resources transfer from the donor resources system (with a minimum of OVI) is performed only if the current ER and the donor safety indicator are acceptable.

4. The resource transfer by the donor system for its objects of influence with the aim of reducing ER (subject to the requirements of LS and ER). Because the donor system transfers as much as you need, ER system of object of influence is reduced after the resources transfer.

5. Further, we considered the following system in ranked-set specified in step 2. Step 3 is repeated.

6. In the case when the donor system is not satisfying the conditions of LS and ER admissibility, the resources transmission is not performed. Next, we study the following donor system (including ties) for the object of influence.

7. Resources transfer is over when: it is impossible to transfer one of the systems in SG resources or the conditions of ER and SI for all systems in SG admissibility are satisfied.

Thus, each donor system must provide the resources to its object of influence, sufficient to reduce its ER. The algorithm of the first strategy implementation is shown in Fig.35.12.

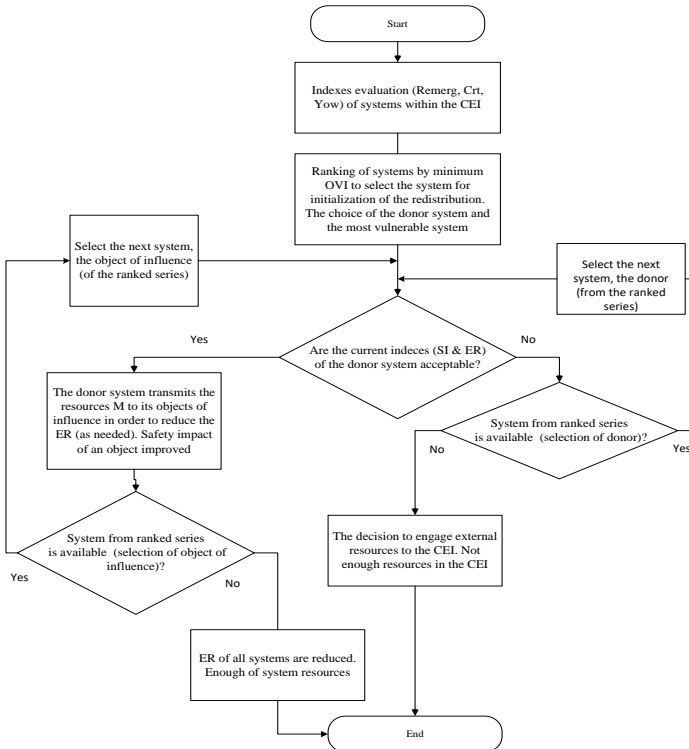


Fig. 35.12 - The first strategy algorithm

35.3.5 Strategy of redistribution with the possible (but insufficient) resource allocation

The donor system transfers to the object of influence as many resources as possible with a view to ensuring the required SI level (with the existing ER relating to the negative influence of other systems), i.e., it allocates a certain surplus of resources, leaving itself just exactly what it needed.

This strategy is acceptable for the donor system because the remaining resource is sufficient to reduce its ER. For the system-object of influence, this approach may not be rational, as the allocated resources may be insufficient to reduce the ER created by the donor system.

Condition. The donor system S_i may allocate resources only if its current SI and ER are acceptable, i.e. $SI_{S_i}(t) \notin \Omega_{SI_{S_i}^{accept}(t)}$, $R_{S_i}^{emerg}(t) \in Y_{R_{S_i}^{accept}(t)}$.

Assumption. The current resource of system provides the donor system LR reduction.

It should be noted that in deployment (for both strategies), there are risks in which the donor system will give more resources than you get from the other systems.

For example, the system S_4 (see Fig.35.11) should give part of its resources to the system S_1 and S_5 . System S_1 receives resources from the systems S_4 and S_5 , transferring the portion of the resources of the system S_2 . The larger the index of RVI system is, the greater the risk of its insecurity resource to reduce LR and ER. The second strategy implementation algorithm is shown in Fig.35.13.

There are 2 special cases in the second strategy framework:

- The amount resources $M_{S_i}^{**}$, transferred by the donor system, are not enough for full ER compensation, i.e. only some of the same resources, the size of which does not compensate for ER, are transferred. This means that you must use the following donor system (if any);
- Resources transferred to another system fully ensure the ER reduction. This case leads to the first approach, therefore only the first case is considered further.

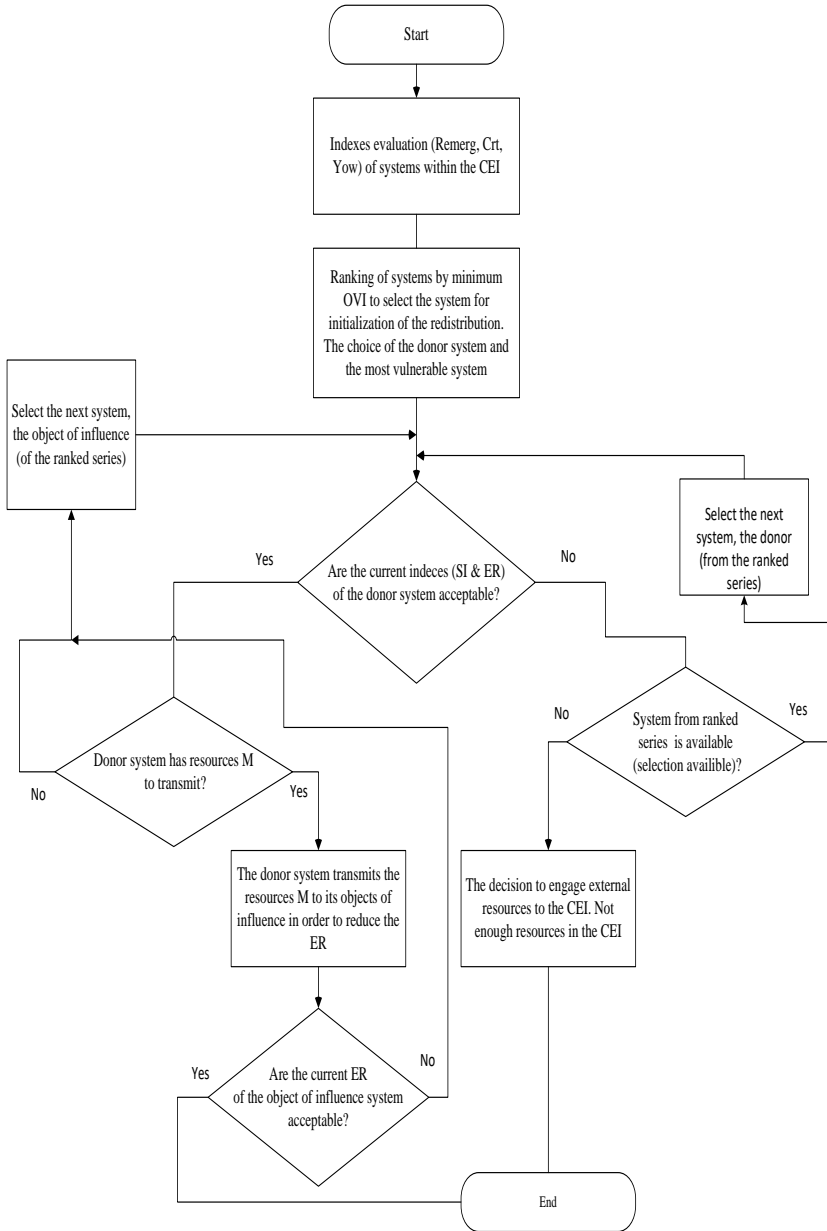


Fig. 15.13 - The second strategy algorithm

The second strategy is more complicated for ER object system of influence reducing, all of the donor systems resources (including ties) can be used, which could lead to a situation where the donor systems can reduce their own ER (because they are subject to influence from other systems).

For the first strategy, the number of possible donors will be less because more strict requirements are defined on the resources transfer to another system. Let's consider the illustrative example of the two strategies implementation.

The source data for the strategies implementation are shown in Table 35.7.

In the present example (see Fig.35.11) we obtained: final risks and resources redistribution (first strategy, see table 35.8); final risks and resources redistribution (second strategy, see table 35.9).

A specific SG feature is to conduct risk management for all SG in general. The decrease in ER for a particular system is due to the allocation of resources across SG.

For example, the first strategy is implemented in two stages: 1) a system with low-level LS and a high resource failure risk level revealed; 2) this system provides resources to other systems (subject to the restrictions on relations), provided that its ER can be parried with the available resources of these systems.

Table 35.7 - Initial data for the strategies implementation

System	Local risk	Emergent risk	System resource	Safety index, SI	RVI	SI/RVI, OVI
S ₁	$R_{S_1}^{Closed}(t)$	$R_{S_1}^{emerg}(t)$	M_{s_1}	Crt (S1)	RVI1	L1
S ₂	$R_{S_2}^{Closed}(t)$	$R_{S_2}^{emerg}(t)$	M_{s_2}	Crt (S2)	RVI2	L2
S ₃	$R_{S_3}^{Closed}(t)$	$R_{S_3}^{emerg}(t)$	M_{s_3}	Crt (S3)	RVI3	L3
S ₄	$R_{S_4}^{Closed}(t)$	$R_{S_4}^{emerg}(t)$	M_{s_4}	Crt (S4)	RVI4	L4
S ₅	$R_{S_5}^{Closed}(t)$	$R_{S_5}^{emerg}(t)$	M_{s_5}	Crt (S5)	RVI5	L5

Comments. When using the first strategy the common ER of all SG are balanced, because the systems transmit their resources to reduce them. In this case, if the system originally allocated the excess resources to reduce LR (with some margin), then LR are balanced in

SG. It is obvious that the second strategy does not only allow you to reduce ER but also LR for individual systems (provided that the transferred resources are not sufficient to mitigate ER).

In this regard, SG cannot provide the desired LS level. For SG, it is advisable to allocate resources.

Table 35.8 – The final risks and resources reallocation for the first strategy

	Resource state, T_0	Resource state due to its redistribution, T_1	The ability to fend off the ER	The ability to fend off the LR
1	M_{S1}	$M_{S1} + M_{S5}^* - M_{S1}^* - M_{S1}^{**}$	+	-
2	M_{S2}	$M_{S2} + M_{S1}^* - M_{S2}^*$	+	-
3	M_{S3}	$M_{S3} + M_{S2}^*$	+	+
4	M_{S4}	$M_{S4} - M_{S4}^* + M_{S1}^{**}$	+	-
5	M_{S5}	$M_{S5} + M_{S4}^* - M_{S5}^*$	+	-

Table 15.9 - The final reallocation of risks and resources for the second strategy

	Resource state, T_0	Resource state due to its redistribution, T_1	The ability to fend off the ER	The ability to fend off the LR
1	M_{S1}	$M_{S1} + M_{S5}^{**} - M_{S1}^{**} - M_{S1}^{***}$	-	-
2	M_{S2}	$M_{S2} + M_{S1}^* - M_{S2}^*$	-	-
3	M_{S3}	$M_{S3} + M_{S2}^*$	-	+
4	M_{S4}	$M_{S4} - M_{S4}^* + M_{S1}^{**}$	-	-
5	M_{S5}	$M_{S5} + M_{S4}^* - M_{S5}^*$	-	+

A software tool has been developed to support this method. This program gives an ability to define system structure, describe elements state and predict a better resource redistribution strategy as a result of calculations.

The software tool was developed on top of Microsoft .NET platform using WPF framework to achieve a fast result and a high user experience.

It gives an ability to easily create extensions and improvements to an application as an applied realization of the method.

35.3.6 Cases

The safety modeling of Siberia power grid was performed as a practical case of strategy application (see Fig.35.14). All generation systems (S_1 - S_5) pull electricity into grid according to their capacities (resources).

The systems' resources are their power (MW) capacity. ER for each station is threat of taking additional power load in case when other systems are lost due to accidents.

The system might be unable to take this additional load and the whole grid will be lost (black out). OVI is calculated after the defuzzification of SI.

All systems have a reserve capacity that can be allocated to support the power grid balance (production and consumption balance). ER is associated with the possible exclusion of one of the stations from the process of power generation.

The remaining systems will have to take the burden if it happens. If the station reserve has been decreased, it means that the system took over a part of someone's load.

Physically, it started additional energy generation (for example, a generator for a power plant). If the reserve was increased, it should turn off these facilities, because the other system has taken over the part of the total load.

Analysis of final data (see Fig.35.15) shows that after resource distribution only two generation stations (Irkusk and Mamakansk HPPs) have improved their capacity to cope with ER, but decreased their capacity to cope with LR.

RR Results

Initial data

System	Local Risk	Emergent Risk	System Resource	Security Index	RVI	OVI
Irkutsk HPP	10	20	662	Low	2	0.33
Bratsk HPP	20	10	450	High	1	2.33
List-Ilim HPP	10	0	384	Low	0	2
Mamakansk HPP	20	10	86	Low	1	0.66
The pilot NR1 of TPP-9	10	10	166	Middle	1	2

Show steps

Cancel Back Next Finish

Fig. 35.14 - The initial data for the first strategy

RR Results

Result

System	Resource State, T0	Redistribution resource state, T1	Can fend off the ER	Can fend off the LR
Irkutsk HPP	662	700	+	+
Bratsk HPP	450	300	+	-
List-Ilim HPP	384	360	+	-
Mamakansk HPP	86	130	+	+
The pilot NR1 of TPP-9	166	80	+	-

Cancel Back Next Finish

Fig. 35.15 - The final data for the first strategy

If such strategy had been considered by Syberia operator during decision-making, it is likely that Sayano–Shushenskaya HPP accident would have been avoided as it would have been based on the station abilities to decrease ER.

Thus, the strategies implemented by the resources reallocation between systems in SG allow you to provide the required level of SI and ER with constraints on resources. Each of the offered strategies takes into account individual preferences in SG systems: to provide as many resources as needed or as possible, taking into account the assessment of individual risks. The first strategy is preferable with the increasing of accidents risks, the second involves the functioning of SG in the moderate risk. Thus, the strategy is chosen due to the current SI systems, interaction dynamics, SG resource safety. LR and ER monitoring will allow you to flexibly choose a particular strategy.

It is advised to support decision-making and implementation approaches. The implementation of the proposed approaches to the resources reallocation is supported by the tool. This tool allows simulating the redistribution taking into account the characteristics of the systems included in SG (strategy, initial resources amount, communications, LR and ER).

35.4 Resilience-oriented measurement of quality of IoT based smart grid service assess

35.4.1 Method for IoT based smart grid resilience assessment

IoT based smart grid is subjected to cyber attacks. According to [13] in August 2011, the Diablo Canyon nuclear plant, north of Santa Barbara, experienced a network break-in, in which the attackers were seeking to identify the operations, organizations, and security of U.S. nuclear power generation facilities. If details of the plant’s security, physical layout, location of critical systems/processes and nuclear material were known and fell into the hands of terrorist or other belligerent agents, an attack could be mounted with serious consequences.

On December 23, 2015, the cyberattack (BlackEnergy3) on the CEI of Ukraine led to a large-scale blackout [14]. Hackers got access to the systems for monitoring and managing the network objects.

The work of the company was completely paralyzed by malicious code, servers and personal computers were broken, and it revealed the Oblenergo information security systems imperfection. In Prykarpattya, as well as in Kiev and Chernivtsi regions, about 220,000 electricity consumers remained without electricity (which accounts for about 1% of all energy consumers in the country). The blackout lasted from 1 to 3 hours in three areas. The total electricity deficit was 73 MW / hour or 0.015% of the daily Ukraine consumption.

In 2017, the Kyivenergo metropolitan power company computer systems were subjected to a hacking attack.

The analysis of these cyber incidents confirms the importance of the task of increasing SG resilience to cyber attacks. Resilience is considered as an ability to withstand and recover quickly from unknown and known threats. For SG cyber resilience means being able to absorb attacks and maintain or quickly restore necessary power supply service level. Thus, the cyber resiliency concept is closely related to the notion of functionality, the ability of the system to restore its functionality after an attack or cyber incident.

Cyber risk management is carried out prior to the occurrence of adverse cyber event. The purpose of cyber risk management is to reduce the effects of an adverse event or to prevent its occurrence. Aspect of SG restoration to the initial (acceptable) functioning level after the occurrence of the cyber incident is taken into account by another SG property, by its cyber resilience.

It should be noted that the cyber risk and cyber resiliency concepts are interconnected. Effective cyber risk management can lead to the increased system cyber resiliency. Meanwhile, there are many differences between notions of resiliency and risk management. Risk management involves preparing the system for the onset of a negative event. In this sense, the system can quickly return to some initial functional level. In traditional cyber resilience's approaches, the emphasis is given on the SG ability to reach the original level of functionality quickly. The functionality and safety (security) are main SG features. So it is advised to introduce a risk-oriented definition of resiliency. Under the risk-oriented cyber resilience, one shall understand the ability of the system to restore the original level of safety (cyber security).

The cyber resiliency concept is wider than risk and includes the ability to restore the required cyber security and safety level (if needed). From the system's ability to withstand the external adverse effects and return to the original (acceptable) level of functionality point of view, resiliency is a more systematic concept than the concept of risk management. SG resilience (R_{SG}) can be represented as an additive convolution of the systems' resiliency (R_s) and resilience of links (RL) between them. In its turn system resilience might be given as a function of four system's capacities: preventive (RP), absorptive (R_{ab}), adaptive (RA), and restorative (RR) (see Fig.35.16). All of them could be measured by resilience capacity parameters.

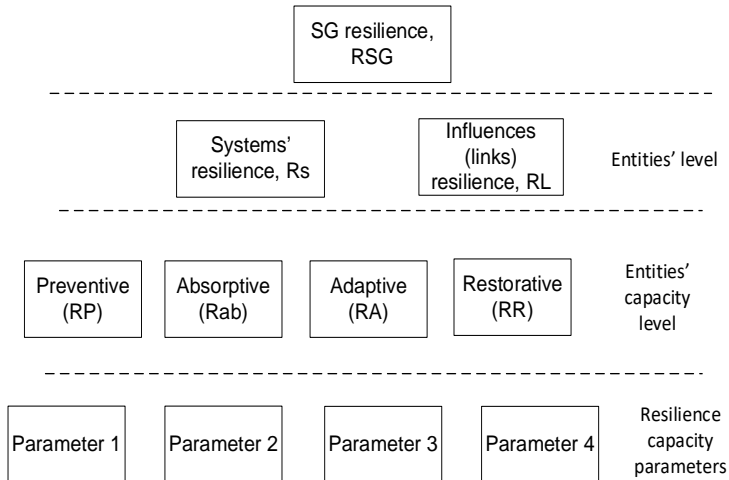


Fig. 35.16 - The holistic approach for SG resilience decomposition

Fuzzy technologies are actively used for SG safety assessment [15]. This task is quite similar in the terms of complexity and needs to use the parameters expressed in various qualimetric scales. Thus, for example, in nuclear industry Fuzzy Logic and Intelligent Technologies are applied intensively for solving fuzzy control problems, which can't be solved using existing methods and approaches.

Under this approach, SG's cyber resilience is treated as linguistic variable. A linguistic variable is characterized by a quintuple $(x, T(x), U, G, M)$ in which x is the name of variable; $T(x)$ is the term set of x , that is, the set of names of linguistic values of x with each value being a fuzzy number defined on U ; G is a syntactic rule for generating the names of x values; and M is a semantic rule for associating each value with its meaning. Thus, for example, cyber resilience can be represented as a linguistic variable with terms {High (H), Medium (M), Low (L)}. The illustration of semantic interpretation of linguistic terms of SG cyber resilience and capacity parameters are presented in Table 35.10.

The SG's cyber resiliency assessment can be performed using multilevel logic-linguistic model (LLM) with the real values of resilience capacities' parameters.

It is also seen from Table 35.10 that resilience parameters are the linguistic values as well.

The multilevel LLM of SG resilience can be written as:

$$RM_{SG} = \{ \{ P_h^{parameter}(S_i) \} = \{ x_i \}_I, \{ MF_i \}_I, \{ RB_j \}_J, \{ R_t \}_T \},$$

$$R_{S_i}(t) = R_i(RM_{S_i}), R_{CEI}(t) = R(R_{S_i}(t), RL(t)),$$

where $\{ P_h^{parameter}(S_i) \} = \{ x_i \}_I$ – set of parameters describing the system's resilience capacities;

$\{ MF_i \}_I$ – set of membership functions;

$\{ RB_j \}_J$ – set of fuzzy interference rules;

$\{ R_t \}_T$ – set of formal relationships (fuzzification procedures, activation, aggregations, etc.);

$R_{S_i}(t) = R_i(RM_{S_i})$ – system resilience is considered as a function of sets, given above;

$R_{CEI}(t) = R(R_{S_i}(t), RL(t))$ – SG resilience is considered as a function of system and interdependencies resilience.

Table 25.10 - Semantic interpretation of linguistic terms of SG cyber resilience and capacity parameters

Resilience level	Description per system resilience capacity and its indicators
Cyber resilience – HIGH	<p><u>RA capacity</u>. High level of changing system architecture ability. Parameters: time and cost of self-organization.</p> <p><u>RP capacity</u>. High level of performing hazard identification and vulnerability assessment ability. Parameters: predication accuracy, resources, etc.</p> <p><u>Rab capacity</u>. High level degree to absorb the impact of system's perturbations. Parameters: time of appropriate performance level keeping after accident happens.</p> <p><u>RR capacity</u>. Recovery duration time is small. Parameters: recovery cost, safety state reached after accident (probability of failure, severity).</p>
Cyber resilience – MEDIUM	<p><u>RA capacity</u>. Medium level of changing system architecture ability. Indicators: as above.</p> <p><u>RP capacity</u>. Medium level of performing hazard identification ability.</p>
Cyber resilience – LOW	<p><u>RA capacity</u>. Low level of changing system architecture ability; mobilizing resources. Parameters: high time and cost of self-organization.</p> <p><u>RP capacity</u>. Low level of performing hazard identification and vulnerability assessment ability. Parameters: low predication accuracy, resources.</p>

Multilevel LLM for SG resilience assessment is given on Fig.35.17. The inference shall be performed from left to right, beginning with determination of parameters set for system resilience capacity (predeictive, absorptive, preventive, restoration) evaluation and link resilience evaluation.

The dependencies (link, influecnes) resilience evaluation RL between system S_1 and S_2 shall take into account the parameters

$$\{x_i\}_I = \{\text{Importance, Vulnerability}\}.$$

These parameters might have the quantitative values and calculated considering the roles for system recovery, functionality, vulnerability.

There are three levels in multilevel LLM.

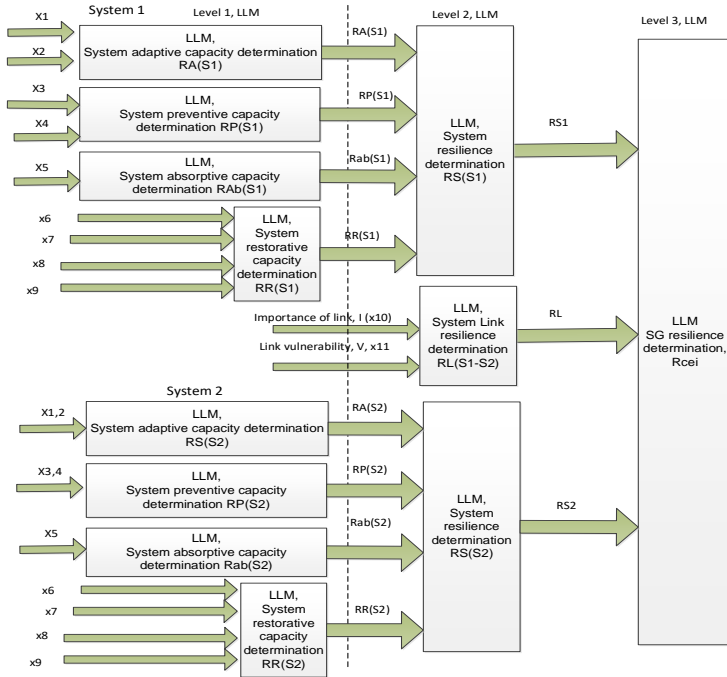


Fig. 35.17 - Multilevel LLM for SG’s resilience assessment

Level I. LLM is used for SG resilience assessment (R_{sg}). This model allows determining the value of SG’s cyber resilience considering the output from LLMs of second level. The purpose is to obtain the linguistic value of SG’s cyber resilience as a whole, considering its systems resilience and resilience of links between them.

Level II. This level includes the following LLMs: LLM for System resilience determination $R(S_1)$; LLM for System Link resilience determination $RL(S_1-S_2)$; LLM for System resilience determination $R(S_2)$.

These models allow determining the system cyber resilience value considering the output from the first level LLM.

The purpose is to obtain each system cyber resilience value separately. Resilience of link is also evaluated with this LLM.

Level III. This level includes the following LLMs: LLM for System adaptive capacity determination RA (S_1); LLM for System preventive capacity determination RP (S_1); LLM for system absorptive capacity determination Rab (S_1); LLM for System restorative capacity determination RR(S_1). These models allow determining the values of four main resilience system capacity (adaptive, restoration, preventive, absorptive). The purpose is to obtain the value of each capacity which determines the resilience of system in SG.

LLM for system and link's resilience estimation includes the following sections (see Table 35.11).

LLM for SG's resilience assessment is constructed by designing and configuring fuzzy knowledge bases [16, 17]. A knowledge matrix describing the SG's functioning defines a system of logical equations that bind the values $x_1 \div x_n$ of capacity parameters with a possible resilience estimate.

One of the important tasks performed during cyber resilience assessment is the capacity parameters selection. System adaptive capacity (RA) might be measured by the following parameters: time for self-organization (x_1), self-organization cost (x_2). System preventive capacity (RP) might be measured by the following parameters: accuracy for prediction (x_3), resource for prediction (x_4).

System absorptive capacity (Rab) might be measured by time of appropriate performance level keeping after accident happens (x_5), etc.

System restorative capacity (RR) might be measured by the following parameters: cyber accident probability (P), (x_6); severity (S), (x_7); system restorative time (T), (x_8); restoration cost (C), (x_9).

Link importance (x_{10}) and link vulnerability (x_{11}) are determined by the expert-based approach.

The parameters list which characterizes the resilience's capacities of SG is determined by scope of tasks, systems peculiarities and links between them.

Table 45.11 - LLM description

LLM section	Short description
Analysis of failures, faults and accidents, cyber incidents	Analysis of failures and accidents, cyber incidents are performed for systems SG
Expert knowledge	Expert knowledge on systems, SG, interdependencies between systems
Fuzzy rule base «IF X, THEN Y»	a set of fuzzy predicate rules, $R = X \rightarrow Y$
Analysis of historical data	Analysis of resilience data for systems of this class
Input parameters of the state and influence	Model inputs. $\{x_1, x_2, \dots, x_k = I(t)_h^{Cl}(S_i \rightarrow S_j)\}$
Fuzzification	Setting the correspondence between: - the input variable numerical value (system input parameters) of the fuzzy output system and - the value of the membership function of the linguistic resilience variable corresponding term
The process of fuzzy logical conclusion	$T(X \cap Y) = \min\{T(X); T(Y)\}$
Defuzzification	$\mu^{d_j}(x_1, x_2, \dots, x_n) =$ $= \max[\mu^{d_j}(x_1, x_2, \dots, x_n)], j = \overline{1, m}$.
Obtaining resiliency assessments for SGS	Output model data. System (SG) resilience estimates

The main stages of the SG cyber resilience assessment approach using the multilevel LLM are:

1. **Formation of a fuzzy rule base for cyber resilience assessment.** The base rules for fuzzy output are intended for the formal representation of the empirical knowledge or knowledge of experts associated with the SG. In fuzzy output systems, the fuzzy products rules are used, in which conditions and conclusions are formulated in terms of fuzzy linguistic statements. To construct a base of rules, one

needs to solve the tasks connected with the analysis of historical data, expert data, etc.

2. ***Model input parameters*** (operational, diagnostic, etc.) ***selection***, describing the resilience capacities. These parameters give a view on four system capacities which make a system resilient. The link resilience parameters should also be considered.

3. ***Resilience capacity parameters fuzzification.***

4. ***Fuzzy logical inference.***

5. ***Resilience value defuzzification.***

6. ***Obtained results analysis, issuing recommendations.***

An additional stage of using the LLM to assess the SG's cyber resilience is to adjust the LLM parameters and refine the structure, taking into account the proposed methods of improving accuracy.

The risk-oriented resiliency concept is introduced. SG's resilience is characterized by systems' capacities and links (dependencies) resilience. There are four important systems' capacities which determine its resilience: preventive (RP), absorptive (Rab), adaptive (RA) and restorative (RR). The proposed approach may be applied to SG cyber resilience assessment, taking into account its systems interdependencies. The exchange of information between SG's owners is also capable of increasing the overall infrastructure resiliency and security (safety). Meanwhile, currently there is no single communication's platform for assessing safety and resiliency in Ukraine. SG's owners conduct their own (industry) safety (security) analysis within a particular industry, without regard to information, status, possible solutions of owners, all interconnected SGs.

This is due to the lack of a single infrastructure security and resilience management. At the same time, taking into account the development of modern information technologies and simulation tools, all of the above tasks should be solved within a single decision making system for safety (security) and resilience assessment. This decision making system shall include the modules for safety assessment, cyber security assessment, cyber resilience assessment.

Next step of the approach enhancement will be related to the development of one holistic IoT based framework for decision making system mentioned above.

35.4.2 SDOE-based development of resilient digital substation

The cyber security aspect of the digital substations' development is becoming relevant. This is due to the increasing number of cyber incidents related to attacks on SCADA type systems.

Trends analysis indicates a steady increase in the number of attacks on industrial systems since 2010 (after Stuxnet). For example, in February 2011, a massive Night Dragon attack was conducted on five oil refining companies. In 2012, in a number of large companies operating in the banking sector of Syria, Lebanon, Sudan, malware ("Flame") was detected, designed to perform spyware, record talks, etc. Thus, there is an obvious increase in the number of attacks on industrial system that will be saved in the future.

Industrial systems developers seek to increase their security against external attacks, reduce the risks to cyber security and potential vulnerabilities. Implementing the IS requirements for systems, developers are striving to develop a secure product. Many requirements for information security can be divided into: requirements of the regulator, regulatory framework, customer, etc. The general requirements group is inconsistent and not harmonized very often. For application development companies, one of the initial tasks is to analyze the requirements, systematize them and determine their priorities.

Taking the results of this analysis into account, the company-developer seeks to develop practical approaches aimed at meeting the entire requirements set.

It should be noted that the requirements analysis and the approaches development of are not separated tasks. We have to deal with a set of agreed tasks, the outputs and inputs of which are interconnected, very often. Thus, we can talk about the need to design (develop) the process of ensuring the information product security in the company. Such process is, in fact, one of the important business company processes, aimed at achieving customer satisfaction with the final product properties, at its cyber security. An effective process design for ensuring the information security of a product can be based on the use of business process engineering approaches.

When developing processes in a company, it is necessary to take the company's resources, the personnel training level, product requirements, the maturity of the technologies used, etc, into account.

The QMS is an important basis for the process design, which is an essential business management system component. It contains a description of all of the company business processes aimed at the quality products obtaining.

Since information security is also an important business process for a company, its design should be carried out taking into account other processes of the company within the framework of the quality management system.

The following process approach to the information security for a product providing can be applied to the development of digital substations or SCADA systems.

Data hubs are an example of industrial control systems that are subject to high demands on functional and information security. So, in particular, in the USA, the Nuclear Regulatory Commission (US NRC) actively uses a number of documents in its practice, the most important of which, from the information security of NPP DH point of view, include the following:

- 10 CFR Part 50, Appendix B, “Quality Assurance Criteria for Nuclear Power Plants and Fuel Reprocessing Plants”;
- Regulatory Guide (RG) 1.152-2011, Revision 3, “Criteria for Use of Computers in Safety Systems of Nuclear Power Plants, etc.

Such documents regulate many aspects, covering stages from the safe development and operation environment to the critical systems security properties, including information security. However, the activities related to information security into the DH life cycle model integration issues remain relevant and unresolved.

It is noted that the computerized systems software security refers to the ability to survive due to unauthorized, unwanted, and unsafe interventions throughout the life cycle of such systems.

Thus, there are many requirements for an information security product. Their implementation can be achieved in the implementation framework of one of the company's important business processes – ensuring information security. The ensuring information security process design should be based on the relationships with other processes in the company. The ensuring information security process should be an integral part of the company's QMS.

A secure development environment is defined as a condition for the availability of appropriate physical, logical, and software measures

during the system design stages to ensure that non-unwanted, unnecessary, and undocumented functionality (for example, redundant code) is not incorporated into security-critical digital systems. A safe functioning environment is defined as a condition for the availability of appropriate physical, logical and administrative measures at an enterprise to ensure reliable operation of I&C systems through the absence of their degradation due to incorrect behavior of connected systems, as well as events generated by unintended access to such I&C systems.

In general, for both environments the main component types are:

- hardware (including technical means of functioning and ensuring the development and operation infrastructures security, equipment for development and operation);
- software (including what is related to development and operation processes, as well as directly to the infrastructures under consideration);
- data network (related to both the development and operation environment);
- staff;
- product (DH, which is developed and then operated).

In addition to the above types of components, an important aspect subject to separate detailed analysis is their configuration, which includes many factors that encompass the physical, logical and behavioral relationships. The configuration largely depends on the quality and completeness of the QMS implementation in the development and operation environments, personnel qualifications, and the quality of the software and hardware components used.

The implementation of SDOE, in the context of RG 1.152-2011, relates to the following aspects:

- measures taken to implement a safe environment for the development of safety-critical DHs that prevent undocumented, redundant and unwanted changes;
- protective measures that prevent a predictable set of undesirable actions that may affect the integrity, reliability or functionality of a DH during its operation.

Cascade life-cycle model phases make it possible to form a structure of special guides on the critical from a security point of view digital systems protection as well as on the SDOE implementation by

identifying and mitigating potential weaknesses or vulnerabilities in each of the phases that may lead to the SDOE or the reliability of such systems degradation.

Security audits are an integral part of the security process during the development, implementation and maintenance of SDOE. Such audits include:

- audit of the development environment: after the establishment of the infrastructure in which the development will be carried out, and before the start of the development project for the I&C system;
- periodic audits: prior to each development phase.

The development environment audit is designed to assess the “basic” level of development environment security; mainly, the relevant measures are implemented by technical means and relate to the such infrastructure networks involved in the development process, physical means of protection, etc.

In turn, periodic audits are intended to assess additional specific measures required for the implementation of each development phase in the life cycle. Each of these audits includes the following steps:

- additional measures for the development phase implementation verification (i.e., what is implemented and how);
- verification of compliance with the guidelines and instructions of the organization related to a safe development environment by personnel (i.e., a practical assessment of whether employees follow the relevant QMS requirements).

The input for each of the audits is the corresponding plan (and, possibly, documents relating to certain aspects of the organization of the development environment or the implementation of processes), and the output is the SDOE audit report, in which the results are documented.

Thus, the information security provision is an important business process of the company. Its design (development) must be carried out taking into account the specifics of the company, its resources and the technologies used. The output of this process is a product that satisfies the customer in terms of quality. The ensuring information security process should be implemented within the company's QMS. When designing the ensuring information security process it is necessary to create a secure application development environment. The basis for developing a secure application can be the creation of a secure

development environment, which can be based on a nuclear QMS and its principles.

35.5 Work related analysis

There are many approaches for the SG's cyber resilience assessment. According to [18] the cyber resilience is considered as the capacity of the power enterprise to maintain its core purpose and integrity in the face of cyberattacks. In general, a primary goal of cyber resilience is to minimize the disruptive effects of cyber threats to utilities' business or mission operations. This goal includes the ability to withstand cyberattacks and the ability to prevent degradation to mission or business effectiveness. As the authors introduced the notion of cyber resilience no metrics and approaches for its estimation was suggested.

In the paper [19], the approach for Cyber Resilience Review (CRR) is given. The CRR measures an organization's operational resilience capabilities through examining cybersecurity practices across ten domains: Asset Management; Controls Management; Configuration and Change Management; Vulnerability Management; Incident Management; Service Continuity Management; Risk Management; External Dependency Management; Training and Awareness; Situational Awareness.

Formally, CRR is a lightweight assessment method that was created by the Department of Homeland Security for the purpose of evaluating the cybersecurity and service continuity practices of CEI. This expert-based approach is appropriate for organization but not good enough for SG. It does not consider interdependencies among systems in SG and mostly oriented on business processes of organization evaluated for cyber resilience. It also does not consider SG main assets (physical, cyber, etc.). As with all complex systems, SG are connected through multiple layers of mutual links which determined the dependencies between system's resilience states. This poses a problem in understanding the effects on the system as a whole as failure in one system may spread to other systems of the interdependent SG.

In paper [20] issued by Risk and Resilience Research Group all suggested resilience indicators are classified into two groups: a-priori and post hoc indicators.

The following a-priori SG resilience indicators are suggested: failure probability as an estimation of the expected impact and degradation of infrastructure following a disturbance or shock; infrastructure quality as an indicator of how well an infrastructure performs. Infrastructures with lower quality are likely to be less operable following disturbance, and this indicator can be used to describe performance over time; interdependence between systems in SG.

It is already mentioned that modern infrastructures are complex and in many cases are characterized by extensive interdependencies. The authors pointed on the importance of interdependences between SG systems for its restoration. It is determined the importance of assessing where interdependence exists, the nature of the relationships, and the criticality of the connections.

The authors do not suggest any approach on how to assess the interdependencies and their resilience level. The authors also suggested the post-hoc CEI's resilience indicators: recovery time post-event as a measure of the amount of time it takes for an infrastructure to be brought back to its pre-event level of functionality.

A positive aspect of the paper is the attempt to classify the indicators into two groups. It is specified that it is necessary to take into account the interconnection (communication) between systems, but a formalized approach is not proposed.

The paper [21] is intended to establish a risk-based framework for institutions to self-assess their risk's profiles and determine the level of security they require. The framework comprises three components:

1. ***Inherent risk assessment*** which measures the banks' cyber risk exposures based on a set of factors. Inherent risk ratings of high, medium or low will be used to set each bank's 'required maturity level' of cyber resilience;

2. ***Maturity assessment*** – a bank's 'actual maturity level' of cyber resilience is to be ascertained through this assessment. By comparing the actual maturity level and the required maturity level of cyber resilience, gaps in the bank's cyber security framework can be identified;

3. ***Intelligence-led cyber attack simulation testing*** – will comprise of simulation test scenarios that are designed to replicate cyber attacks based on specific and current cyber threat intelligence.

This approach for cyber resilience is quite specific and only applicable for bank's IT infrastructure and merely might be applied for SG's resilience assessment.

The approach for identifying, characterizing, and defining cyber resiliency metrics is suggested in paper [22]. There are more than 50 metrics such as: percentage of cyber resources that are properly configured; number of attempted intrusions stopped at a network perimeter; number of attempted intrusions deflected to a honeypot; length of time between an initial adversary act and its detection, etc.

The authors give a summary table where all metrics are accumulated. No approaches for estimation of such metrics are suggested in the paper.

Thus, common disadvantages of various approaches discussed above are the following:

- the absence of a unified system approach to resilience assessment that takes into account the basic properties of SG's systems (adaptability, ability to recover, etc.);
- the peculiarity of approaches. They are difficult to adopt for SG cyber resilience;
- the proposed approaches are aimed at attracting experts - there are no formalized approaches to assessing the cyber resiliency of enterprises, business organizations;
- there are no approaches for evaluation of SG's cyber resiliency with consideration of interdependencies, complexity of SG nature, relation between cyber resilience and safety;
- generally, there is a lack of publications devoted to SG cyber resilience assessment and no holistic approaches are found.

In [23] the authors present a comprehensive survey of cyber security issues for the Smart Grid. Specifically, they focus on reviewing and discussing security requirements, network vulnerabilities, attack countermeasures, secure communication protocols and architectures in the Smart Grid. Basically the authors target to get a deep understanding of security vulnerabilities and solutions in the Smart Grid and shed light on future research directions for Smart Grid security.

The paper [24] presents a good approach to solve the tasks such as: develop a methodology for risk assessment that addresses the specific challenges of the smart grid; create appropriate tools to

support this methodology; build a simulation environment that can be used to measure the impact of a cyber-attack. The most interesting part of this work is an attempt to perform safety and security co-analysis with aim to reuse of results across analyses, increase the ability to consistently prioritise different types of threats, i.e., attacks versus faults

The [25] deals with the cyber security evaluation of active distribution grids characterized by a high level penetration of renewable Distributed Energy Resources. This evolution of the energy infrastructure introduces significant changes in the control and communication functions needed for meeting the technical, security and quality requirements during the grid operation. The analysis focuses on a Voltage Control function in medium voltage grids addressing voltage stability of the power grid when a consistent amount of distributed renewable sources are connected. The book presents an experimental environment for the security testing and evaluation of voltage control communications. This includes the test bed set up, the test cases and the evaluation framework to be used for measuring the attack effects on substation-DER communications and verifying the mitigation capability of standard security measures.

This section was developed considering ALIOT's partner universities and the contents from their master programs such as:

- Master's programmes in Smart Electrical Networks and Systems (SENSE);
- Master's programme in Innovative Sustainable Energy Engineering;
- Master's Programme in Security and Cloud Computing (SECULO).

This section was also developed considering the state of art papers written by researchers from ALIOT's partner universities as described below.

In the paper [27] authors propose IoT-grid, a programmable, small-scale, direct current (DC) grid to facilitate deployment of IoT-based grids in domestic environments that can be easily implemented with low-power hardware with limited processing capacity. The proposed grid adopts relatively cheap DC-DC converters which not only provide high conversion efficiency but also accommodate existing small-scale DC power systems (e.g. solar panels). The authors explore

the communication aspects of IoT-grid, namely, control and monitoring functions. The mechanism for problem mitigation was proposed based on sending burst commands with scheduled responses.

In the paper [28] author analyzes how characteristics of power system applications can be leveraged for detection and mitigation of data integrity attacks. A single and multi-area power system state estimation was considered. Security metrics were defined that quantify the importance of particular components of the communication network, and that allow us to optimize the deployment of network, transport and application layer security solutions. For multi-area state estimation, the integrity of data was investigated that exchanged between the control centers of neighboring areas in face of a targeted trojan that compromises an endpoint of the secure communication tunnel. The multiple attack strategies were determined and it was shown they can significantly disturb the state estimation. Moreover, the schemes were proposed that could be used for detection, localization, and mitigation of data integrity attacks.

In project [29] the possibility of improving the integrity using realistic energy storage systems to physically change the consumption patterns of the prosumer as well as the best suited measurement of integrity is investigated. In the paper [30] author shows that an attacker that compromises the communication infrastructure of a single control center in an interconnected power system can successfully perform a denial-of-service attack against state-of-the-art distributed SE, and consequently, it can blind the system operators of every region. As a solution to mitigate such a denial-of-service attack, a fully distributed algorithm was proposed for attack detection.

Furthermore, a fully distributed algorithm was proposed that identifies the most likely attack location based on the individual regions' beliefs about the attack location, isolates the identified region, and then reruns the distributed SE. The proposed algorithms were validated on the IEEE 118 bus benchmark power system.

The paper [31] address the analysis and evaluation of different architectural concepts for securely integrating Customer Energy Management Systems into smart distribution grids. A risk analysis of the multiple communication network architectures is performed to reduce the risks associated with connecting the households to the comprehensive monitoring and control architecture,

Through this analysis the impact of different access network strategies on security can be assessed to select the most appropriate one, to ensure a reliable operation of the mission-critical Smart Grid communication network infrastructures. The probability of a successful attack has been evaluated as a function of the relative efforts for attackers to compromise these systems. The results show the relative robustness of the considered architectures as a support to the design of highly secured and reliable infrastructures down to these IT devices in the households.

The paper [32] authors outline an approach to model and analyze smart grids and discuss the major challenges to be addressed in stochastic model-based analysis to account for the peculiarities of the involved system elements. The main idea of paper is to represent a dynamic and flexible behavior of generators and loads, as well as representation of the complex IT control functions. All of these are required to preserve and/or re-establish electrical equilibrium in presence of changes need to be faced to assess suitable indicators of the resilience and quality of service of the smart grid.

In the paper [33] authors propose a novel policy-based framework aiming to exploit Software Defined Networking and Network Function Virtualization security features, by efficiently coupling with existing IoT security approaches. The proposed framework is validated in a testbed.

IoTSec project [34] addresses the basic needs for a reliable and efficient, uninterrupted power network with dynamic configuration and security properties. It addresses in addition the needs of businesses and end users of additional IoT services by exploring use cases for value-added services with the intent to design the building blocks for future services that consider the necessary security and privacy preconditions of successfully deployed large-scale services.

The project areas of research: Semantic system, application, and attack description, Development of security models and modules for IoT systems, System versus Goal analysis for measurable security.

Conclusions and questions

This Section presents a comprehensive demonstration of smart grid safety/security management as systematic approach to planning,

organisation and allocation of resources, humans and tasks with aim to reach demanded safety/security level of smart grid. The following elements of SSMS are selected:

- humans (owners, operators, etc.),
- safety/security assessment and assurance processes (safety processes);
- IoT technologies which support the safety/security processes in SG;
- documentation and smart grid assets – facilities which are objects of safety/security processes implementation in SG.

The role of IoT devices (such as sensors) in implementation of safety/security management is very vital. The use of sensors will greatly improve the quality, speed, safety of the production process. During process monitoring these devices can quickly send an alert every time a problem occurs during this process. Monitoring systems and sensors will help with solving these problems and increase safety/security.

Connecting legacy equipment to smart grid IoT applications allows electric utilities to:

- **Push Data in Real Time** – Relying on centralized polling of data causes significant latency and limited ability to scale. Many IoT devices poll data locally and create data models that can communicate with traditional SCADA systems as well as cloud-based platforms to take advantage of modern web services.

- **Leverage Cellular Infrastructure** – IoT devices allow grid monitoring devices to take advantage of cellular connectivity, forming secure connections with multiple backends or cloud systems.

- **Leverage the Cloud** – As distributed grids become increasingly complex with many more devices to manage, IoT devices are able to connect to cloud-based infrastructure and share real-time data and analytics with users through cloud-managed dashboards.

- **Enhanced Grid Security** – Legacy grid monitoring systems (when IP-networked) are vulnerable to cyber attacks. They lack robust cybersecurity capabilities because the legacy protocols were not designed with modern threats in mind. IoT devices can minimize security risks using the latest security methodologies and update and patch security features to adapt to ever-changing cybersecurity threats.

In addition, this study gives an overview of challenges in smart grid safety and security in context IoT which are existing due to the impact of safety factors and influences between SG systems' safety states. IoT based smart grid security/safety challenges and risks could be downplayed through selection of smart grid model that allows the influence formalization.

This study gives the short overview of IoT based smart grid safety and security assessment and assurance, set of smart grid safety strategies is also described in this section. The short highlights for Resilience-oriented measurement of quality of IoT based smart grid services and SDOE-based development of resilient digital substation is given.

In order to better understand and assimilate the educational material that is presented in this section, we invite you to answer the following questions.

1. What is safety and security of smart grid?
2. Do IoT technologies have a positive impact on smart grid safety/security?
3. What are the main challenges in smart grid safety and security in context IoT?
4. Name the main smart grid and I&C safety factors? How to decrease their negative influence on safety and security?
5. What are main components of smart grid model? Name them.
6. Why is it important to take into account NPP safety for smart grid?
7. What are the features of IoT based smart grid safety and security assessment and assurance?
8. Name the main type of influences between smart grid systems?
9. What is first safety strategy about?
10. Name the main steps of strategy of redistribution with the mandatory allocation of sufficient resources?
11. What is a smart grid resilience? How IoT can improve this?
12. How can it be measured?
13. How IoT security can be improved by SDOE-based development techniques?

References

1. Internet of Things-aided Smart Grid: Technologies, Architectures, Applications, Prototypes, and Future Research Directions/ Y. Saleem, N. Crespi, M. Rehmani, R. Copeland.
2. A. Basit, G. A. S. Sidhu, A. Mahmood, and F. Gao, Efficient and autonomous energy management techniques for the future smart homes, IEEE Transactions on Smart Grid, in Print, 2016.
3. W. Shu-wen, Research on the Key Technologies of IOT Applied on Smart Grid,” in International Conference on Electronics, Communications and Control (ICECC), 2011, pp. 2809–2812.
4. Y. Wang, W. Lin, T. Zhang, and Y. Ma, “Research on Application and Security Protection of Internet of Things in Smart Grid,” in International Conference on Information Science and Control Engineering (ICISCE), 2012.
5. <https://www.kyrio.com/blog/internet-of-things-impact-on-smart-grid-security>
6. M. Madonna, G. Martella, et. al. The human factor in risk assessment: Methodological comparison between human reliability analysis techniques / Prevention Today, Vol. 5, no. 1/2, 67-83.
7. P. Pekka, Human reliability analysis methods for probabilistic safety assessment / P. Pekka // Technical research centre of Finland. - 2000. - 67 p.
8. A. Swain, THERP, SC-R-64-1338 / A. Swain. — Albuquerque: Sandia National Laboratories, 1964.
9. I. Watson, Review of Human Factors in reliability and risk assessment / Symposium Series No. 93, pp. 323-351.
10. M. Madonna, The human factor in risk assessment: methodological comparison between human reliability analysis technique / M. Madonna, G. Martella // Prevention Today. — №5 (1/2). — C. 67—83.
11. C. Lopez, A. Sargolzaei, et. al. Smart Grid Cyber Security: An Overview of Threats and Countermeasures/ Journal of Energy and Power Engineering 9 (2015).
12. Aloul, F. 2012. “Smart Grid Security: Threats, Vulnerabilities and Solutions.” International Journal of Smart Grid and Clean Energy 1 (1): 1-6.
13. Safety Management Systems Guide for Major Hazard Facilities/<http://www.worksafe.nt.gov.au/SafetyAndPreventions/Documents/mhf-safety-management-systems.pdf>
14. Critical National Infrastructure: The Threat Landscape/ White paper <https://www.thalesgroup.com/sites/default/files/asset/document/thales-critical-national-infastructure-the-threat-landscape.pdf>

15. TLP: White Analysis of the Cyber Attack on the Ukrainian Power Grid http://www.nerc.com/pa/CI/ESISAC/Documents/E-ISAC_SANS_Ukraine_DUC_18Mar2016.pdf.
16. E. Brezhnev, "Risk-analysis in critical information control system based on computing with words' model", in Proceeding of 7th International Workshop on Digital Technologies, Circuit Systems and Signal Processing, Slovakia, 2010, pp. 67-72, 2010
17. Zadeh, L. A. "Computing with Words — Principal Concepts and Ideas, Studies in Fuzziness and Soft Computing, 2012, Vol. 277.
18. П. Кукса, "Методы обучения нечетких систем", <http://pkuxa.org/~pkuxa/publications/fz-learning.methods-iu-04.pdf>
19. The Cyber Resilient Organization in the United Kingdom: Learning to Thrive against Threats, Ponemon Institute, 2015, 34 p.
20. Cyber Resilience Review (CRR): Method Description and Self-Assessment User Guide, Homeland Security, 2016, 49 p.
21. Measuring Critical Infrastructure Resilience: Possible Indicators, Risk and Resilience Research Group. Center for Security Studies, 2015, 14 p.
22. Cyber resilience assessment framework, Honk Kong monetary authority, 2016, 97 p.
23. D. Bodeau, R. Graubart, et al. Cyber Resiliency Metrics, Version 1.0, Rev. 1, 2012.
24. W. Wang, Z. Lum, Cyber security in the Smart Grid: Survey and challenges/ Computer Networks Volume 57, Issue 5, 7 April 2013, 1344-1371 pp.
25. <https://project-sparks.eu/wp-content/uploads/2014/04/sparks-smart-grid-security-analysis.pdf>
26. James D. McCalley, et.al Cyber Security of Smart Grid Communications: Risk Analysis and Experimental Testing/ Springer, Berlin, Heidelberg, 2015.
27. V. Tanyinyong, R.Olsson, M. Hidell, et.al. IoT-grid: IoT Communication for Smart DC Grids / Proceedings of 2016 IEEE Global Communications Conference, GLOBECOM 2016, Institute of Electrical and Electronics Engineers (IEEE), 2016, US.
28. O. Vuković, Cyber-security in Smart Grid Communication and Control / Doctoral Thesis in Electrical Engineering, Stockholm, KTH Royal Institute of Technology, Sweden, 2014, 71p.
29. STOMP - energy STORage for smart Meter Privacy/ <https://www.kth.se/eme/research/topics/energy-storage-for-s/stomp-energy-storage-for-smart-meter>

30. O. Vuković, Security of Fully Distributed Power System State Estimation: Detection and Mitigation of Data Integrity Attacks/ IEEE Journal on Selected Areas in Communications, Vol. 32, # 7, 1500-1508 pp.

31. C. Hagerling, A.Daidone, Felicita Di Giandomenico, et.al. Security risk analysis and evaluation of Integrating customer energy management systems into smart distribution grids /Proceedings of CIRED Workshop, Rome, 2014.

32. Felicita Di Giandomenico, N. Murru, et.al On a Modeling Approach to Analyze Resilience of a Smart Grid Infrastructure / Proceedings of Dependable Computing Conference (EDCC), 2014, UK.

33. Enhancing IoT security through network softwarization and virtual security appliances/

<https://onlinelibrary.wiley.com/doi/full/10.1002/nem.2038>

34. IoTSec - Security in IoT for Smart Grids/
<https://www.mn.uio.no/its/english/research/projects/iotsec/index.html>

PART X. IOT FOR SMART BUILDINGS AND CITY
36. HIERARCHY AND INTERACTIONS BETWEEN SMART IOT SYSTEMS

Prof., DrS. D. A. Maevsky, Ass. Prof., Dr. E. J. Maevskaya (ONPU)

Contents

Abbreviations	196
36.1. Elements of System Theory for IoT	197
36.1.2 Natural and artificial systems	199
36.1.3 The concept of an ideal system.....	201
36.2. Internet of Thing: Hierarchy of Smart Systems.....	203
36.2.1 Constructing of the hierarchical structure for IoT	204
36.2.2 The concept of risk and methods of its evaluation	206
36.2.3 Build of risk matrices and its analysis	207
36.3. Expert assessment method and its applications for the IoT risk analysis	208
36.3.1 Main definitions and purpose	208
36.3.2 Observational error and its evaluation.....	210
36.3.3 Examples of using the expert assessment method for IoT risk analysis	211
36.4 Work related analysis	215
Conclusions and questions.....	217
References	219

Abbreviations

AS – Artificial System

DASD – Direct Access Storage Device

EE – Expert Evaluation

FoT – Fog of Things

IBM – International Business Machines

IoT – Internet of Things

KTH – Royal Institute of Technology

In this section we will consider interesting questions in context of Internet of Things (IoT), in particular IoT for smart cities, considering theory of systems and their hierarchical construction. We have heard the word "hierarchy" many times and intuitively imagine its meaning. For this term there is a series of more or less similar definitions. For example, in [1] the hierarchy is defined as "the arrangement of parts of the whole in a certain order." The word "hierarchy" comes from two Greek words: *ιερός* – sacred and *ἀρχή* – domination. It is believed that this term was first used in the fifth century by Saint Dionysius Areopagite in his treatises "On the heavenly hierarchy." Hierarchically organized forms exist in all spheres of objective reality: inorganic, biological, social; with the emergence of the general theory of systems, the concept of "hierarchy" has become applicable to the description of any system objects.

And here we come to the notion of "system". With their definition, that is, the isolation from the surrounding is a problem. The essence of this problem stems from the emotional expression of the creator of the theory of systems, the Austrian scientist Ludwig von Bertalanffy - "Systems everywhere!". Really, they are everywhere. Everything around us is systems. But in order to determine what such a system is, it is necessary to use concepts that do not belong to any system. And systems are everywhere! What then to use the concepts to explain, and what is a system.

In our first section, we will try to understand, what is a system and plunge into an interesting and fascinating world of the general theory of systems, interpreting it in relation to the systems of Internet of Things.

36.1. Elements of System Theory for IoT

Now we learn about what "system" is, what can be the systems and to which laws they obey. We hope that after you read this section, you will have another understanding about the world that surrounds us.

36.1.1 Key concepts of System Theory

It is necessary to start with definition - and what is the system? Immediately need to say that the only common definition does not

exist. First, this is due to the fact that when we say "System", then in different cases we mean completely different concepts. Thus, by the word "System" we denote a certain theory (philosophical system), way of practical activity (system of labor protection), certain classification of something (periodic system of elements of Mendeleev), way of interpreting reality (decimal system, binary system), set of objects (Solar system), elements of social activity (political system, economic system) and many others. Therefore, to determine, and what is the system, it is necessary to determine in what context we will use it.

Internet of Things is, of course, a technical system. Therefore, by studying the system properties of IoT, we will talk about it as a technical system. There are many different definitions for the technical system, each of which covers one or another aspect of this concept. For example, in terms of [2], the technical system is this «the portion of the universe that is being studied».

The creator of the general theory of systems Ludwig von Bertalanffy gives a wider definition. According to [3], the system is a complex of components that interact with each other. It is intuitive as to what is being discussed. But if you think about it - you will have questions. In this definition is told about the components. Question - components of whole? If it is customary to say that these components are components of the system, then again it is necessary to determine - and what is the system? And we are back to the definition of system again.

Let us turn to another, more detailed definition according to Bertalanffy. In work [4] he says, that "the system is a set of elements that are in certain relations with each other and with the external environment." It's also intuitive. But from a formal point of view, we are again faced with the necessity to determine, and what is an element? And about element of what is being discussed. It is intuitively clear that this is a element of system. And what is the system? And we are back to the beginning.

This situation is not accidental. In 1931, the Austrian mathematician Kurt Gödel [5] proved the theory, which made chaos among mathematicians. Still it is the subject of debate and the lively interest of all - from scientists to housewives. You can read in detail about this theorem and its consequences by reference [6]. The theorem has a strict mathematical formulation, but its consequences go far

beyond the limits of mathematics. In simple language, Kurt Gödel proved that using the terms (alphabet) of the system, it is impossible to describe this system. Do not be confused with the word "system", which again appears in this phrase. Her meaning is deeper. When we tried to determine what a system was, we meant the system at all. But, as we remember, "Systems everywhere"! That is, we use the system to determine the system! System of signs, words, concepts. But again, the system! And Kurt Gödel proved that such a definition is not possible. And he proved it strictly mathematically. All mathematicians of the world agree with it.

Thus, in principle, we cannot define the system, because we are always in this very system, in the system of our world. Outside of this system, according to Saint Dionysius Areopagite, there is only God. And he sees everything from above.

Therefore, we will not do the wrong thing - let's stop trying to do what is impossible. We will use the incomplete definitions given by Ludwig von Bertalanffy. Consider now the basic laws of systems development. After all, if the IoT is a system, then it must obey the laws that are inherent in all systems. But keep in mind that everything that will be said below is inherent not only in IoT. Everything that surrounds us is a system. And we ourselves are just one of the systems. And this means that the laws of the general theory of systems also apply to us.

36.1.2 Natural and artificial systems

Let's return to the point of view of Ludwig von Bertalanffy on the system. We mean his thesis "Systems everywhere". Further development of this thesis can be considered the opinion of I. S. Alekseev: "Any object in solving certain problems with the help of certain cognitive means can be presented as a system" [7].

The outstanding scientist A. I. Uemov and his coauthors [8] consider the system as a complex of things, their properties and relations between things and properties. It is proposed to highlight a system factor that distinguishes a system from not a system. As such factor is used an intended purpose of the system. That is, it is assumed

that any system must have some result, in order to achieve, that this system exists.

By this point of view, we are confronted with very interesting questions regarding this result. Indeed, let's try to answer the simple question - what does the solar system exist for? It is a system in terms of all definitions. There are elements of the system, in our case: it is the Sun, planets, their satellites, asteroids and so on. There is an interaction between these elements - they interact with gravity. But for what does this system exist? It is hard to believe, that only for the existence of mankind on one single element of the system! Maybe there is some kind of higher goal of the existence of the solar system, but we are not exactly aware of it.

Other similar questions - and why there is the sea, mountains, forest, rivers? Well, not only, so that we can go there. That is, man can conclude that not all systems have the result of their existence. This criterion is the presence of a result, or as G. S. Altshuller says, "The main function of the system" [9] is a criterion for the division of all systems into two large classes: natural systems (native systems) and artificial systems.

Only artificial systems have the main function, the result of the work. These systems are created by man to meet human needs. For example, the main function of the calculator is the execution of calculations, and the clock - time tracking. And the main function of the storage computer devices is to storage of information. An artificial system can have not one function, but depending on its specific application, we can always distinguish one function as the main one.

It is believed that systems created by nature, in contrast to artificial systems, do not have a basic function. Do they really do not, or we just do not know it - this is a philosophical question. There is no answer to this question. Yes, and we are not interested in this issue, because Internet things are, of course, an artificial system.

Every artificial system is not a unchanged. It goes through its life cycle of ideas, through technical devices, to the end of its existence. So, once, trains were brought into motion by steam locomotives. By the way, search the Internet who and when did the first steam locomotive? The steam locomotives have lasted for about 200 years and have long since gone into the past. This is the fate of any artificial system.

Imagine someone and ever, maybe in our life, will not remember what a Smartphone, using any other, fundamentally new artificial system. Can we make a prediction - and what can this artificial system be? It turns out that we can. After all, all artificial systems follow one simple law - the main law of the development of artificial systems. Let's get acquainted in detail with this law.

36.1.3 The concept of an ideal system

Now we will consider the concept of "ideal system" and learn about the basic law of the development of artificial systems. Consider this on an example of memory devices; we will get the basic law of the development of artificial systems. To do this, look at the history of the development of storage devices.



Fig. 36.1 – HDD Storage

Device for IBM 360, 1980 year

In Fig. 36.1 is showed an image of device for access to information on hard drives, which were used in computers in the 1970s (the word "computer" was not used at that time) in the IBM 360 series. It was a device with measuring 80 by 80 centimeters and about one meter high and weighing about 50 kilograms. In it is possible to mount a hard magnetic disk (as shown in the picture above), which is a package of ten aluminum disks with a diameter of 40 centimeters. The height of such a package was about 20 centimeters, and the weight - 5 pounds. But this did not seem inconvenient, because one such package of disks had a huge capacity - as much as 20 megabytes. Yes, 20 megabytes, it is not a mistake! Everyone who came to work on IBM 360 brought his information at such information carrier. The package of disks was spinning by an electric motor with power of 1 kilowatt.

In 1976, for the IBM 62PC computer, also called Piccolo, was developed the first built-in hard drive (Fig. 36.2) - the prototype of

modern Winchester. If you do not know why the hard drive got that name, refer to the link [11].

According to [12], the IBM 62PC (Piccolo) 65 MB capacity drive introduced in 1979 used six 8-inch disks with one surface dedicated to servo position data. The drive employed a sector servo



Fig. 36.2 – HDD for IBM 62 PC,
1976 year

position control and a rotary voice coil actuator to eliminate temperature effects. The lower power consumption of the small disk diameter eliminated the need for external air cooling and simplified integration of the unit as sub system into a variety of machines. A sealed disk enclosure design assured a reduction in disk surface contamination and improved reliability. IBM also sold the

unit as the 3310 attachable direct access storage device (DASD). 360,000 units were shipped from Jan 1979 through Feb 1990. As you can see, size and weight of the new drive have decreased. Accordingly, power, which it consumed, is also reduced. But despite this, its main function, which can be characterized by the amount of stored information, began to use better - the capacity of the device has increased to 65 MB.

The modern Seagate Barracuda Pro hard drive has a capacity of 10 TB, with a power of only 7 Wt and a mass of 0.6 kilograms (Fig. 36.3). Its capacity has increased by five hundred thousand times, in comparison with the drive on Fig. 36.1, and the consumed power at the same time decreased by 160 times! The mass at that time became less than eight times.

Analyzing of the tendency to reduce the weight, size and energy consumption, we can already say in what direction the memory devices develop - all indicators de-crease, in addition to their main function. It is not difficult to see that this trend is also true for all other artificial systems.



Fig. 36.3 – Seagate BarraCuda Pro, 2018 year

Continuing on, we can predict that an ideal storage device should not have mass at all, should not consume electricity, but should only store information. Actually, for this purpose they are intended! Such a system, which does not exist, but whose main function is performed, is called the ideal system. And the law, according to which all artificial systems develop in the direction to ideal, is the main law of the development of artificial systems.

By continuing to analyze the systems that accumulate information, we can see that these systems in their development have almost reached the level of the ideal system. Today, each computer has access to cloud

storage repositories. That is, we have access to memory that is not physically present on our computers. For example, all users of Microsoft Office 365 receive 1 TB of memory in cloud storage One Drive for free [12]. On your computer, this cloud storage with a large capacity does not take up space at all, does not matter and does not consume electricity. And the main function is fulfilled - we can record and read information. And this is already an ideal system.

Modern cloud storage is one of the elements of the general system of Internet things. Now is the time to get acquainted with the hierarchy of the systems that are part of it.

36.2. Internet of Thing: Hierarchy of Smart Systems

The attempts to construct various hierarchical IoT models were made repeatedly [18, 19, 20]. The basis for the hierarchy construction in [18] is the architecture of IoT construction (sensors, network, applications). In [19] the five-layered (five levelled) model is offered: edge technology layer (level), access gateway layer (level), internet layer (level), middleware layer (level) and application layer (level). In

[20], three layered model (three levelled) is suggested. This model has sensing extension layer, network layer and application layer. Sensors and physical devices take part in sensing extension layer. Network layer and application layer fulfills similar task to other models.

The variety of hierarchical models is completely justified because IoT is a multifaceted object and each of the hierarchies is one of its facets. Hereinafter the authors will suggest one more approach to the hierarchy construction based on IoT fragmentation into subsystems based on the main function executed by them. It is true, IoT is an artificial system made by a moreover, as we already know from [1] every artificial system necessarily possesses its own main function.

36.2.1 Constructing of the hierarchical structure for IoT

According to the type of the main function, the IoT can be represented in the form of hierarchical structure consisting of nine levels:

1. The system of “Internet of things”
2. Smart state
3. Smart area (region, state, federal district, etc.)
4. Smart city
5. Smart district of the city
6. Smart house (apartment house)
7. Smart apartment (dwelling)
8. Smart room (workplace)
9. Smart device.

At the first highest level of hierarchy the IoT system itself exists as a whole phenomenon of the planetary scale. The system functions at this level is to organize the interstate cooperation to solve the problems of civilization survival as a whole. This can be achieved on the account of optimum and timely solutions of environmental, demographic, raw materials and other international problems of modernity.

At the second hierarchical level there is a smart state. Its main function is to ensure the rights and freedoms of citizens on the account of the optimum governing and close interconnection of all state structures.

The third level is the one of a smart region as an independent territorial association in the state. The main IoT function at this level is to organize the sustainable operation of the region's infrastructure.

At the fourth level of the hierarchy a smart city exists as a part of region. We should stress that the word combination “smart city” means not only a modern metropolis with several million inhabitants. City is a territorial unit with its own borders within which some amount of residents’ lives. In this aspect, the word “city” means just such a territorial formation. “City” in IoT system is both a metropolis and a small village. The main function of this territorial formation depends on its size, geographic position and natural resources. The main IoT function at this level is the optimum governing of all processes providing vital activity of the city and its connections with other cities.

The fifth level of IoT system is a smart city district. City district is a strictly territorial unit, boundaries of which are conditional. The main IoT function at this level is governing and controlling the systems providing normal conditions of vital activity and interconnections of objects existing in the district territory.

The sixth and seventh IoT levels are devoted to smart house and smart apartment. We are integrating both of these concepts because one can sometimes draw a clear line between them but they are sometimes united in one whole. E.g. if we are speaking of an apartment house these concepts are different. However, if we mean a private house in a cottage village then the concepts “house” and “apartment” are different.

The main function of a smart apartment (or private house) is comfortable conditions of habitation of some small separate group of people – a family as well as its security and energy saving. IoT function in an apartment house is accounting and controlling the resources consumed by a separate apartment.

The eighth IoT level is a smart workplace, the role of which a separate room plays more often in the apartment or private house. The main function at this level is the provision of comfortable working and rest conditions of one or a few persons.

The last, ninth level consists of strictly speaking smart things that have termed the whole direction – Internet of things. A smart thing is e.g. TV, fridge, washer, microwave, etc. These are things surround a modern person at present but they become more and more intellectual every year. Even now a smart TV is capable of recording the necessary

program in the absence of a host independently, and a smart slow cooker – making dinner by his (a host) returning. All this determines the main function of smart things – to meet the specific human needs at a specific time.

As we have seen in transiting from the lowest level to the highest ones of this hierarchy the globalization of the main function occurs, and it becomes more and more common and multipronged. However, IoT is a technical system, in which various accidents and damages are possible. Any accident or damage is ultimately the function execution discontinuation by a subsystem. That is why the evaluation of risks for vital activity of a person, which arise in stopping the main function execution at each of the nine levels of the Internet of things system is a very important and interesting problem.

36.2.2 The concept of risk and methods of its evaluation

In this context the term “risk” will further preserve its classical definition as the characteristic of situation which has an uncertain outcome in the obligatory presence of adverse effects. To assess the risks the product of probability of an adverse event occurrence by the quantitative assessment of damage from such event is commonly used. However, this approach to the risk assessment is lately criticized. For example, Nassim Nicholas Taleb in the book “Black Swan” [13] notes that events the probability of which is “in the tails of Gaussian curves” have as rule not only adverse but also catastrophic effects. Besides the quantitative damage caused by an event is still open to question. How one can count, for example, a human life in money? Uncertainty of evaluation can be seen especially clear in risk assessment in heterogeneous systems. E.g. in terms of money the fire damage in an apartment and the one in an ammunition depot cannot be compared to each other. However, from the viewpoint of a host of the apartment his personal damage is catastrophic while he is not sensitive to the fire damage somewhere far away in an ammunition depot.

The intellectual subsystems of IoT system distinguished in section III are just such kind of heterogeneous subsystems. That is why in the given article in order to assess the risks in IoT the relative risk

evaluation is applied, which is indicated based on negative consequences of some event for this very subsystem.

36.2.3 Build of risk matrices and its analysis

We will assess the risks arising in smart IoT subsystems on a twelve-point scale the basis of which is the extent of negative effect of risk factor on the main function execution by appropriate subsystem. Let us consider the risk degree scale.

Degree 0 – risk is fully absent.

Degree 1 – there is the most minimal risk the consequences of which are negligible for system functioning, i.e. risk factor may not be eliminated.

Degree 2 – there is a risk the consequences of which are noticeable but do not impact on the main function execution.

Degree 3 – the risk with tangible consequences; risk factor should be eliminated but not immediately.

Degree 4 – the risk with tangible consequences, which have to be eliminated immediately.

Degree 5 – the risk with significant consequences interrupting the main function execution in the acceptable period.

Degree 6 – risk with the consequences interrupting the main function execution in the period close to critical one but not exceeding it.

Degree 7 – risk interrupting the main function execution in the period equal to critical one.

Degree 8 – risk interrupting the main function execution in the period of time, which is more than critical but on eliminating the factor the main function can be restored.

Degree 9 – risk in which the restoring of system functioning is unlike but possible.

Degree 10 – the restoring of functioning is impossible but a system (its elements) is kept.

Degree 11 – complete and irreversible destruction of all of the system elements.

The fact that this scale is based on the main function execution of a subsystem allows applying it in two cases. Firstly, it allows assessing the extent of risk arising from the effect of some negative factor, which

emerges in the given subsystem, on the subsystem itself. Secondly, we are able to assess the so-called “cross risks” which arises from the effect of some negative factor, emerging in the given subsystem, on the effect of the main function execution by the other subsystems. Wherein we can create a risk matrix of the following form: along the main diagonal the own risk assessments are placed, and on the sides – the ones of cross risks. This is especially valuable for IoT system, the subsystems of which are closely integrated one in another.

36.3. Expert assessment method and its applications for the IoT risk analysis

36.3.1 Main definitions and purpose

Method of expert evaluations is widely used in conditions when a management decision must be made in context of incomplete or fuzzy information. Very often man has to perform forecasting development of the situation, guided by such uncertain categories as “better - worse”, “cheaper - more expensive”, “faster - slower” and so on. As you can see, not all data here can be expressed in numbers. So, if we have two things and need to compare them, which one is cheaper, and which is more expensive, this evaluation is more often not a difficult task. It is enough to open price-lists and compare costs to solve this task. It’s harder to rate “better - worse”. First, the price-lists here will not help, and secondly, these concepts themselves are often vague. Different people can understand the categories “better” and “worse” in their own way, guided by such a fuzzy foundation as everyday experience.

However, in most cases there is a need to build forecasts precisely when a fuzzy formulation of the problem and guided by fuzzy criteria. For example, the answers to such questions are important: “How will the economic situation change over time?”, “Will the environmental safety of industrial production be ensured?”, “What method of treatment to choose for this disease?”, “Will this system be sustainable under these external influences?”. Each of us have repeatedly encountered in life with similar questions. When solving them, people usually ask for advice from other, more experienced people. It is clear that the more experienced these people are and the

greater their number, the more accurate the forecast can be made on the basis of their opinions.

The scientific direction of decision-making based on the experience of qualified specialists (experts) began to develop in the 40s of the last century. This scientific direction was called the “Method of expert evaluations”. Methods of expert evaluations — these are methods of organizing work with expert experts and processing expert opinions. These opinions are usually expressed partially in quantitative, partially in qualitative form. Expert research is carried out with the purpose of preparing information for decision-making. To carry out work on the method of peer review, need to create a working group that organizes the activities of experts, united in an expert group.

There are two groups of expert evaluations: individual evaluations that are based on using the opinions of individual experts, independent of each other; collective evaluations based on the use of collective expert opinion.

For evaluation, experts can use the following methods:

1. Ranking is the arrangement of objects in ascending or descending order of any property. Ranking allows you to choose from the studied set of factors the most significant.

2. Pair comparison is the establishment of a preference for objects when comparing all possible pairs. It is not necessary here, as in the ranking, to order all the objects, it is necessary in each of the pairs to identify the more significant object or to establish their equality.

3. Direct evaluation. It is often desirable not only to order (rank the objects of analysis), but also to determine how much one factor is more significant than the others. In this case, the range of changes of characteristics of the object is divided into separate intervals, each of which is assigned a specific score (point), for example, from 0 to 10. That is why the method of direct evaluation is sometimes also called the point method.

Various methods of mathematical statistics are used to analyze the results. These methods can be combined and vary in depending on the type of task and the desired result. For the formation of a generalized evaluation of the group of experts are used average values most often. Sometimes it is necessary to determine how important a particular factor is in terms of some criterion. In this case, at the

beginning you need to determine the weight of each factor, and then use the weighted average.

36.3.2 Observational error and its evaluation

In the case of participation of several experts in the survey, differences in their evaluation are inevitable, but the value of this difference is important. Group evaluation can be considered sufficiently reliable only if there is a good consistency in the responses of individual specialists. For the analysis of variance and consistency of estimates, statistical characteristics are used - measures of variation. Most often, as a measure of the variation are used variation range, average linear deviation, standard deviation and variance. These values are calculated based on the results of expert evaluation using the formulas:

variation range – $R = x_{\max} - x_{\min}$:

average linear deviation – $a = \frac{1}{n} \sum_{i=1}^n |x_i - \bar{x}|$;

standard deviation – $\sigma = \sqrt{\frac{1}{n} \sum_{i=1}^n (x_i - \bar{x})^2}$.

In these formulas: n – the number of evaluations, \bar{x} – the average of all evaluations.

The method of expert evaluation has the following advantages:

1. The possibility of obtaining quantitative estimates in cases where there is no statistical information, or the indicator has a qualitative nature.

2. The quickness of obtaining results.

One of the main drawbacks of method is that the accuracy and reliability of the study primarily depend on the competence of the specialists participating in the survey. There are no guarantees that the estimates obtained are valid. The existing methods for determining the reliability of expert evaluation are based on the assumption that, in the case of consistency of expert opinions, the reliability of the estimates is guaranteed. It is not always possible to agree with this statement, as there are cases when separate experts, who disagree with the majority opinion, gave correct estimates.

Consequently, the unanimity of most experts is not always a criterion for the reliability of estimates. Hence the necessity for careful selection of experts. The fact is that when discussing many issues, especially non-standard ones, and in marketing and advertising they are practically all non-standard, highly qualified experts should participate. The forecasts made by "average" experts will be based at best on traditional, customary estimates, while highly qualified specialists will discover and appreciate the hidden factors.

Often, expert evaluations are not sufficiently stable, i.e. an expert can evaluate the same events in several re-examinations differently. The more stable the scores, the more you can trust them. However, in practice, re-examination is rarely carried out due to organizational and financial problems, i.e. there are certain difficulties in conducting an expert survey and processing the data.

The reliability of evaluations can be improved as follows. It is necessary to analyze data on discrepancies of expert evaluations and their actual values found in the process of realization of events and make the appropriate reassessment of the competence of experts. Experts with low competence, in the future is not recommended to involve in the examinations.

36.3.3 Examples of using the expert assessment method for IoT risk analysis

For the quantitative risk assessment with the help of this scale a method of expert evaluation is applied. The authors of this article and the other disinterested specialists in IT field participated as the experts. In all, 25 experts were involved for risk assessment. The results of risk assessment in IoT subsystems are presented in table 1.

The table contains nine lines and nine columns, in which the mean arithmetic assessments of risk given by all experts are registered. The numbers of lines and columns corresponds to the ones of subsystems allocated in section 36.2.1. In the cells with the similar numbers of line and column (situated on the main diagonal) the degrees of risk arising from the effect of some negative factor, which emerges in the given subsystem, one of the main function executions by this exact subsystem are presented. In the cells with line number i and

column j the degrees of risk arising from the effect on the subsystem with number i from a negative factor, which emerges in the subsystem with number j (cross risks) are given.

First of all, we can see that the most influential system is the system of IoT at whole. Rank of influence of this system on another systems is 7,3. According to degree`s scale (section 36.2.3) this rank corresponds to the degree 7 – “Risk interrupting the main function execution in the period equal to critical one”. The most depended system is subsystem 7 – “Smart house”. The risk of negative effects of other subsystems on this system also corresponds to degree 7.

Table 36.1 Results of Risk Assessment for IoT Smart Systems

		1	2	3	4	5	6	7	8	9	
		The system of IoT	Smart state	Smart area	Smart city	Smart district	Smart house	Smart apartment	Smart room	Smart device	Average
1	The IoT system	10,9	7,1	6,0	5,2	3,9	3,0	2,5	2,0	1,3	4,7
2	Smart state	8,9	10,9	7,2	5,8	4,6	2,9	2,3	1,6	1,1	5,0
3	Smart area	8,3	8,7	10,9	7,2	5,8	3,7	2,8	2,1	1,5	5,7
4	Smart city	7,8	7,8	8,4	10,8	7,3	4,2	3,3	2,6	1,8	6,0
5	Smart district	7,0	7,0	7,6	8,4	10,8	6,2	4,4	3,4	2,2	6,3
6	Smart house	6,2	6,4	6,6	7,1	7,4	10,8	7,0	5,1	3,8	6,7
7	Smart apartment	6,0	6,2	6,3	6,7	7,0	8,2	10,8	7,6	5,0	7,1
8	Smart room	5,6	5,7	5,9	6,4	6,5	7,6	8,5	10,8	6,0	7,0
9	Smart device	5,4	5,3	5,7	5,7	6,0	6,6	7,1	7,4	10,7	6,6
Average		7,3	7,2	7,2	7,0	6,6	5,9	5,4	4,7	3,7	

In order to facilitate the analysis, we should consider several diagrams, which are created based on the data of table 36.1.

In Fig. 36.4 a diagram of dependence of the degree of risk for the main function execution by IoT system as a whole (level 1 of the hierarchy) on the negative factors, arising at all other levels, is presented. The numbers of these levels are given along the axis abscissa of the diagram.

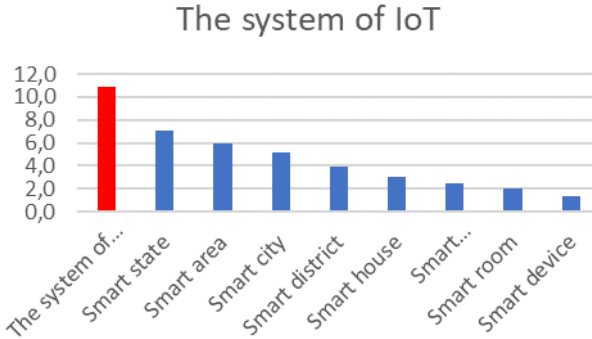


Fig. 36.4 – The degrees of risks for IoT system (level 1)

As we can see in Fig. 36.4 the highest risk for IoT system corresponds to the global negative factors arising in this very system. In transitioning to the lower levels of the hierarchy the risk degree drops fast. A negative factor arising in a subsystem of level 9 (a separate sensor in Fig. 36.5.

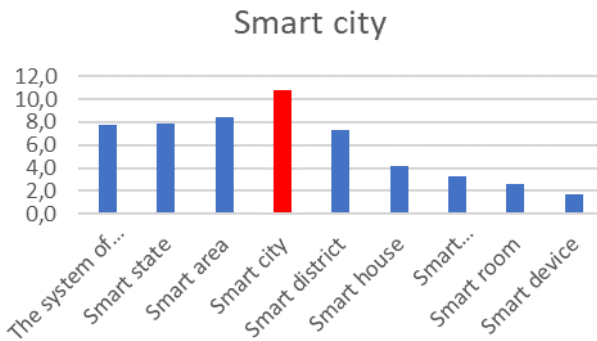


Fig. 36.5 – The degrees of risks for IoT system (level 4)

a workplace) does not effect on the main function execution by a smart house system.

In Fig. 36.5 the dependence of the degree of risk for the main function execution by a subsystem of level 4 (smart city) on the negative factors, which emerges at all other levels, is shown. To make the comparison of the degrees of risk more suitable the scale of the axis ordinate is similar to the one in Fig. 36.4. All experts have come to one and the same conclusion: the risks arising at the “smart city” level (in the subsystem of lower level of the hierarchy) are generally lower than for IoT system. At this level the trend of lowering the risk degree in rising the subsystem hierarchy level persists as well. Indeed, all risks for subsystems 5, 6, etc. are lower than the degree of the own risk (marker emphasized with a rhomboid in the curve). Along with this, the negative factors arising in the higher-level subsystems are simultaneously the most dangerous for the functioning of “smart city”. However, the risks, which emerge in the subsystem of level 9 (“smart things”) do not effect on the “smart city” functioning at all. However, at the level of the “smart house” subsystem (level 6 of the hierarchy) the degree of risks changes (Fig. 36.6).

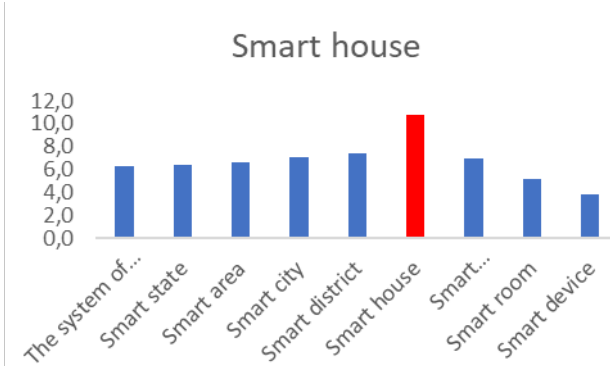


Fig. 36.6 – The degrees of risk for the “smart house” system (level 6)

Firstly, the mean value of risk degree is lower here as a whole than in subsystems of the higher hierarchy level. Secondly, unlike the subsystems considered earlier the negative factors, emerging in the subsystems of higher hierarchy levels, effects more and more on the

“smart house” subsystem functioning. And, thirdly, effects of risks, arising from the malfunction of “smart things”, on the “smart house” subsystem functioning cannot be negligible.

In Fig. 36.7 the dependence of the degree of risk for the main function execution by the subsystem of the lowest level (level 9 – “smart device”) on negative factors which emerge at all the levels, is shown.

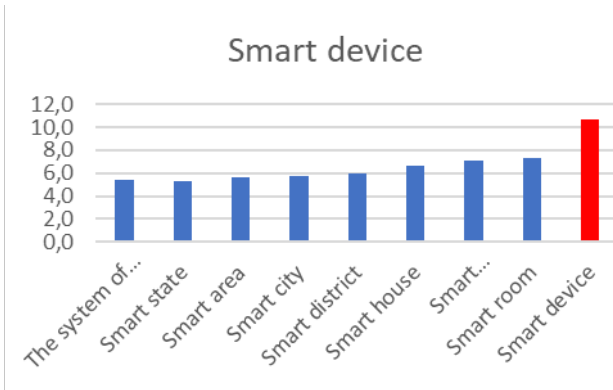


Fig. 36.7 – Degrees of risk for the system “smart device” (level 9)

The nature of the risk degree changes is completely different here. The “smart things” functioning impacts on all the subsystems. The lower is a subsystem in the hierarchy the more is the effect. And certainly, the greatest danger for a “smart thing” functioning are risk factors inherent in this exact “smart thing”.

36.4 Work related analysis

Internet of Things in general and the problem of its safety and security in particular is a relatively new line of research. However, in recent year the significant growth of number of articles dealing with IS reliability and safety can be observed. All researchers understand that widespread AS IoT implementation in the modern society can have risky consequences for its existence.

G. Bandini from KHT, Sweden, wrote that the virus attack on uranium enrichment plants in Iran in 2010 was without radiation

leakage and human victims only by chance [14]. But this attack has shown that a potential target of terrorists can become the objects the destruction or disruption of which will influence catastrophically on the human habitat.

A.-M. Rahmani with coauthors from KTH [15] give their attention to one of the particular issues – IoT system safety used in the field of public health. The real scheme of storing and processing the data concerning chronic diseases of the elderly is taken as the basis. In the article the heuristic approaches are proposed to analyze the risks arisen in storing the personal information in this system.

In 2010, on the conference “II Congresso Internamonal e VI Encontro Nacwonal de RISCOS”, University of Coimbra, Portugal, was presented analysis of components of such concepts as “safety” and “security” [16]. The authors argue that these concepts contradict each other quite often when they are used for complex industrial control systems. Nevertheless, in order to decrease the risks in operating the industrial control systems one should consider these concepts only in the combination with each other. According to the authors’ opinion, it is the methods of system engineering proposed in this article which are able to be useful.

The authors team from Newcastle University [17] the risks of widespread introduction of “smart buildings” are investigated. They proposed a multi-model methodology for assessing the security of these systems, which utilizes a suite of modelling, simulation, and analysis tools for designing cyber-physical systems. Using a fan coil unit case study, the authors has shown how its security can be systematically assessed when subjected to Man-in-the-Middle attacks on the data connections between system components.

Article [18] deals with the analysis of safety and risks arising in the so-called “Fog of Things” (FoT). The origin of FoT concept is associated with “Internet of things” development. After Internet of things introduction many objects surrounding humans have built-in microprocessors capable of solving the computational problems. Smart phones, “smart watch”, “smart spectacles”, etc. can be referred to such kinds of objects. This in its turn allows distributing the calculation problems solved by humans among these devices. Such type of parallelism permits to greatly increase the speed of problem solution and simultaneously relieve the load of cloud servers. The computer

processing the data can perform their processing not on account of the load on cloud but on account of the neighboring “smart” devices, which are situated near the computer. Thus, the cloud “descends” to an end user and its components are the “smart” devices surrounding a user. Such a descending cloud forms “Fog of Things”. And besides the devices, which form the fog, do not necessarily belong to that exact end user! Any of them can be switched off and shifted to solving another problem any moment. E.g. if your neighbor runs his own data processing on your smart phone without your (and his) knowledge but at IoT server will then you can switch your smart phone off and interrupt this processing any moment. If this situation is not correctly approached to the risks of data loss are possible. Article [18] discuss existing research works and gaps in resource allocation and scheduling, fault tolerance, simulation tools, and Fog-based microservices.

Of all the analysis of articles presented here we have come to the two important conclusions.

Firstly, introducing the IoT technology in human life, we face along with the obvious advantages, the serious threats of technological and social nature. At that, these threats can potentially emerge actually in all directions of IoT implementation.

Secondly, in order to decrease the risks in operating the IoT systems one should together consider both concepts – safety and security. At last, we should note that the authors in their majority aim at the researches of risks and harmful consequences of comparatively particularistic fields. However, at present there is no research of IoT system risks in general. After all each of the directions considered in this analysis cannot exist and function apart from the others. All of them are connected with each other and form a system. That is why outside the analysis presented in the articles the risks remain, which emerge in interacting the individual subsystems united in one common system called “IoT”.

Conclusions and questions

On the foundation of these results the following conclusions of the degrees of risks emerging at each of the structure levels can be made:

1. Each of the subsystems emphasized in our paper effects on risks, which are global for all IoT system;

2. The total degree of risks decreases as the subsystem level lowers.

3. The risk factors arising in the given subsystem do not lead to the biggest risk for this exact subsystem in all cases. It can be numerically seen in table 1, in which the maximal number is not always along the main diagonal. The examples of such kinds of subsystems are “smart city”, “smart district of the city” and “smart apartment”.

4. The biggest risks emerge in the highest-level system – the one of Internet of Things as a global planetary object. At present IoT is not still planetary. But its fast growth shows that the humankind has not a lot of time to analyze the probable global risks and to develop the means to counteract these risks.

In order to better understand and assimilate the educational material that is presented in this section, we invite you to answer the following questions.

1. What is a system?
2. Why is every object around us a system?
3. Give examples of systems that you know.
4. Who is the founder of the general theory of systems?
5. What does general systems theory study?
6. What is a natural system?
7. What is an artificial system?
8. Define the basic function of the systems.
9. Why only artificial systems have the main function?
10. What is the ideal system?
11. Formulate the basic law of the development of artificial systems
12. Give examples of the development of artificial systems in accordance with the basic law.
13. Give examples of IoT systems.
14. By what criteria in this section were the subsystems of the Internet of things classified?
15. Can you suggest other signs to classify the Internet of things systems?
16. What is risk?
17. What do you know about risk assessment?
18. What risk scale was proposed in this section?
19. What is the method of expert estimates?

20. What are the requirements for an expert group?
21. In what cases the use of the method of expert assessments is most justified?
22. What is a weighted average?
23. How can we assign weights for assessments that are performed by individual experts?
24. What methods do you know about processing the results of expert evaluations?
25. How to evaluate the estimation error in the method of expert assessments?

References

1. Wolf, A. "A history of science, technology and philosophy in the 16th and 17th centuries". Bristol: Thoemmes Press, 1999
2. Lee, Edward. "The Past, Present and Future of Cyber-Physical Systems: A Focus on Models. Sensors" (Basel, Switzerland)? 2015. doi:10.3390/s150304837.
3. Bertalanffy, Ludwig Von. "General system theory" - A Critical Review. *General Systems* 7, 1962, pp. 1-20.
4. Bertalanffy, Ludwig Von. "The History and Status of General Systems Theory". *The Academy of Management Journal*, 1973, Vol. 15, No. 4, General Systems Theory, pp. 407-426.
5. Gödel, K. "Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme. Monatshefte für Mathematik und Physik", 1931, No. 38, pp.173-198.
6. P. Smith, "An introduction to Gödel's theorems". Cambridge: Cambridge University Press, 2013.
7. Алексеев И. С. "Способы исследования системных объектов в классической механике", Системные исследования. Ежегодник, 1972, стр. 73.
8. Уемов, А., Сараева, И., Цофнас А. "Общая теория систем для гуманитариев". Warszawa: Uniwersitas Rediviva, 2001, стр. 37.
9. Альтшуллер Г. С. "Алгоритм изобретения". Москва: Московский рабочий, 1969, стр. 81
10. Stevens, L. D. "Evolution of Magnetic storage", *IBM Research and Development Journal*, 1981, No. 25, pp. 1-3.
11. "IBM Archives: IBM 3340 direct access storage facility", www-03.ibm.com, 2018. [Online]. Available: https://www-03.ibm.com/ibm/history/exhibits/storage/storage_3340.html. [Accessed: 30-Nov- 2018].

12. SearchMobileComputing. "What is Microsoft OneDrive? - Definition from WhatIs.com. [online] Available at: <https://searchmobilecomputing.techtarget.com/definition/Microsoft-OneDrive> [Accessed 13 Nov. 2018].
13. N. Taleb, *The black swan*. New York: Random House, 2012.
14. G. Bandini et al. "Safety Analysis Results of Representative DEC Accidental Transients for the ALFRED Reactor", International Conference on Fast Reactors and Related Fuel Cycles: Safe Technologies and Sustainable Scenarios (FR13), 2013.
15. A.M. Rahmani et al. "Smart e-Health Gateway: Bringing Intelligence to Internet-of-Things Based Ubiquitous Healthcare", In 2015 12th ANNUAL IEEE CONSUMER COMMUNICATIONS AND NETWORKING CONFERENCE, 2015, pp. 826–834.
16. A. Amílcar and M. Alves da Silva, "EPISTEMOLOGIA E MECÂNICA DO RISCO: REFLEXÕES", in II Congresso Internamonal e VI Encontro Nacional de RISCOS, Coimbra, 2010.
17. Mace, C. Morisset, K. Pierce, C. Gamble, C. Maple and J. Fitzgerald, "A multi-modelling based approach to assessing the security of smart buildings", *Living in the Internet of Things: Cybersecurity of the IoT - 2018*, 2018.
18. R. Naha, S. Garg, D. Georgakopoulos, P. Jayaraman, L. Gao, Y. Xiang and R. Ranjan, "Fog Computing: Survey of Trends, Architectures, Requirements, and Research Directions", *IEEE Access*, vol. 6, pp. 47980-48009, 2018.

37. DEVELOPMENT OF SMART SBC SYSTEMS

Prof., DrS V. A. Bousher, Prof., DrS A.O. Bojko (ONPU)

Contents

Abbreviations	222
37.1 Classification of the Building Management System, the purpose and basic properties of control, executive and sensor elements	223
37.1.1 Introduction in Smart House and IoT systems	223
37.1.2 Classification of intellectual components, sensors, executive units of Building Management Systems	229
37.1.3 Subsystems of Smart House: microclimate control, lighting, security in residential and industrial premises.....	231
37.2 Organization of the interaction of subsystems and elements of Smart House and IoT.....	237
37.2.1 Microclimate control – functions, executive and sensor units	237
37.2.2 Lighting – lux meters, astronomical timers, security components as sensor and control units in lighting subsystem.....	241
37.2.3 Security subsystem – interaction with lighting, access control and protection subsystems	243
37.3. Construction of Smart House and IoT subsystems based on Moeller / Eaton xComfort.....	243
37.4 Work related analysis	245
Conclusions and questions.....	245
References	247

Abbreviations

BMS – Building Management Systems

CA – Collision Avoidance

CNR – National Research Council

CSMA – Carrier Sense Multiple Access

HVAC – Heating, Ventilation, Air Conditioning

EIB – European Installation Bus

FC – Frequency Converter

GSM – Groupe Special Mobile

LED – Light-Emitting Diode

NTC – Negative Temperature Coefficient

PWM – Pulse-Width Modulation

SBC Smart Building and City

TRIAC – TRIode for Alternating Current

USB – Universal Serial Bus

37.1 Classification of the Building Management System, the purpose and basic properties of control, executive and sensor elements

37.1.1 Introduction in Smart House and IoT systems

The most important factors affecting health, productivity and quality of a person's rest are the conditions in which they are located. These terms can be divided into several groups:

1. Air quality, which consists of a comfortable ratio of temperature, humidity, flow velocity and level of harmful impurities in the air;
2. Lighting in the room and surrounding areas;
3. Water and heat supply;
4. Human and Home Security.

Automated systems that solve problems related to the provision of necessary conditions for these groups, today must take measures to save on all types of resources: electricity, fuel, gas, water [7].

The success is to optimally solve the individual components of this task and in the integrated management of automation systems of premises. Then the house can be proudly named SMART HOUSE.

Modern microprocessors have sufficient software resources to solve such a problem, but the number of communication lines between elements of the system may become excessive. It also complicates the struggle with the mutual obstacles between them. Therefore, the transmission of standard analog signals 0 – 10 V or 4 – 20 mA for large distances to each device becomes impossible. In industry, this task is solved by the use of reliable serial digital networks ProfiBus, CANOpen, and others. The standards of these protocols require adherence to specific strict rules regarding the physical and program organization of the network.

For systems of automation of residential constructions, networks with properties that are more suited to the living conditions and human psychology are developed. It is human interaction, automation systems and individual components that interact with the principles of IoT [3, 6, 9].

The features of household networks and protocols, above all, are that automatic devices in the house can appear gradually, without a detailed master plan. Therefore, expansion of the network should occur easily, without difficult reprogramming of all other elements and without excessively stringent requirements for cable laying [5, 12]. In the world, networks with protocols BaCNET, LON Works and others are distributed. One of the most popular standards in this area was the development of ABB i-bus®EIB – European Installation Bus. After the unification of many manufacturers, the network was named EIB / KNX [10, 16].

The network has four main means of communication – an independent low-voltage network, modulation of signals by power cables PowerBus, infrared and radiofrequency communications.

In a low-voltage network all devices marked in Fig. 37.1 can be connected by a pair of wires in any topology – tree-like (a), linear (b), mixed (c), and various connectors.

The main feature of the EIB network is the requirement only for the rules of data exchange, and how to ensure the implementation of these rules at the physical level – each manufacturer can find their own solutions. For example, Siemens has developed a KNX bus with two information wires: black (CE) and red (CE +). Belimo uses a three-wire MP-Bus network and a communicational module for connecting to the EIB / KNX (Fig. 37.2).

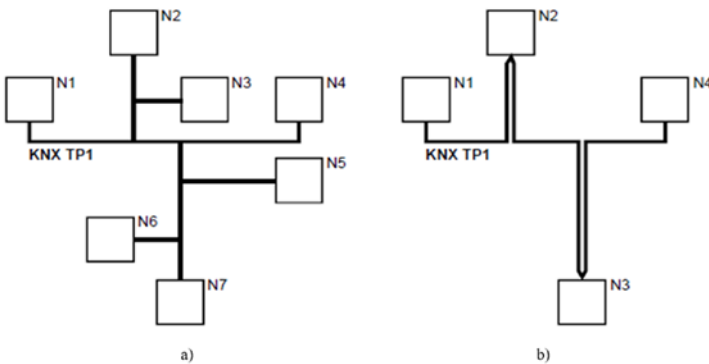


Fig. 37.1 – Topology of network: tree-like (a), linear (b)

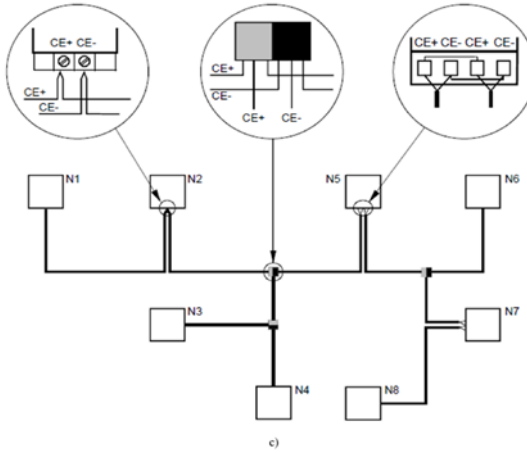


Figure 37.1 – Topology of network: mixed (c)

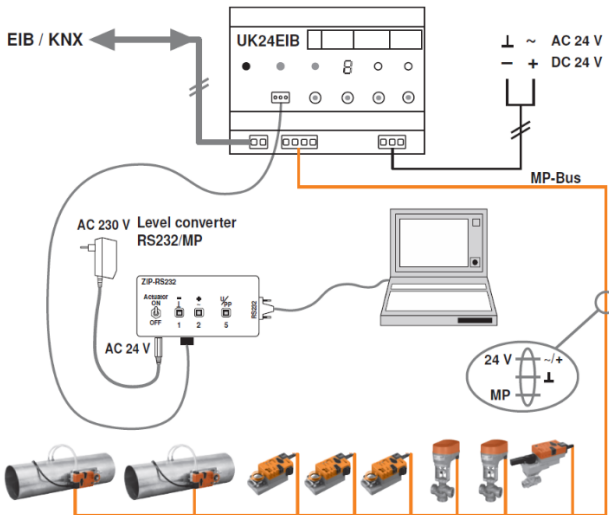


Fig. 37.2 – MP Bus of Belimo in HVAC systems

Several companies (Siemens, Moeller) manufacture 868MHz radio-frequency devices (RF-system), which meets the EIB's requirements. This version of the network allows you to completely

eliminate the control wires and significantly reduce the length of the power circuits.

Let's consider more in detail the EIB / KNX network in automation systems.

Such a network can have a hierarchical structure with three levels (Fig. 37.3). The lowest level (Line) is controlled by the linear connector Lc (Line control), which can combine up to 64 components. With linear amplifiers, the number of components in a line can be increased to 256, but at the design stage it is necessary to limit the number of components to 40-45.

The maximum length of the line should not exceed 1000 m, the distance between two components should not exceed 700 m, and the distance between the power supply and the component should be no longer than 350 m. If the power of the line is provided by two sources, then the distance between them should be longer than 200 m. In radio networks, the distance between elements should not exceed 50 m, and with routers – 150 m.

Up to 16 lines could be merged into a segment (Area). This is the second level of the hierarchy. Special segment connectors Ac (Area control) are used for this purpose.

The lines in the segment are connected by a zero or a main line (Area line 0). This is the third highest level of the hierarchy. The requirements for the length of the main line are the same as for normal lines. With the help of the main line up to 15 segments could be combined into a system that can eventually consist of tens of thousands components located throughout the residential quarter.

The addresses of each component of the EIB system are subdivided into physical and logical (group) addresses. The physical address determines the location of the component in the system and consists of a sequence of digits separated by a dot corresponding to their level. The first group of digits denotes a segment, the second is a line, and the third is the component number.

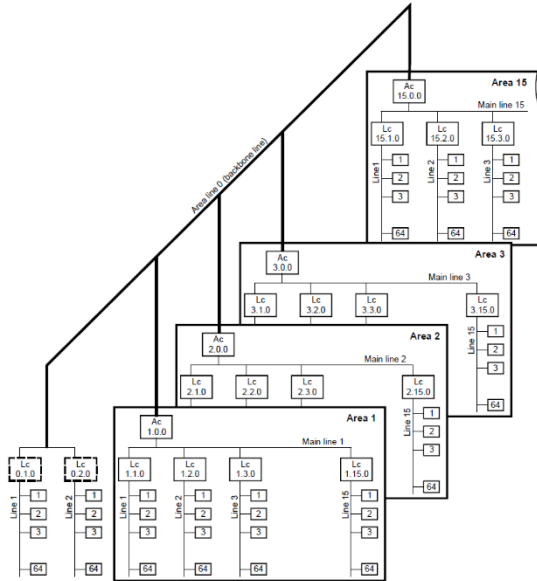


Fig. 37.3 – Hierarchical structure and addresses in EIB / KNX

For example, address 6.11.38 belongs to the thirty-eighth component of the eleventh line of the sixth segment. The physical address of the component is stored in the ROM component and may be modified if it is necessary. The logical address connects components of the system (for example, the sensor and the console). When designing, it is possible to select any logical address from 16 main groups, each of which contains 2048 subgroups. The main groups can be divided by function, ie control of lighting, heating, ventilation, etc. In this way, one component of the system can have not one, but several logical addresses.

The protocol for exchanging data in the EIB / KNX network between devices is based on the reception / transmission of short messages – telegrams. A telegram contains several information blocks – a priority field, an address field, a command field. The transfer rate is 9600 baud, that is to transfer one bit of information to 140 μ s. Each device permanently operates a data receiver connected to the line. If a telegram appears on the line, all receivers begin to receive it. Then the telegram analysis is performed. If the address matches the item in the

list stored in the memory of the individual device, then this device executes the command and sends a message about its execution.

To prevent collisions (conflicts with information damage) when exchanging messages, CSMA / CA (Carrier Sense Multiple Access / Collision Avoidance) access protocol is used. The principle of this protocol is as follows. If the line starts sending telegrams, the receivers block their own transmitters. But if at the same time two or more devices started transmitting, then each sent and received information is compared on each device. As long as the bits match, the device continues to transmit. But at some point when the bit in a telegram of one device is equal to 1 (recursive value) and the second is 0 (dominant value), the line will be set to 0. Then, in the device transmitting 1, the receiver blocks the transmitter and the device passed 0, can continue to work. Thus, the information will be transmitted to the line with the highest priority, that is, with a smaller value of the priority field and address (Fig. 37.4).

The EIB protocol accepted exceptionally detection of collisions to block communication. The device that noticed an error sends the Shut Up command (0x0000FFFF) which prevents other devices from transmitting information. Therefore, all participants in the data exchange "silence". In each of them, the generator generates a random pause from 1 to 3 seconds, after which the device again tries to restore the connection, if the network is free. Each device has three attempts.

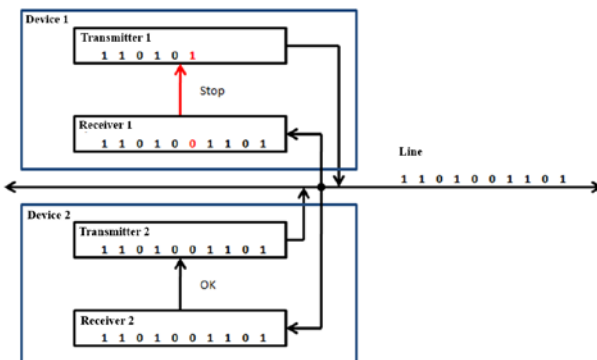


Fig. 37.4 – Collision Avoidance in serial bus

The EIB system has exceptional flexibility. One cable combines all electrical appliances at home. This simplifies switching systems (especially if some components are connected to the radio network), the cost of design and laying of cables is significantly reduced, reducing the risk of fire. System expansion and function change are achieved by simply rearranging, adding or reprogramming components of the system. Each component of the EIB system can interact with any other component (or simultaneously with a group of components) that are part of the system. The EIB system allows you to control electrical power systems at home both locally (in a specific room) and centralized (from the control panel or computer). Use of timers, light sensors, wind forces, temperatures, movements, etc. makes possible the fully automatic decentralized operation of all house systems depending on the season, day of week (working day / weekend), time of day and specific external conditions. This eliminates over-consumption of electricity and promotes the creation of extremely comfortable indoor conditions.

37.1.2 Classification of intellectual components, sensors, executive units of Building Management Systems

The EIB / KNX network combines three types of devices:

1. Sensors – analog and relay temperature sensors, motion sensors or presence, illumination, window integrity, pressure, humidity, speed and air quality, etc .;
2. Actuators – power executive devices (relays and TRIAC voltage regulators), modules for transmitting analogue 0 – 10 V or 4 – 20 mA and discrete signals, routers (devices for distributing the network coverage area);
3. Managing devices – buttons, remote controls, personal computers with communication modules, climate control modules, room control modules or buildings with the ability to communicate with external networks GSM, Ethernet, Internet, dispatching consoles.

Table 37.1 shows some components of the Eaton / Moeller xComfort system with the EIB RF-System [14].

Table 37.1. Components of Eaton / Moeller xComfort

Type	Technical data
Actuators	
CSAU-01/01	Switching actuator, 8 A, 230 VAC
CSAU-01/02	Switching actuator Voltage-Free, 8 A, 230 VAC
CSAU-01/03	Switching actuator All-Poles, 6 A, 230 VAC
CJAU-01/02	Shutter actuator, 6 A, 230 VAC
CDAU-01/02	Dimming actuator, 250 VA, 230 VAC
CDAU-01/04	Universal dimming actuator for R, L, C, LED
CAAE-01/01	Analogue actuator, 8 A, 230 VAC, 20 mA, 0-10 VDC
Sensors	
CSEZ-01/01	Temperature Sensor PT1000, -50 to +200°C
CSEZ-01/16	VOC Air Quality Sensor, 0-10VDC linear to air quality
CBEU-02/02	Door / window binary input unit with battery
CBEU-02/03	Binary input unit, 2 inputs (A, B), 4 modes
CEMU-01/02	Energy meter sensor, 8A, 230 VAC
CSEZ-01/18	Water leakage sensor
CSEZ-01/19	Smoke Detector
CSEZ-02/08	Wind / Rain Sensor
CSEZ-01/12	PIR Motion sensor, Area covered: 200 °, 16 m at h 2 m
CSEZ-01/14	Brightness sensor, 3–300 lux... 600–60k lux
CSEZ-01/17	Humidity sensor with Temperature PT1000,
CTEU-02/01	Temperature Input Unit
Control and communication unit	
CTAA-01/04	Push-button, Power supply 3V via CR2450N battery
CTAA-02/04	Number of rockers depending on type
CTAA-04/04	
CRMA-00/01	Room Manager
CHMU-00/02	Home Manager
CKOZ-00/02	GSM-Modem
CROU-01/01	RF Router
CHSZ-12/03	12-Channel Remote Control
CKOZ-00/03	Communication Interface USB/RS232

37.1.3 Subsystems of Smart House: microclimate control, lighting, security in residential and industrial premises

In recent decades, the most common device for providing comfortable temperature in the room became the air conditioner, especially with the double action of "winter-summer". But modern technology interferes not only into technical devices, but also into construction methods. All new and refurbished rooms provide modern hermetic windows and doors. Just then the one but significant lack of air conditioners is noticeable – they do not provide an upgrade of air indoors. Therefore, the level of CO_2 , water vapor, other harmful impurities gradually increases, the feeling of comfort disappears, and eventually the mold and fungal stains appear in the room. Therefore, in rooms with limited natural ventilation it is expedient to restore air due to forced inflow and exhaust ventilation.

Local forced-flow ventilation systems (for part of the structure) could be channel or non-channel, single-or multi-zone. Local systems include inflow and exhaust fans with speed control, air damper and filters, electric heaters with power control. In large buildings, it is economically feasible to install a centralized cooling and heating system – a chiller, from which the coolant (purified water, possibly with antifreeze) is fed into heat exchangers (fan coils) of local systems of inflow ventilation. Private houses also install gas boilers, which provide two independent heating circuits and hot water supply. Hot water in the heating circuit is supplied to the radiators in separate rooms. Electric and water heaters provide a comfortable temperature, and fans – exchange of air. Since energy consumption for heating-air cooling of the air flow is proportional to its speed, it is advisable to have co-regulation of these devices to save energy [1, 4].

The basic functional diagram of the system of inflow and exhaust ventilation is shown in Fig. 37.5, where M1, M3 – fan motors, M2 – water valve actuator, T1, T2 – temperature sensors of the inflow air after the heat exchanger and indoors, dP – differential pressure sensor, which controls the condition of the filter and the fan.

In addition to the depicted elements of the system, there are air quality sensors in the room for controlling the speed of fans, humidity sensors, if humidifier-dehumidifier is installed, passive or active

recuperators, which perform heat exchange between the inflow and internal air in order to save energy.

Elements of climate control systems. Air damper drive

Air flaps are installed on external vents for protection against dust and insects when fans do not work, and on the inner vents of the ventilation duct for possible adjusting of the proportion of air flow. Therefore, the air damper actuators (Fig. 37.6) perform two types: two-position (closed-open) and three-position (closed-intermediate state-open). The electromechanical damper actuator consists of an electric reducer motor of direct current, a reverse spring mechanism, a feedback rheostat on the position and control system.

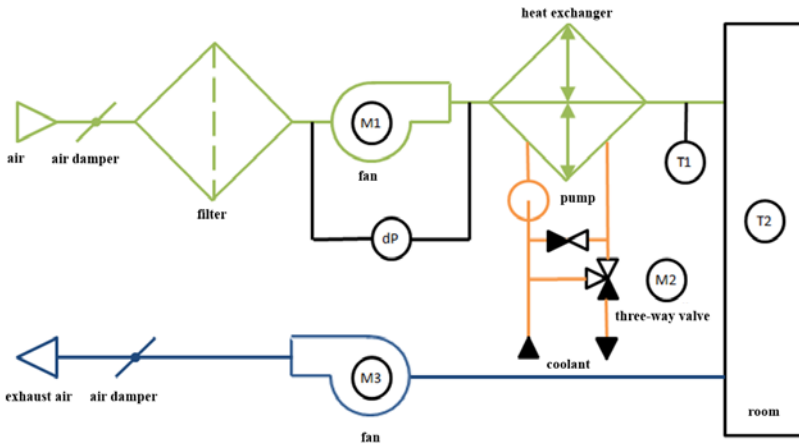


Fig. 37.5 – Functional diagram of the climate system

The drive is powered by $\sim 220\text{ V}$ or $\sim / = 24\text{ V}$ through the built-in rectifier. For two-position drives, the power supply is an open command. The three-position drives are additionally provided with an analogue control signal to the position $0 - 10\text{ V}$ or $4 - 20\text{ mA}$. On the other hand, the analogue feedback signal can be removed from the same level by the position of the damper. The control system is a position regulator with a zone of insensitivity for small oscillations of the task signal (for protection against network interference) and a relay output that supplies the voltage to the motor. When the damper is open

and does not move, the engine current decreases approximately three times. This is enough to counteract the spring and the moment of resistance and keep the engine stationary, but the engine heats up. When the power supply is removed (including due to the accident of the power supply network), the spring mechanism turns the actuator into a "closed" position. On the internal holes, the drives of the damper are installed without a spring mechanism.



Fig. 37.6 – Air damper with actuators

Water valve actuator

When the house is equipped with a chiller, the control of the air temperature in the fan coils is provided by water valves, which regulate the flow of coolant. Use two- or three-way valves. The two-way valve changes the amount of coolant that is supplied to the heat exchanger. The disadvantages of such a tool are essentially nonlinear dependence of heat transfer on the position of the valve stem, as well as the risk of icing at a negative temperature of the outside air and the low speed of the coolant. The three-way valve with circulation pump (as shown in Fig. 37.5) provides control of the temperature of the coolant in proportion to the position of the rod and the continuous circulation of the coolant with constant velocity in the heat exchanger, regardless of the position of the stem. This protects the heat exchanger from freezing.

The same temperature is regulated in radiators of separate rooms with a centralized heating system.

The actuator of the water valve (fig. 37.7) moves the stem, which changes the intersection of the pipeline. Stroke is only 10 – 30 mm. The power of the electric drive system comes from the networks ~ 220 V or

$\sim / = 24 \text{ V}$ through the built-in rectifier, and the analogue position control signal has standard levels 0–10 B or 4–20 mA.

But the control system is significantly different from the control system of the three-position actuator of the air damper. With the first switch on, the modern microprocessor control system moves the stem from one extreme position S_{\max} (valve closed) to the second S_{\min} (the valve is open) and memorizes the corresponding voltage levels of the feedback potentiometer. In the future, these provisions will meet the minimum and maximum levels of the control signal. In this way, the actuator of the water valve becomes invariant to the mechanical actuator (the stroke).



Fig. 37.7 – Drives of water valves

With control signals $<10\%$ and $>90\%$, the drive completely closes or completely opens the coolant flow due to the fact that for temperature control processes the difference between these valve states is insignificant and the drive is switched off. In addition, in order to protect the mechanical part from excessive wear, the control system performs the analysis of the level and the derivative of the control signal. Quick changes and short-term small changes in control signal are ignored. The resulting delay is not essential for significantly slower thermal processes. The microprocessor system calculates the stock speed chart in the form of trapezoidal or triangular to move it to a given position S_{set} . This prevents continuous operation of the mechanism, reduces energy consumption, increases service life.

Sensors in climate control systems

To ensure the comfort of the room, it is necessary to measure and adjust three basic parameters: temperature, air quality (chemical composition) and humidity. For these parameters, appropriate analog sensors are used.

The most common temperature sensors are platinum types PT100, PT500, PT1000. The numbers in the sensor type determine its nominal impedance at $0\text{ }^{\circ}\text{C}$. And the most important characteristic of such sensors is the same temperature coefficient, regardless of type and manufacturer. In the range of domestic temperatures this coefficient is equal $0.003851\text{ }^{\circ}\text{C}^{-1}$. So,

$$R_T = R_0(1 + 0.003851T),$$

where R_T – electrical resistance at temperature $T\text{ }^{\circ}\text{C}$, R_0 – electrical resistance at temperature $0\text{ }^{\circ}\text{C}$.

To process signals of temperature sensors, special modules are used, which include the current source $1 - 10\text{ mA}$ and analog-to-digital converter. Depending on the distance between the sensor and the control system, different connection schemes are used: 2-, 3- or 4-wire. The last two ones allow to exclude the influence of the active resistance of the wire on the measurement results.

In the *air quality sensors*, complex catalytic reactions are used, which changes the resistance of the measuring plate, depending on the chemical composition of the air. There are sensors that measure the relative amount of CO_2 , CO , CH_4 , NH_3 , CH_3OH and other components separately or in a mixture. These reactions last for a while, so the characteristic feature of air quality sensors is their inertia with a constant time of several minutes. In addition, the resistance of the measuring plate significantly depends on atmospheric pressure and operating time. Therefore, manufacturers of sensors deliver them in the form of electronic modules, microprocessors which perform correction of the results. Thanks to the microprocessors, the output signal of the sensors for use in the control systems lies in the standard ranges $0 - 10\text{ V}$ or $4 - 20\text{ mA}$.

Air humidity sensors also use the dependence of resistor resistance or condenser capacitance from organic or organometallic materials from the partial pressure of water vapor. It should be noted that the resistance of the sensor also depends on the voltage and the

temperature of the air. To get the correct results, the typical connection diagram of the sensor includes a negative temperature coefficient (NTC) resistor and a bipolar input voltage of 1 kHz, 5 V. Condenser sensors are thermostable, but the input voltage has a frequency of 4 – 100 kHz.

On the basis of temperature sensors, modules for installation in climate control systems are manufactured (Fig. 37.8), the output signal of which meets the standard requirements 0 – 10 V or 4 – 20 mA.

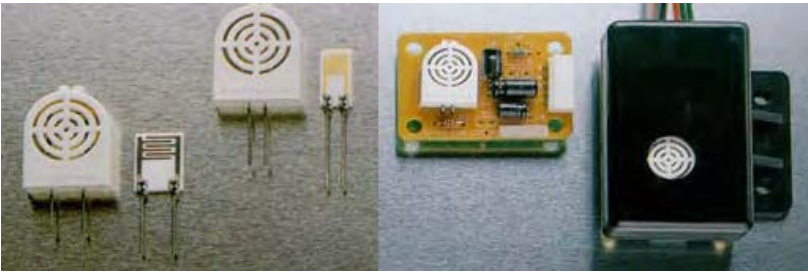


Fig. 37.8 – Humidity sensors and modules based on them

Methods of speed control of fans

In ventilation systems, axial fans with single-phase asynchronous motors with power up to 350 W and radial fans with three-phase asynchronous motors are used.

TRIAC voltage regulators are used to control the speed of single-phase motors. To ensure satisfactory control accuracy without speed feedback for a standard fan load, calculate the dependence of the angle of phase control on the required speed and load it into the memory of the microprocessor. Depending on the task of speed from the corresponding table find the necessary value of the angle. The error resulting from power voltage and load fluctuations is not essential for many ventilation systems. But at low fan speeds, the fan motor may overheat.

To improve accuracy and reduce overheating, single phase motors can be connected to frequency converters (FC) with scalar or vector control according to the scheme shown in Fig. 37.9, a. Phase-holding capacitor C1 may not be used, but it is often installed in the asynchronous motor and therefore can not be turned off. Three-phase

motors are used in conjunction with standard frequency converters (Fig. 37.9, b).

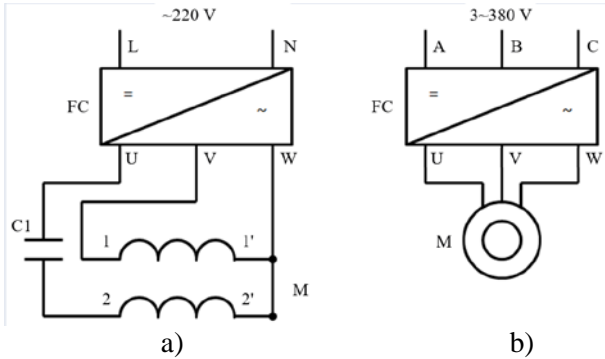


Fig. 37.9 – Diagrams for connecting fan motors

37.2 Organization of the interaction of subsystems and elements of Smart House and IoT

37.2.1 Microclimate control – functions, executive and sensor units

To organize the interaction between the components of the automation systems in the premises it is not enough to construct only logical algorithms. The main feature of climate control systems is the inertia of both changes in the temperature in the premises and heat carriers. Therefore, to build systems, you need to have some basic knowledge of the principles of automatic control.

Mathematical models of elements of climate control systems

1. The equation of heating the air in the heat exchanger or heater in the ventilation duct is as follows:

$$T_H \frac{dT_C}{dt} + T_C = \frac{H^*}{\omega^*} \Delta T_C + T_O \quad (1)$$

where T_O, T_C – the temperature of the external environment and air at the end of the channel; T_H – time constant of the heater, which depends on the heat capacity, mass, coefficient of heat transfer of the heater; ΔT_K – nominal overheating of the air in the "fan-heater" system,

which selects these elements in a certain climatic region and which depends on the nominal power of the heater P_H and the nominal speed of the fan ω_v ; H^* – relative power of the heater; ω^* – relative fan speed.

The regulation of the temperature of the air in the channel becomes possible by two means: to reduce the temperature it is necessary to reduce H^* , and raise the temperature, if $H^* = 1$ is possible by reducing ω^* .

2. The equation of overheating of air in the room due to the heater in the inflow ventilation channel, without taking into account convection and air diffusion, can be written as follows:

$$T_R \frac{d\Delta T_R}{dt} + \Delta T_R = k_R T_C, \quad (2)$$

where T_R – time constant of the room; k_{II} – conditional gain factor of the room relative to the air temperature in the inflow ventilation channel; ΔT_R – overheating in room.

But it should be noted that the actual temperature in the room depends, in addition to the heater, on the external temperature, on the heat transfer of the room through the walls, windows, floor, roof to the external environment, the capacity of the additional heaters in the room (including people, equipment, computers).

In addition, the time and gain have become dependent on speed, atmospheric pressure and relative humidity. But the air speed in the room is much less than the air velocity in the ventilation duct and is one-tens of millimeters per second. Such a flow of air is already influenced by the phenomena of convection, diffusion. Convection leads to the temperature distribution in the vertical direction. In this regard, it is recommended to set temperature sensors at the level where most of the time are the chest and the head of the person. The process of diffusion leads to the transfer of air mass in directions that do not coincide with the flow of ventilation. There is also a delay, which is associated with a certain distance between the position of the sensor and the opening of the supply ventilation channel. Due to these factors, it is almost impossible to determine the exact parameters of the room, so the actual process of changing the temperature in the room may differ from that given by the solution of equation (2).

In these conditions, to improve the dynamic and static characteristics of climate control systems and to reduce their dependence on assumptions when calculating parameters, it is expedient to use multi-circuit systems of subordinate regulation and the system of automatic identification of parameters of control objects [11].

The inner subordinate close-loop regulates the air temperature in the inflow ventilation channel. To receive a feedback signal, install a sensor of the temperature of the inflow air (T1 in Fig. 37.10). When using a water heater with a proportional-integral (PI) regulator this circuit is tuned to the technical optimum. The close-loop may also be configured when using an electric heater. But in slip mode, which provides a relay controller with a hysteresis loop, the dynamic parameters are the best and least dependent on the nonlinear properties of the heater. The width of the hysteresis loop ΔT_p ($^{\circ}C$) can be calculated by the method of harmonic linearization. Approximately for providing a given period of fluctuations T_{PWM} its value is

$$\Delta T_p \approx \frac{T_{PWM}}{4T_H} \Delta T_C. \quad (3)$$

The external close-loop of room temperature with feedback from the temperature sensor (T2 on Fig. 37.11) is set with the PI- or PID-controller to the technical optimum. It takes into account the parameters of the internal close-loop and the worst conditions of the stability of the room settings.

If the air quality sensor is installed to increase the efficiency of the system, then create a closed loop for this parameter. Since the mathematical description of the heat processes in the air of the premises and the processes of air mass transfer are identical, the air quality control loop is tuned in the same way as the external circuit of the temperature controller. The output of this regulator is the task of the speed of the fuel fan. If at such speed the temperature of the inflow air becomes unsatisfactory (lower than the set room temperature in winter or higher – in summer), then the signal is reduced depending on the signal of the temperature T_C regulator.

It should also be noted that increasing the value of the sensor signal usually corresponds to the deterioration of air quality, and speed increase improves this indicator. Therefore, the task of the acceptable level of quality is negative, and the feedback signal is positive.

If the performance of the tidal and exhaust ducts is balanced, the speed of the exhaust fan ω_{EF} is changed depending on the speed of the inflow fan ω_{IF} :

$$\omega_{EF} = \omega_{IF} \pm \Delta\omega, \quad (4)$$

where negative value $-\Delta\omega$ is used for living quarters, $+\Delta\omega$ – for kitchens and office premises where sources of dust or unpleasant smells are possible. Values $\Delta\omega$ are set to provide some pressure drop. Usually $\Delta\omega$ is a few percent of the rated fan speed.

Thus, a structural scheme of the climate control system presented on fig. 37.10.

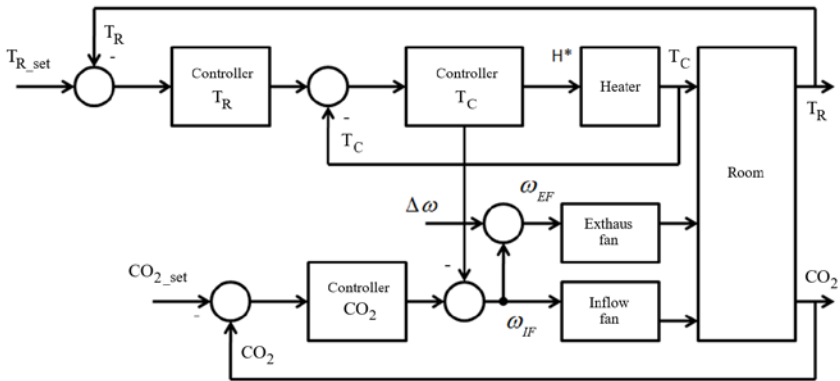


Fig. 37.10 – Structural scheme of the climate control system

The software of system must solve the following tasks:

1. Support for the temperature of the inflow air and / or the temperature in the room with the processing of signals of temperature sensors in subprograms of PI regulators or relay regulators with a hysteresis loop;
2. Electric heater control with the help of the simistronic electronic relay by the method of pulse-width modulation with a period of 1 minute;
3. Control of water heat exchanger with three-position valve with electric drive;
4. Control of two- or three-position flaps in air channels;
5. Speed control of fans, including smooth overclocking when switching on and a smooth stop when switching off the system;

6. Protection of the electric heater from overheating and water from icing, control of air filters, shutdown of the system when triggered by a fire alarm.

37.2.2 Lighting – lux meters, astronomical timers, security components as sensor and control units in lighting subsystem

The functions of the lighting control system will be listed as a list of tasks, scenarios and tools for their implementation.

1. Passage corridors and rooms with multiple entrances

1.1. The problem is that every person who enters and goes out of the room changes the position of the switch at the entrance. Lighting, respectively, must be switched on or off.

1.2. In order to implement the scenario, you must have either pass-through switches (for corridors) or conventional two-way switches and a program in a controller that will implement the Exclusive OR function for many logic signals.

2. Maintaining lighting at the required level.

2.1. This scenario can be used in rooms where it is necessary to maintain a constant level of illumination regardless of the time of day when the level of natural light changes, for example, in the office.

2.2. Elements used to implement the scenario: a light sensor with an appropriate actuator: a symmetric voltage regulator and a halogen lamp or 12, 24 V power supply and a PWM for an LED lamp.

3. Maintaining natural lighting at the required level.

3.1. This scenario can be used in rooms where a constant level of natural light is required irrespective of the time of daylight.

3.2. Elements used to implement the scenario: a light sensor with an appropriate actuator: actuator blind, drive motor.

4. Turning the light on when moving in the room.

4.1. This scenario can be used either as a security alarm, or in long corridors, where the movement is periodic.

4.2. Elements used to implement the script: motion sensor with corresponding executive lighting device.

5. In long corridors, when triggering the motion sensor, several light bulbs must be fired successively in intervals of 3-10 seconds. If after the triggering movement is absent, the lamps should go out in reverse order with the same interval.

5.1. Elements used to implement the scenario: motion sensor with corresponding actuators: relay actuators (for example, CSAU-01/01) and lamps.

6. Advanced light level adjustment scenario due to natural and artificial lighting. Two factors must be taken into account: the actual light level and time of day. Thus, in the light of day, the daylight is controlled by the shutter, in the dark by adjusting the voltage on the incandescent lamps. This scenario will save you a lot of energy.

6.1. Elements used to implement the scenario: light sensor, simulator voltage regulator, halogen lamp, actuator blind, drive motor.

7. Switch on the devices and lighting according to the schedule of work in the room (for example, in the halls of the shopping centers).

7.1. To implement the scenario, an astronomical timer with scheduled work schedules on weekdays and weekends is required, hall layout on the zones, actuators for individual lighting zones.

8. Scenarios for controlling climatic installations and the ventilation system. To implement them, humidity sensors, temperature, air quality and analogue actuators that output the task signal to the corresponding devices, astronomical timers are used to schedule the desired temperature at the time of day or season.

8.1. Support for the required indoor temperature by adjusting the heating performance. This scenario can be used to maintain a comfortable temperature under the influence of various factors: the periodic opening of doors and windows, the heating of the room as a result of the work of the plate or electrical appliances.

9. Support for the required indoor air quality by adjusting the ventilation efficiency. This scenario can be used to maintain air purity with a variety of factors: cooking, increasing the number of people in the room, air pollution by other outsider, the efficiency of the ventilation system may decrease, depending on the presence of people, time of day.

9.1. Elements used to implement the scenario: an air quality sensor with an appropriate actuator: an analog actuator, a ventilation control system, a presence sensor, and an astronomical timer can be added.

37.2.3 Security subsystem – interaction with lighting, access control and protection subsystems

Security systems are usually separate systems, equipped with specialized controllers and sensors with a separate network of communications with a security company.

But within the frame of Smart House functions several scenarios can be implemented, which work as a supplement to the main security system.

1. Switching on the lighting in the room and near the private house, shutting down the roller if the security system is on, but the motion sensor or window sensor has been triggered or the ALARM button is pressed. This feature allows you to frighten an alleged offender.

2. Send a message to the owner of the room when triggering movement sensors or window sensors in the mode when the security system or the "No one is" mode is activated. To implement this scenario, you need to configure the connection channel of the controller with the Internet or with the mobile operator.

3. The mode of presence simulation is implemented to prevent criminal intent in the absence of tenants in the house. A system that remembers the sequence of switching on / off the lighting devices by tenants for a long time (week, month) is considered an effective one. When you click on the "Simulate Presence" button, this sequence is repeated according to the astronomical time and day of the week.

37.3. Construction of Smart House and IoT subsystems based on Moeller / Eaton xComfort

To build a system of intelligent control of a building, it is necessary to pick up sensors, executive and control elements of the system and to perform their connection, as an example, built on the basis of Eaton / Moeller xComfort.

Between the elements, in addition to the wired power connections, there is also radio communication and bilateral exchange of information according to the EIB protocol.

Visualization and configuration of the wireless connection are performed using the Moeller RF-System software environment.

The typical system includes the following radio elements: Remote control; Room-Manager; Motion Detector; Window sensors; Switching actuators; Push-buttons; Communication devices, USB interface; analog control actuators for the HVAC; Light, Air quality, Humidity, Temperature sensors.

Homeputer system is used to visualize control over lighting devices and to centralize management. The system is implemented using a personal computer equipped with the USB / RS232 communication interface and Homeputer Studio software.

System setup works in several stages, examples for which are listed below.

1. Establishing communication between individual elements
2. Installing wireless communication between the elements via the USB / RS232 interface and the Moeller RF-System software by creating Datapoint-file according configuration (fig. 37.13).
3. Using the prepared Datapoint-file, import the configuration of the elements into Homeputer Studio 2.30.
4. Development of the Macro program management system in Homeputer Studio to create a scenario for your syste. The macro is written in a language like a BASIC, an example of text is given below.

<i>if Bin_Batt_1A switchedon then Lamp3 switchon end-of-if-block</i>	If the door is open, the actuator is switched on
<i>if Bin_Batt_1A switchedoff then Lamp3 switchoff for 30 seconds end-of-if-block</i>	If the door is closed, then the actuator is switched off for 30 seconds

When the program is ready, you need to save the changes and execute the Run command.

37.4 Work related analysis

Smart house and its components are an object of research in lot of works. E. Ferro P. Barsocchi, F. Palumdo, F. Potorti, R. Bolla, O. Parodi, M. Girolami and S. Chessa provide solutions for area of the Italian National Research Council (CNR) in Pisa with 130 000 m² village where 3000 people live and move daily. They use heterogeneous networking in the home environment. It can thus be considered as a laboratory where smart solutions to problems that can be encountered in any town or city can be tested. The UCD Institute of Food and Health tells us that cognitive decline, malnutrition and sedentariness are the main causes of morbidity and premature mortality in older people. Lot of research are directed to application of smart devices for healthy ageing. Cognitive games, sensor networks, location systems and other smart devices developed under the DOREMI project could help counter these evils. [1-6].

M. Horynski, J. Lavaei, S. Low, R. Baldick, B. Zhang, D. Molzahn, F. Dorfler, H. Sandberg explore energy management in households as part of the sustainable development of the energy economy and guest editorial distributed control and efficient optimization methods for Smart Grid [7, 8].

Many projects use wireless protocols such as Bluetooth and Wi-Fi [5, 9, 12]. However, large projects, especially intelligent home and secure control systems, large scale networks base on the KNX / EIB bus protocol with radio frequency communication. D. Pang, S. Lu, Q. Zhu, K. Paridari, A. Parisio, H. Sandberg, K. Johansson, P. Park, S. Ergen, C. Fischione, C. Lu, E. Tegling, S. Henrik explore wireless network for control systems, in particular with PI and PD control [10, 11, 13, 15, 16].

Conclusions and questions

The lecture material provided the basis for building Smart House with principles of Internet of Things:

- Classification of the Building Management System, the purpose and basic properties of control, executive and sensor elements, introduction in Smart House and IoT systems;

- Classification of intellectual components, sensors, executive units of Building Management Systems;
- Principles, scenarios and executive elements for subsystems of Smart House: microclimate control, lighting, security, access control and protection subsystems in residential and industrial premises;
- Organization of the interaction of subsystems and elements of Smart House & IoT. As an example, were shown Construction of Smart House & IoT subsystems based on Moeller / Eaton xComfort.

In order to better understand and assimilate the educational material that is presented in this section, we propose you to answer the following questions.

1. What are the most important factors affecting a person can be controlled by automation systems and IoT?
2. Why is the use of digital networks in the automation systems of premises extending?
3. What are the features of digital networks for home systems?
4. What are the main methods of communication using EIB / KNX on the physical level?
5. What kinds of topologies can we use in EIB / KNX networks?
6. How does the Moeller RF-System (EIB) radio network work?
7. How is the problem of collisions in the serial EIB / KNX tires resolved?
8. What are the main features of the Carrier Sense Multiple Access / Collision Avoidance protocol?
9. How is the EIB / KNX hierarchical model implemented?
10. What are the main types of devices (which element base) which are used in SMART HOUSE with IoT?
11. What is the system addressing devices in the EIB network?
12. How does the connection and breakdown of communication with the actuator or sensor on the EIB radio network?
13. Which basic parameters of air provide comfortable conditions?
14. What is the principle of operation of the air damper drive?
15. What is the principle of operating a water valve drive?
16. Which sensors are used in climatic systems?
17. How can the fan speed in climatic systems be controlled?
18. How to regulate the power of a water heat exchanger?

19. How can the power of an electric heater be controlled?
20. What is the complexity of obtaining a reliable mathematical description of the thermal processes in the room?
21. Which regulators are used in climate control systems?
22. How is energy saving provided during the construction of SMART HOUSE?
23. What is a "macro" and how does macros perform?
24. Why do you think Moeller uses the simplest programming language to prepare macros like BASIC?
25. Which steps are needed to set up the Moeller / Eaton xComfort system?

References

1. Barsocchi, P., Ferro, E., Palumbo, F. and Potortì, F. (2018). Smart meter led probe for real-time appliance load monitoring. [online] Openportal.isti.cnr.it. IEEE SENSORS 2014, Valencia, Spain, 3-5 November 2014. Available at: https://openportal.isti.cnr.it/results?option=com_dnetindexclient&view=doc&id=people_____:37353ae80a8d45719033641a5f42b4e5
2. Bolla, R. and al. (2006). Heterogeneous networking in the home environment. [online] Openportal.isti.cnr.it. Available at: https://openportal.isti.cnr.it/results?option=com_dnetindexclient&view=doc&id=people_____:ed37a0e8fdf1d6186bd37a2ae1eda83b
3. Ferro, E. (2018). Smart Solutions for the CNR campus in Pisa. Openportal.isti.cnr.it. Available at: https://openportal.isti.cnr.it/results?option=com_dnetindexclient&view=doc&id=people_____:680a59763c98f06ffc49f48f8abfcc22
4. Ferro, E. and Parodi, O. (2018). Smart devices and applications for healthy ageing. [online] Openportal.isti.cnr.it. Available at: https://openportal.isti.cnr.it/results?option=com_dnetindexclient&view=doc&id=people_____:cc895aea31a19a92c32bfca2bd7c9746
5. Ferro, E. and Potortì, F. (2018). Bluetooth and Wi-Fi wireless protocols: a survey and a comparison. [online] Openportal.isti.cnr.it. Available at: https://openportal.isti.cnr.it/results?option=com_dnetindexclient&view=doc&id=people_____:dfca78582b0ad050e9c73c55e7cfbf5a
6. Girolami, M., Chessa, S. and Ferro, E. (2015). Discovery of Services in Smart Cities of Mobile Social Users. Openportal.isti.cnr.it. Available at: https://openportal.isti.cnr.it/results?option=com_dnetindexclient&view=doc&id=people_____:5faa8a06fc35e0dd189b65e86873fb21https://openportal.isti.cnr.it/results?option=com_dnetindexclient&view=doc&id=people_____:b25f392df022ed7db659996da585a64a

7. Horyński, M. (2017). Energy management in households as part of the sustainable development of the energy economy. 2017 International Conference on Electromagnetic Devices and Processes in Environment Protection with Seminar Applications of Superconductors (ELMECO & AoS). Available at: <https://doi.org/10.1109/ELMECO.2017.8267721>

8. Lavaei, J., Low, S., Baldick, R., Zhang, B., Molzahn, D., Dorfler, F. and Sandberg, H. (2018). Guest Editorial Distributed Control and Efficient Optimization Methods for Smart Grid. [online] DIVA. Available at: <http://kth.diva-portal.org/smash/record.jsf?dswid=3396&pid=diva2:1206634>

9. Marksteiner, S., Jimenez, V., Valiant, H., Zeiner, H. (2017). An overview of wireless IoT protocol security in the smart home domain - IEEE Conference Publication. [online] Doi.org. Available at: <https://doi.org/10.1109/CTTE.2017.8260940>

10. Pang, D., Lu, S. and Zhu, Q. (2018). Design of Intelligent Home Control System Based on KNX/EIB Bus Network. Available at: <https://doi.org/10.1109/WCSN.2014.74>

11. Paridari, K., Parisio, A., Sandberg, H. and Johansson, K. (2015). Robust Scheduling of Smart Appliances in Active Apartments With User Behavior Uncertainty. [online] DIVA. Available at: <http://kth.diva-portal.org/smash/record.jsf?dswid=3396&pid=diva2:904282>

12. Park, P., Ergen, S., Fischione, C., Lu, C. and Johansson, K. (2018). Wireless Network Design for Control Systems : A Survey. DIVA. Available at: <http://kth.diva-portal.org/smash/record.jsf?dswid=3396&pid=diva2:1220077>

13. Sandberg, H. and Johansson, K. (2018). Secure Control Systems | KTH. Kth.se. Available at: <https://www.kth.se/ac/research/secure-control-systems>

14. Technical specification EATON RF System. Eaton.eu. (2018). [online] Available at: http://www.eaton.eu/ecm/idcplg?IdcService=GET_FILE&allowInterrupt=1&RevisionSelectionMethod=LatestReleased&noSaveAs=0&Rendition=Primary&dDocName=PCT_1572103

15. Tegling, E. and Henrik, S. (2018). On the Coherence of Large-Scale Networks With Distributed PI and PD Control. [online] DIVA. Available at: <http://kth.diva-portal.org/smash/record.jsf?dswid=3396&pid=diva2:1111853>

16. Vanus, J., Cerny, M. and Koziorek, J. (2015). The proposal of the smart home care solution with KNX components. [online] Available at: <https://doi.org/10.1109/TSP.2015.7296410>

38. ENGINEERING OF SOFTWARE/HARDWARE PLATFORM FOR SMART BUILDING SYSTEM

Assoc. Prof., Dr. A. V. Parkhomenko (ZNTU)

Contents

Abbreviations	250
38.1 Embedded systems as the basis of the IoT infrastructure.....	251
38.1.1 Embedded systems design techniques	253
38.1.2 Hardware/software platforms for embedded systems realization	254
38.1.3 Protocols and technologies for embedded systems interaction with other devices and Internet.....	257
38.2 Implementation of the software/hardware platform for Smart Building System	263
38.2.1 The development of Smart Building System architecture	264
38.2.2 The usage of Raspberry Pi and OpenHAB platforms for Smart Building System control	265
38.3 The application of the remote laboratory Smart House&IoT for Smart Building System prototyping	268
38.4 Work related analysis	276
Conclusions and questions.....	278
References	280

Abbreviations

API – Application Programming Interface

AP – Access Point

CDMA – Code Division Multiple Access

ES – Embedded System

IoT - Internet of Things

OS – Operating System

PWM – Pulse Wide Modulation

RFID – Radio Frequency IDentification

RL – Remote Laboratory

SBS – Smart Building System

38.1 Embedded systems as the basis of the IoT infrastructure

As known, Internet today is not only environment of communication and information exchange between people, but it is a tool and technology of interaction between customers, "things" and devices. Therefore, industry wants effectively design, create and deploy modern smart connected products based on the Internet of Things technologies (IoT).

Today the IoT technologies greatly extend the possibilities of collecting, analysis and distribution of data, which humanity can transform into information and knowledge. The IoT opens new perspectives and gives more opportunities to increase economic efficiency by automating processes in various fields of activity [1]. At the beginning of 2016 the main segments for IoT applying were Manufacturing, Energy and Transportation [2]. The impact of the IoT on companies' activities is increasing. Smart, connected products and the data they generate are transforming traditional business functions, sometimes significantly [3].

Of course, there are still many issues that must be solved: more and more new unique IP-addresses, sensors' autonomous power supply, IoT devices certification, security, protection of personal information, etc. [1]. But even today, thanks to IoT technologies, the world begins to interact with physical and virtual "things" and devices in other way.

More often, the concept of IoT is inseparably connected with something smart: Smart House, Smart Transport, Smart City, Smart Businesses and so on [4]. The concept of such systems as Smart City, Smart Building and Smart House creating is popular all over the world. The main regions that are actively implementing Smart House technologies are Northern America, the Asia-Pacific region and Western Europe [5-6].

Nevertheless, according to the Gartner company's investigations, making decisions about Smart House system usage is still at the early stage and users do not fully understand the prospects and usefulness of such smart technologies. An online survey of nearly 10,000 respondents from the United States, the United Kingdom and Australia has shown that only about 10% of families currently use connected Smart House solutions. Three-quarters of respondents indicated they were happy to set temperature and lighting controls manually versus only one-quarter

expressed an interest in having devices that anticipate needs in the home. Furthermore, 58 percent of respondents showed a preference for using stand-alone devices. However, respondents are starting to see the value of one application for integrating their connected home devices, appliances and services as well as the importance of brand certification for their connected home devices and services [7].

The market of intelligent home automation in Ukraine is developing not for a long period of time. However, in the last few years many people have already begun to build smart houses from scratch or equip existing houses and apartments with home automation systems. The most popular are the solutions for "smart" resources usage (electricity, water, various types of fuel) and home security. The issues of safety and security providing are very important and widely discussed [8-9]. The concept of security concerns not only the penetration of strangers into the house, but also the occurrence of fires, water leaks, short circuits, carbon monoxide, smoke or fire. Another important component of security is the cybersecurity and smart house's information security. And if the issues of energy efficiency and safety of such systems are paid great attention, the cybersecurity issues remain in the shadow, although cyberattacks of recent years have shown the danger of such an attitude.

At present, a lot of Ukrainian companies (Smart Home Company, SmartON, IntelSity, MiMi Smart, IQDim, 1m-Smart home, Gira, etc.) offer a comprehensive Smart Building System (SBS) based on the individual wishes of the end user.

Technologies of Smart House creating are interesting and useful for people, as they allow to make our life more comfortable, safe and to provide resource saving. Some users want to create their own home automation systems to save money and to know the peculiarities of their systems in details.

As well as the author of [10], we have accepted the following definition as a basis: *«The Internet of Things (IoT) is the interconnection of uniquely identifiable embedded computing devices within the existing Internet infrastructure»*. As known, Embedded Systems (ES) can be used in conjunction with sensors and actuators for collecting the information and turning the collected or received information into actions. Also the ES can use a range of technologies

for connecting with other devices or the Internet (Wi-Fi, Bluetooth, RFID, Ethernet, GSM, CDMA and so on) [11].

In this case it is possible to distinguish several practically-oriented educational tasks: analysis of existing approaches to ES design, learning of ES software and hardware features, studying of the principles of ES interaction and connection to the Internet.

38.1.1 Embedded systems design techniques

ES are one of the most complex design objects for developers of computing systems [12]. Even a cursory analysis of typical requirements and constraints that must be considered during ES development confirms this. The main of them are

- minimal own power (possibly self-powered);
- minimal own size and weight;
- toughness and rigidity of the design;
- thermal control;
- radiative and electromagnetic resistance (possibly working in vacuum);
- guaranteed time between failures;
- term of availability solutions on the market, etc. [13]

The task of development of modern methods of computer aided design is still relevant due to the necessity of increasing of efficiency of ES computer aided design against the backdrop of growing requirements for reducing the design time of ES while ensuring their quality.

Experts [14-15] present and analyze the following, most perspective approaches to ES hardware/software design that address the problems of the traditional approach: parallel design (co-design); object-oriented design; platform-based design.

CoDesign is considered as one of perspective approaches to ES design. CoDesign technique has both advantages and disadvantages. On the one hand, it complicates the embedded systems' design, and on the other hand it improves significantly the characteristics of the final product in comparison with alternative versions of design solutions [14].

Object-oriented design of the ES took over the general methods used for software development. In this approach, software methods are

used to the hardware description languages. This approach allows to use advantages of the object-oriented methodology (the reuse methodology and managing the complexity) [16].

The platform-based approach is based on the reuse methodology [17] and allows to reduce significantly design time by reusing pre-implemented and tested software and hardware components of the system. Reusable software components include: real-time operating systems, application programming interfaces (APIs), libraries, drivers, etc.

Revolution of platform-based approach in the design was the beginning of the new concepts of ES quick development and prototyping. Ready hardware/software platforms give possibility of systems components reuse for the design process efficiency improvement. As reusable components hardware-software platforms (Arduino, STM Discovery, Raspberry Pi etc.) are used. The application of such platforms simplifies the design phase of the ES due to the usage of ready-made constructive solutions. In addition, the specialized software supplied with them, a high-level programming language, a large number of standard functions and libraries, simplify the writing and debugging of the ES software.

The method of ES computer aided design was improved on the basis of joint application of parallel and platform-oriented approaches, reuse methodology and remote engineering tools (recommendation system and remote laboratory) (Fig. 38.1). The recommendation system allows to reduce the time of transition between the system and the functional-logical levels of ES design and to increase the level of design works automation at the expense of hardware-software platform automated selection [18-20]. The remote laboratory allows to share the equipment and software for prototyping of designed ES, and thus to drop the cost of projected products [21-22].

38.1.2 Hardware/software platforms for embedded systems realization

Today, in the field of ES design is very popular the usage of ready hardware/software platforms allowing to accelerate development of products so to reduce the time to market.

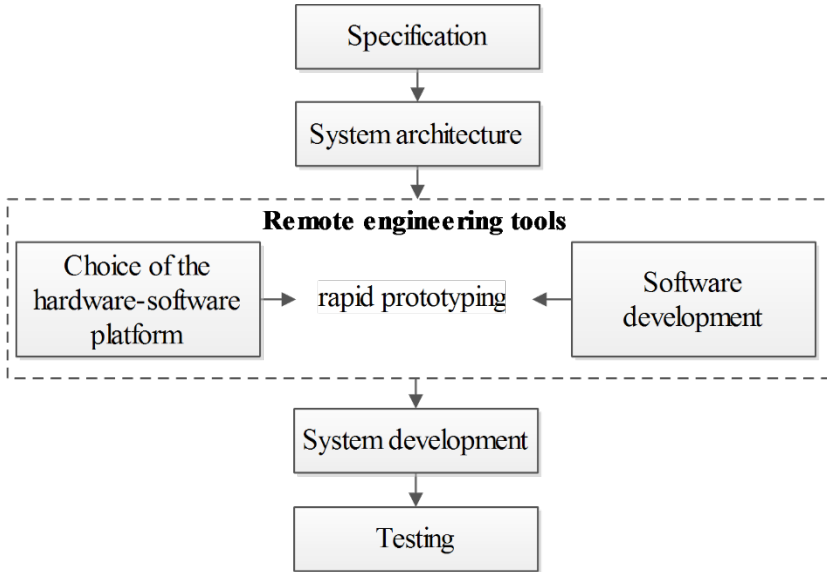


Fig. 38.1 – Modern design flow of embedded systems

There are many different manufacturers of hardware/software platforms: Arduino, Texas Instruments, Parallax Inc., Netmedia, Microchip, Digilent, MBED, Raspberry Pi, Cyclone. Each platform has the form factor and functionality, and designer's choice depends on the task. Thus, the designer of ES has to know possibilities of the ready platforms existing in the market and be able to make the responsible decision concerning application of a certain hardware-software platform. Unfortunately, the information which is offered on the website not always allows to make the right reasonable choice and optimally implement the project. Acquisition of a huge number of various platforms by small and medium-sized enterprises is unacceptable for the analysis of their opportunities, despite the relatively low prices.

Due to growth of popularity of ready hardware-software platforms, a number of the companies (e.g., Autodesk) offer applications for virtual simulation of their work. For example, it is possible to allocate such simulators for Arduino as: 123D Circuits, Virtualbreadbord, Simulino, Virtronics, Simuino, Arduino Simulator

and others. However, the simulation doesn't replace real work with the hardware and software. In fact, instead of real physical process the simulator allows to study only its mathematical model. Many software simulators are not free, requires time for their studying, have limited functionality and incomplete element base. There are also powerful packages of circuitry design, such as: ISIS PROTEUS, Altium Designer and others. However, the usage of their full functionality isn't always required, and the cost is quite high.

Therefore, the application of specialized remote laboratory for research of ready hardware-software platforms based on remote experiment is relevant [21-22].

There are already many articles comparing various development boards [23-25]. For comparison the following well-known platforms were chosen: Arduino Uno, LaunchPad, PCDuino, Raspberry Pi, BeagleBone Black (Table 38.1).

It is clear that Arduino and LaunchPad are in a different league than the PCDuino, Raspberry PI, Beagle Bone Black. The Arduino and LaunchPad are the microcontrollers. A microcontroller is just one tiny part of a computer. The Arduino can be programmed in C, but can't run an operating system. Arduino and LaunchPad are just perfect for electronics projects and prototyping. They allow rapid, cheap prototyping of ES.

Table 38.1. Well-known platforms' comparative analysis

	Microcontroller boards		Mini computer boards		
	Arduino Uno	Launchpad MSP430	PCDuino 3	Raspberry Pi	Beagle Bone Black
Price	20\$	10\$	59\$	35\$	45\$
MC/CPU	16MHz, ATmega 328	16MHz, MSP430 G2553	1GHz ARM Cortex A8	700 MHz ARM 1176JZFS	1GHz TI Sitara AM3359 ARM Cortex A8
RAM	2KB	512B	1GB	512MB, SDRAM	512MB, DDR3
Pins	14, 6	20, 3	32	2x13, 8	2x46
Overall size (mm)	68.6x53.4	66x51	121x65	86x54	86.4x53.3

On the other hand, the Raspberry Pi and PCduino are mini computers. They need an operating system to work. Those devices can run the operating system alone. The major differences between Arduino and LaunchPad are in the cost and the memory. A lot of the power of the Arduino is in its community code libraries. Besides the shields for LaunchPad are practically absent.

So, in comparison with other similar platforms, Arduino has a lot of advantages:

- the project was developed and develops as the project with an open code which works as the network project/community, allowing participants to exchange experience and ready applied practices, further accelerating the process of development and debugging;
- the low cost of the microcontroller and expansions for it;
- the simplicity and cross-platform of the programming environment (OS Windows, Macintosh OSX and Linux: 32/64bit).

38.1.3 Protocols and technologies for embedded systems interaction with other devices and Internet

Today a wide nomenclature of control and executive devices for home automation systems are presented in the market, but the issues of their unifying and certifying as well as integration into a single, easily configurable system are still open [26]. The analysis of exist smart components for SBS showed the necessity of a variety of platforms, devices, sensors, actuators application in one common system. On the other hand, a lot of wired and wireless technologies (KNX, Ethernet, ZigBee, Z-Wave, Wi-Fi, Bluetooth, etc.) for serving smart home needs are proposed, but their choice and implementation aren't the trivial tasks [27]. The main problem is the compatibility of the used protocols and network topologies. At the same time, the basic requirements for SBS are the simplicity of installation and exploitation, high degree of data protection and minimization of the costs associated with resource consumption [28-30]. Thus, the development of efficient and reliable SBS is an actual scientific and practical task that requires the application of a system approach and consideration of the entire set of requirements at all stages of system's life cycle [31-32].

It should be noted, that today, both wired and wireless technologies are actively used for connection of devices in the home

network. The wired technologies, which typically based on data transmission standard IEEE 802.3 (Ethernet), require individual cables for each home device, therefore they are expensive and difficult in the implementation.

The wireless technologies are used for data transmission at different distances without using wired communications, in places where it is impossible to use wires or it is unreasonable. For example, wireless technologies can significantly reduce the cost of home automation systems installing in finished premises, so they are preferable for most existing houses and apartments. Wireless technology is more easy to use, the cost of wireless devices is constantly decreasing and, at the same time, their speed and quality are permanently increasing. However, the issues of wireless connection stability and data transmission efficiency improvement require further study [33-34].

The wide range of wireless networks and popular protocols for them is presented in Fig.38.2.

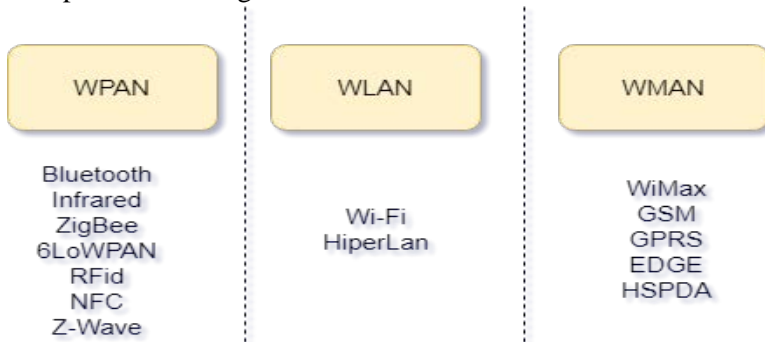


Fig. 38.2 – The wireless networks and popular protocols

Wireless Personal Area Networks (WPAN, IEEE 802.15) are used for local wireless connection, transmission of data from peripherals or sensors at short distances (0-100m). These networks are characterized by low bandwidth and low power consumption.

Wireless Local Area Networks (WLAN, IEEE 802.11) are used for personal computers and devices wireless connection (0-500m). The advantages of WLAN are prevalence of technology and high data rates [35-36].

Wireless Metropolitan Area Networks (WMAN, IEEE 802.16) are city-wide networks for devices connection within the city or in larger space. This class of networks is not used for SBS devices connection, but it allows to transmit the necessary data from house to house.

In order to create a wireless WPAN network for the SBS, it is advisable to choose a communication protocol that can provide the necessary functions and the reliable working of predefined types of smart components (devices, sensors, actuators, etc.). The results of comparison analysis of the widespread wireless protocols for SBS are shown in Table 38.2.

It's obvious, that the cost of the modules which support protocols Z-Wave, 6LoWPAN is relatively high and the user looks for cheaper options (Bluetooth, Wi-Fi) for SBS implementation.

The next important step is to choose one of the network topologies (Point-to-Point, Star, Tree, Mesh) for SBS wireless network development. There are clear recommendations for the usage of certain protocols within certain topologies. It is possible to organize the network using a protocol that is not functionally intended for target topology, but in this case the system's security and dependability will be under the threat, that is unacceptable for SBS. The results of the analysis of the options for different protocols and wireless network topologies are shown in Table 38.3.

Table 38.2 The comparison of the most popular wireless protocols

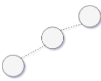



Technology	Bluetooth	ZigBee	Z-Wave	6LoWPAN	Wi-Fi	RF
Frequency, GHz	2,4	2,4; 0,915; 0,868	up to 1,0	1,0; 2,4	2,4; 5,0	0,433 ; 0,315
Speed, Mbps	up to 24	up to 0,25	up to 0,1	up to 0,250	up to 300	up to 0,01
Approx. range, m	up to 100	up to 100	30	800	up to 100	50
The cost of the module, UAH	120	170	330	500	100	43

The mixed solutions for networks topology are increasingly spread in practice. For example, a mixed topology with the allocation of SBS subsystems can be proposed that unites different topologies and protocols recommended for them (Fig. 38.3).

A big amount of ready solutions (SBS out of the box), based on wireless technologies (for example, Xiaomi Smart Home (ZigBee), Apple HomeKit (HomeKit Accessory Protocol), Orvibo (ZigBee), Fibaro (Z-Wave), Broadlink (QUIC), INELS (ZigBee), Connect Home (Z-Wave), Aeotec (Z-Wave), lifesmart (RF433 GFSK), Ferguson Smart Home (ZigBee, Wi-Fi), etc.) are presented today in the market for SBS realization.

The analysis shows that a lot of manufacturers prefer Z-Wave and ZigBee protocols which are currently relevant [37]. These protocols support Mesh network topology that satisfies the end-user preferences in the stability, dependability and security of the SBS. Moreover, they use low power and miniature radio frequency modules, which are embedded in consumer electronics and various devices.

Table 38.3 The analysis of options for different protocols and wireless network topologies

				
Protocol	Point-to-Point	Star	Tree	Mesh
Bluetooth	+	+		
Infrared	+	+		
RF433	+	+		
ZigBee	+	+	+	+
6LoWPAN	+	+	+	+
RFID	+	+		
NFC	+			
Z-Wave	+	+		+
Wi-Fi	+	+	+	+

At the same time, Wi-Fi protocol is widely used and popular for home applications [37]. The Wi-Fi technology is advanced and there is a large segment of low cost solutions (communication modules) for its implementation. Different Wi-Fi modules for data transmission (WizFi210, WI-FI UART shield, Arduino SPI Wi-Fi Module, RN171, etc.) provide quality and necessary range of communication and can be recommended for SBS as cheaper solutions. However, it should be borne in mind that for some modules the problems of significant power consumption and a lack of energy saving modes exist, which contradict the requirements of a long stand-alone work in SBS [38].

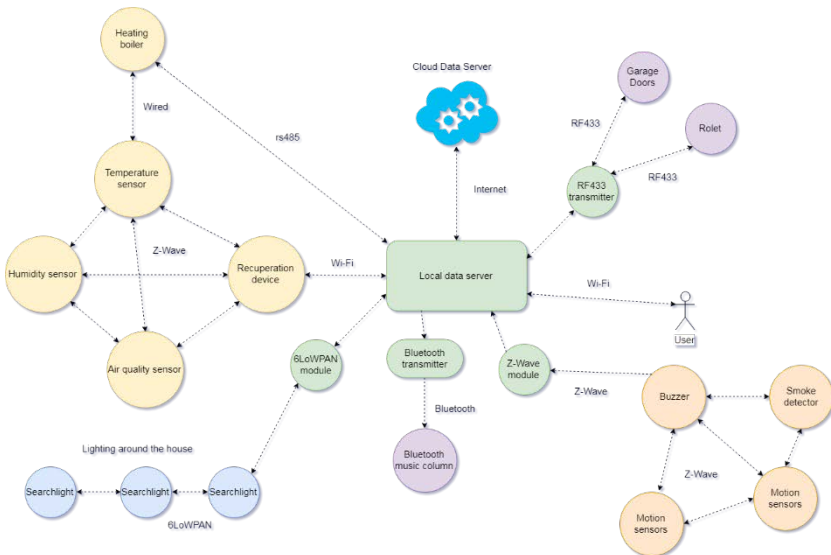


Fig. 38.3 – The example of SBS heterogeneous network based on different topologies and protocols

In order to investigate the features of WPAN/WLAN mesh network realization for SBS, the Wi-Fi microchip ESP8266 with full TCP/IP stack and microcontroller capability was selected. The microcontroller has a low price, supports hardware libraries and provides the abilities to execute programs from external flash memory with the interface SPI, as well as to build a communication network with different topologies.

During the experiment the wireless network with mesh topology was created for SBS based on several modules ESP8266. Such network topology has a rather complicated configuration and it is commonly used for large-scale mobile or other specific networks systems (WMAN). However, a high fault-tolerance is realized with such a topology and it is important for ensuring the reliability and safety of the SBS wireless network. A typical features of the mesh network are self-organization and self-configuration that provide the following capabilities: the usage of wireless transport channels for the structure of the network with the topology "Everyone with Everyone", the scaling of the network and the dynamic changing of coverage area, the stability of the network to the loss (rejection) of separate elements of the network.

The experiment was performed with the usage of the PainlessMesh [39] library, which implements the ad-hoc network without the necessity of central controller or router application. Any system with one or more nodes self-organizes itself into a fully functional Mesh network without the usage of TCP/IP. JSON objects are used as the messages. The device identification in the network is created due to the ID chip of the device. The library has the ability to send and receive messages.

The total size of the network is limited by the amount of the memory that can be allocated in the module. Each module functionally implements an access point (AP) and a client that connects to AP of another segment. There is a limit for the number of clients per node (4 clients for ESP82, 10 clients for ESP32) in the network. Each module periodically checks for unused APs that are nearby during the network organizing. The connection is made to the AP, which is unknown to the entire network in advance but it has the strongest signal. The node module connects to an unknown node avoiding the organizing of the ring topology of the network and implementing one route between a pair of nodes at a given time.

The experiment was performed for testing of the SBS Mesh network self-organization and stability (Fig. 38.4). The devices (ESP8266) were installed in the form of a rectangular triangle and a debugger output device was attached to each device. The transmission of information took place every three seconds in broadcasts (All to All). During the first turn, the network was self-organized and data was

transmitted between all devices (Fig.38.4, a). The next step was to shut down the device №2 (Fig.38.4, b) and to use an artificial barrier made of alloy steel for device №1. As a result, the working radius of the device №1 was reduced. After the device №2 was turned on again, the network was self-organized (Fig.38.4, c) in such a way that device №3 started to receive information from device №1.

Thus, the performed experiment proves the expediency of using Mesh networks for SBS and it confirms the possibility of the popular ESP8266 Wi-Fi (or new ESP32) modules usage for these purposes.

As the result, the heterogeneous network which is based on several topologies (including Mesh) and protocols can be recommended for the development of reliable home network.

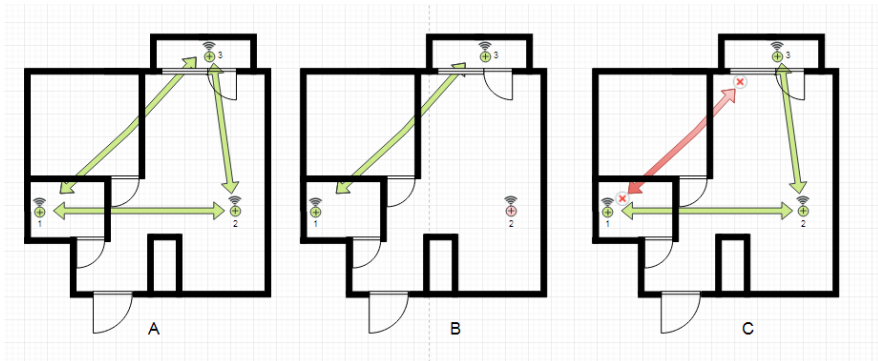


Fig. 38.4 – The schemes for Mesh network self-organization testing

38.2 Implementation of the software/hardware platform for Smart Building System

The realization of the architecture of SBS is connected with the problem of simultaneously executing of several critical requirements: using a wide nomenclature of control and executive devices, ensuring a high degree of data protection and minimization of the costs associated with resource consumption [28, 29, 31]. Depending on the customer's requirements, the architecture of the home automation system, as well as the set of hardware and software solutions, can differ significantly.

On the one hand, there is a huge number of devices, platforms and technologies for creation of home automation systems on the market [26]. The main requirements for them are interoperability, flexibility, security, simplicity of installation and exploitation, etc. Some of the companies offer the integration of their smart assistants into existing devices (Alexa, Google Home). The others are working on the new smart home devices (Nest, Walmart, ABB, British Gas). There are a lot of wired and wireless technologies (KNX, Ethernet ZigBee, Z-Wave, Wi-Fi, Bluetooth, etc.) for serving smart home needs [27]. There are smart home platforms (Wink, SmartThings from Samsung, HomeKit from Apple, Iris from Lowe) and solutions from security providers (for example, Tor Home Assistant) [40].

On the other hand, the issues of devices unifying and certifying, as well as of their integration into a single, easily configurable system are still open. The consequence for the industry generally is the slowing of the market pace, because consumers doubt the efficiency and safety of such systems and don't rush to install them.

The development of efficient and reliable SBS is an actual scientific and practical task that requires the application of a system approach and consideration of the entire set of requirements (energy efficiency, safety, cybersecurity etc.) at all stages of its solution.

38.2.1 The development of Smart Building System architecture

Today, the main trends of the SBS development are the Internet of things and devices, mobile and cloud technologies, as well as telematics. IoT technologies are actively used for the control of smart devices, transmission and processing of information, control of the energy system, water supply system, etc.

Telematics provides the correct interaction between wireless and wired systems, as well as it allows remote monitoring of smart home devices. That's why users increasingly prefer to use mobile devices for remote monitoring and control.

The usage of cloud technologies and services for convenient interaction of smart devices and software, as well as storing of the various information (images from video-cameras, data from various sensors, etc.) become more popular.

However, the main problem of the information security is precisely the permanent connection of intelligent home systems to the Internet. As the results there are risks associated with storing personal data in the network and the possibility of access to them by strangers. Nowadays, home automation systems do not have the proper level of protection to repel attacks of intruders. The most vulnerable smart devices are Wi-Fi or 3G-4G-routers and video cameras.

Hackers can not only crack the house access control subsystem, but also deactivate certain sensors, blind video-cameras, switch off the fire safety system, remotely control the heating / ventilation systems and even destroy the data and the house control software. The consequences of these actions are fraught with great material damage and are dangerous for people's health and life. Moreover, the access to the control system of a large number of people (several family members) is significantly weakening the protection of the SBS.

Therefore, professionals give clear recommendations on the level of house security improvement and minimizing the risks of cyber-hacking [41]. As long as most smart devices do not practically resist cyber-attacks, also it is necessary to adhere to certain rules related to their using [42].

In this way, the task of ensuring the reliable functioning of the home automation system should be solved at all levels, starting with requirements analysis, system architecture development and ending with system's operation. At the same time, it is necessary to apply methods of qualitative and quantitative assessment of the level of functional and information security at all stages of the system life cycle in order to timely identification of the vulnerabilities and the development of measures to eliminate weaknesses and reduce the risks of attacks.

38.2.2 The usage of Raspberry Pi and OpenHAB platforms for Smart Building System control

Eventually we propose to use two the most popular embedded platforms for SBS control - Arduino and Raspberry Pi [4, 9, 43, 44], as well as OpenHAB (Open Home Automation Bus). OpenHAB is the software for integrating different home automation systems and

technologies into one general solution that allows comprehensive automation rules and offers uniform user interfaces [45].

SBS subsystems can be based on Arduino boards: Solar station, Lighting control, Climate control, Access control, Safety control, Zone control, Presence control, Ventilation, Illumination control, etc.

All subsystems can be built on the basis of a typical structure (Fig. 38.5), which allows to integrate them into a common system effectively. A typical structure includes a communication module and Arduino controller for receiving, processing data from sensors, and controlling actuators. In order to upgrade and improve the protection of the laboratory the Modbus protocol is used, which guarantees the delivery of information packets, and in the case of data integrity violation, delivery is not performed.

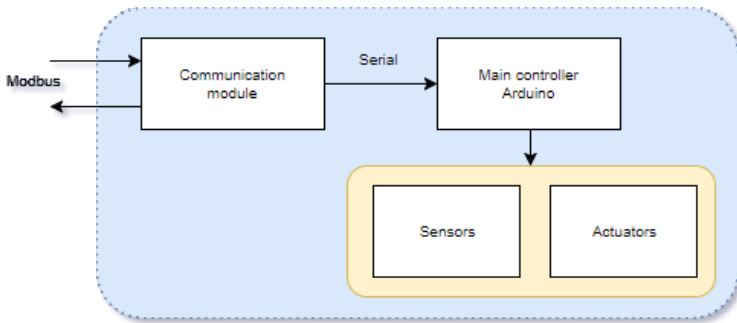


Fig. 38.5 – Typical structure of SBS subsystems

From the point of view of reliability improvement, the additional communication shield can be recommended, the usage of which would reduce the number of connecting wires, thereby reduce the number of failures. The structure of the communication shield and the scheme of its interaction with SBS server are shown in Fig. 38.6. Communication Shield is a platform for the placement of the Arduino controller, communication module RS485-TTL, as well as screw connectors, which provide a quality connection to the sensors and actuators of the subsystem.

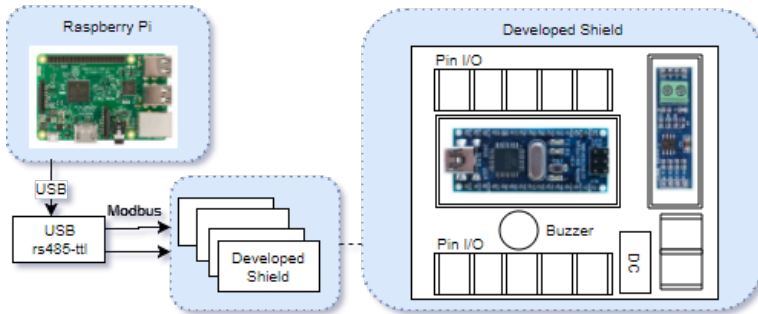


Fig. 38.6 – Communication shield structure and interaction with SBS server

Mini computer Raspberry Pi can perform the role of the SBS server with installed OpenHAB platform. Additional libraries Modbus TCP Binding be used for connection it with Arduino boards with USB interface and Modbus RTU protocol. Sequential line RS-232 can be used for communication between electronic devices.

Each Arduino board contains a program, which handles input and output data. Arduino uses open Modbus Master-Slave library. With the help of this library the holding registers of sign or non-sign type which available for recording and reading were created in each board (subsystem). Registers contain 8 or 16 elements of 16 bits length each. Thus, the structure for data exchange is created. Each Arduino board operates as Master. OpenHAB platform reads or adds data to registers when it interrogates the devices. Each element of the register is correlated to individual parameters of sensors or actuators.

The developers can use standard and create original Actions within Scripts and Rules for execution OpenHAB specific operations. For example, such Actions as Telegram, my.openHAB and other can be used for SBS events notification or feedback. Thus, connection to the Telegram allows sending messages to Telegram clients from a bot-client (for example - sending notifications to the user about the air conditioner turn on/off). With my.openHAB, users can connect to OpenHAB from any device from everywhere with the Internet

connection, to provide access to other users as well as to keep all activities and events in the cloud my.openHAB.

The administration of events executed by OpenHAB can be realized with MailControl binding. It provides the possibility of receiving commands sent via email in JSON format. The following types of commands can be sent: decimal, HSB, increase – decrease, on – off, open – closed, percent, stop – move, string, up – down. Also the integration with Google calendar for SBS is possible. Users can create events and manage the SBS on a schedule (on/off lighting, air conditioning, open/close the door for a predetermined time, etc.).

38.3 The application of the remote laboratory Smart House&IoT for Smart Building System prototyping

The Remote Laboratory (RL) Smart House&IoT is the part of the integrated complex REIoT, which also includes the RL RELDES (REmote Laboratory for Development of Embedded Systems) [46].

The RL Smart House&IoT can be effectively used for IoT technologies studying and investigations of the features of SBS development (Fig. 38.7). The laboratory includes IP camera D-Link DCS-2121 which transmits video streaming for users to view the experiments' current status. This IP-camera is a complete system with a built-in CPU and Web-server that transmits high quality video with resolution of 1280 x 1024 pixels and speed 10 frames per second. IP-camera and computer are connected via Ethernet cable and interact using protocol TCP/IP. Router D-Link DIR-300 allows to connect to the laboratory via Wi-Fi and also to add devices using network cables.

For the integration of two REIoT complex parts as well as for Smart House&IoT lab administration OpenHAB REST API was used [47]. To access Smart House&IoT lab experiments, RELDES administration system sends HTTP GET request to the OpenHAB REST API and receives results in JSON format. On receiving the list of available in the Smart House&IoT lab experiments, RELDES include them into the total list of experiments and after that a queue, statistics and other functions are available for them. Subsequently, to carry out the experiment, RELDES refers REST methods to the Smart House&IoT lab, for example HTTP PUT and HTTP GET requests are used for illumination level change and result control.

In order to start the streaming broadcast, we have used the utility ffmpeg [48]. Ffmpeg is a set of free libraries with open source code that allow record, convert and transmit digital audio and video in various formats. Library ffmpeg starts to catch video from our camera with resolution 1280 x 1024, codes it to MPEG format with 10 fps and bitrate 800kbit/s, and after that uses HTTP for sending to local server, which sends this video stream to the end user. In order to divide video for blocks (to cut and select the part of video for each experiment), the filter "crop" is used. As a result, we have got some video fragments for each experiment or for group of experiments.

The RL Smart House & IoT gives possibility for practical studying of SBS networks based on wired (Modbus RTU, Ethernet) and wireless (Wi-Fi) technologies.

The RL Smart House&IoT (Fig. 38.8) can be effectively used for investigation of the issues of energy efficiency, safety and cybersecurity of the SBS, as well as for solving the task of its comprehensive analysis, qualitative and quantitative assessment of the system indicators.

Several experiments can be united to groups and performed simultaneously. In this case, the users study the principles of interaction between subsystems, define the process logic, create effects, evaluate the reaction of the elements and analyze the results.

Scenario 1. The studying of the issues of resource conservation and energy efficiency based on the group of experiments, which enable the parameters of solar energy, lighting, heating, air conditioning, ventilation and recuperation subsystems controlling.

Components of the experiments: Arduino Nano V3 (5V); Solar Paner (6V, 250mA); Resistive divider (1/2); Charge Controller (TP509); Battery (3.7V, 1100mA); Loads driver L298 (5-35V, 2A); RGB and white LED tapes; DC Power Supply 5V, 1A and 12V, 4A; Relay 5V; Peltier element; Temperature and humidity sensors DHT22 and DHT11; Air quality sensor MQ135.

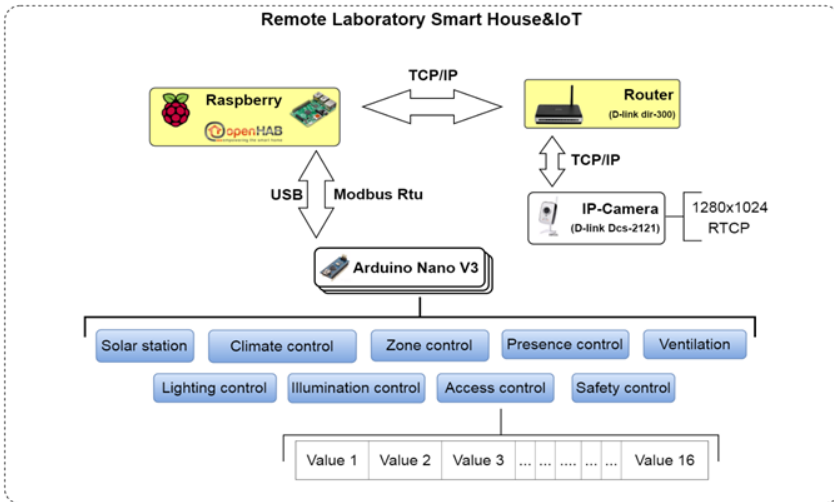


Fig. 18.7 – Smart House&IoT lab structure

Experiment Solart station allows studying the principles of solar energy obtaining and accumulating and demonstrates the typical scheme for organizing of the process of energy accumulation in batteries. During the experiment, it is possible to trace the change of the voltage produced by the solar panel when the illumination intensity is changed (Fig. 38.9).

Experiment Illumination control give possibility to study the basics of the loads driver functioning and the principle of multicolored (RGB) LED lighting systems creating, as well as RGB LED tape control Arduino NANO has the ability to generate a PWM (Pulse Wide Modulation) signal on some pins, which is transmitted to the inputs of the L298N load driver.

The L298N module acts as RGB controller and gives possibility to control four DC load channels, depending on the PWM input signal. The level of output DC on the channels of RGB tape is proportional to the input channel. The multi-colored (RGB) LED tape (depending on the type of tape) has 4 inputs (RED, GREEN, BLUE, + 12V). Depending on the level of DC, the brightness of the required color sets on the LEDs. * The L298N load driver has the ability to control loads with a current of 2A. Pay attention to the characteristics of the LED tape.

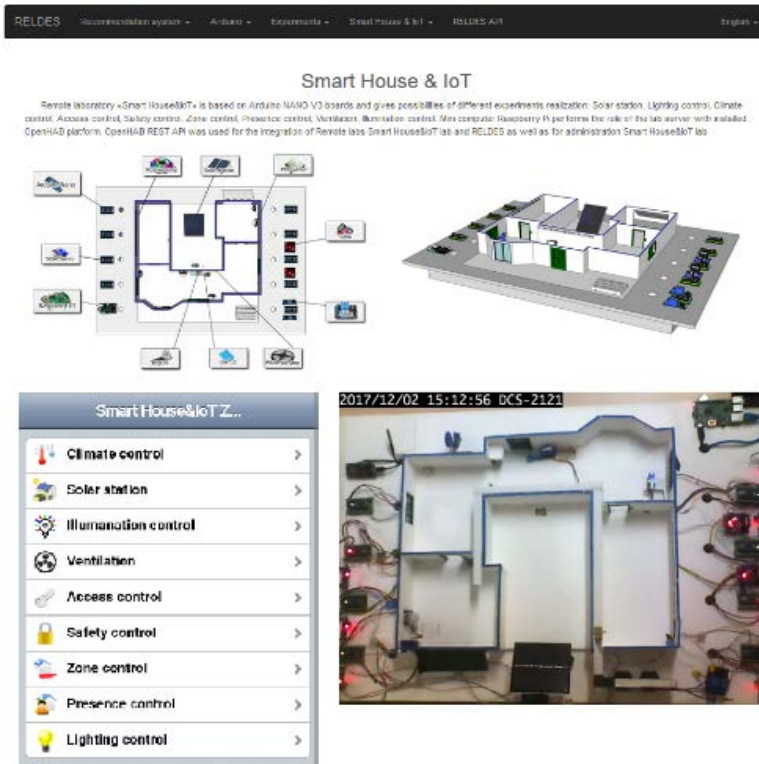


Fig. 38.8 – Web interface of the RL Smart House & IoT

Experiment Lightning control gives possibility to study the basics of dimmer's operation using the example of control of a white LED strip. The dimmer allows you to control the electrical power and thus control the level of illumination. The experiment also makes it possible to reproduce the automatic control algorithm under the necessary conditions. Arduino Nano receives a numerical value for the required level of illumination and generates a PWM signal for the load driver.

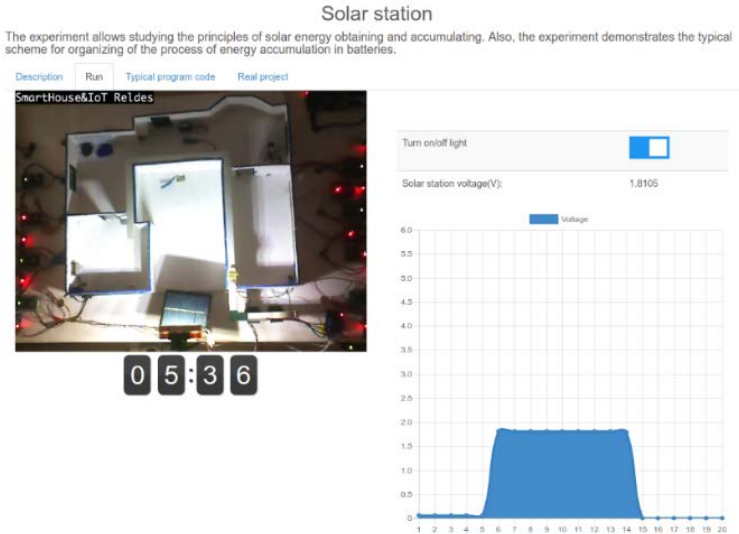


Fig. 38.9 – Experiment Solart station web-page

The load driver controls voltage on the LEDs. Thus, the illumination level is controlled. The load driver performs the dimmer function. The dimmer, depending on the type, can control the alternative and direct voltage.

Experiment Ventilation demonstrates the principles of ventilation system constructing with air flow speed controlling and air heating for heating the rooms. Arduino Nano generates a wide-pulse signal for the L298 load driver thereby controlling the fan speed. Also, Arduino Nano controls the Peltier element by the means of relay module for air heating. DHT22 sensor measures the temperature and humidity of the heated air. To conduct the experiment, drag the slider to the desired position, thereby adjusting the speed of the fan in the ventilation system.

Experiment Climate control allows studying the method of climate control, based on data from temperature and humidity sensors. Also, the possibility of air quality control implemented, using of sensor for chemical impurities determining in the air. The experiment demonstrates the principles of temperature control at different points of the room. Also, experiment demonstrates the operation of temperature

and humidity sensors with different accuracy, as well as, the air quality sensor that analyzes the presence of impurities (gas, ethyl). An important controlled indicator of climate control is the ratio of room temperature to humidity. Controller Arduino Nano makes interrogation of humidity and temperature sensors DHT11 and DHT22, as well as analog sensor of air quality MQ135. Also, Arduino Nano controls, the Peltier element, which realize air heating.

Scenario 2. The studying of the safety and security issues based on the group of experiments, which enable to monitor access to controlled zones and objects.

Components of the experiments: Arduino Nano v3; RFID reader RC522; Loads driver L298 (5-35V, 2A); RGB LED tape; DC Power Supply 5V, 1A and 12V, 4A; Servomotor SG90; PIR sensor; Laser Module KY-008; Light Sensor (LDR) VT90N.

Experiment Safety Control demonstrates the principles of the security system of the premises working as well as its components the notification subsystem, object control and the subsystem for the state of the room monitoring. Most security systems are implemented at a low level to achieve greater fault tolerance and are self-contained, i.e. their work will not be affected by the work of other systems. Once armed, the Arduino Nano controller locks all doors and windows in the room and monitors the statuses of the PIR motion sensors. In the case of a break-in or penetration into one of the monitored areas, a light indication occurs (Fig. 38.10).

Experiment Access Control allows studying the principles of creating of access control systems to different rooms using a combination lock. The access identifier is the RFID card or keychain and the RFID reader RC522. The RFID reader RC522 reads the radio tags, which are within the range of the reader, permanently. The RFID module does the polls with a frequency of 13.56 MHz and interacts with the Arduino NANO v3 controller using the SPI interface. It is necessary to authorize one of the keys for the experiment holding. Only one key is allowed for entering. The result of the experiment is the granted access to enter. (The actuator fires that and the the door opens). When one of the keys (card or keychain) is moved to the reader, the key is read and compared with the database of users with authorized access in the controller. Users who do not have permission are denied.

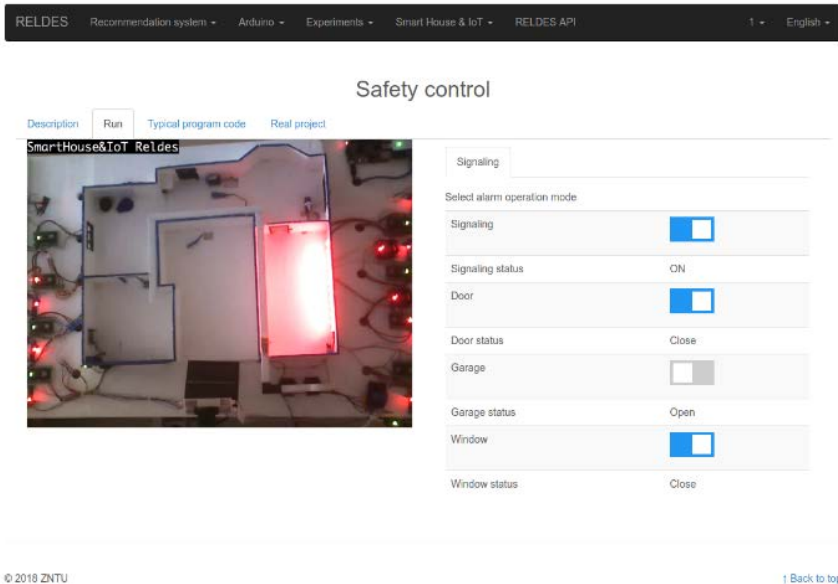


Fig. 38.10 – Experiment Safety Control web-page

Experiment Presence control allows studying the principles of presence monitoring systems and security systems functioning by changing the operation mode of the subsystem. The possibility of motion control in several areas can be realized based on PIR sensor usage. This task is also matches previous scenario, because allows to control different equipment according users presence or absence.

Experiment Zone control allows studying the principles of security systems creation based on lasers. It gives possibilities of realization of invisible controlled barriers for specific zones.

Scenario 3. The studying of the cybersecurity issues based on the group of experiments, which provide the usage of wireless, cloud and mobile technologies for system monitoring and control, as well as for data collection and visualization.

Components of the experiments: minicomputer Raspberry Pi, Wi-Fi module Node MCU ESP8266; digital temperature and humidity sensor DS18B20; Wi-Fi adapter TP-link 722n; Router d-link dir-300.

Experiment OpenHAB control allows studying additional features of the OpenHAB platform (my.openhab, MailControl and

Telegram), which allow to control SBS through the Internet, collect device statistics, receive notifications on users mobile devices.

Experiment Wi-Fi security allows studying the principles of connecting devices via Wi-Fi protocol, checking the stability and security of the connection, as well as the demonstration of exceptional situations.

The experiment uses the attack method with the aim of wireless clients deauthentication. This attack sends packets to one or more clients that are currently connected to a specific access point with the aim to be disconnected. Clients can be disconnected based on several actions. The capture WPA/WPA2 handshakes by forcing customers to disconnect is realized in this experiment. The results of the experiment for temperature measurement based on ESP8266 and digital temperature and humidity sensor DS18B20 are presented in Fig. 38.11. It is obvious, that the lack of data from the sensor can lead to undesirable consequences in the SBS working.



Fig. 38.11 – Experiment Wi-Fi security web-page

The task of SHS online laboratories development and usage is an actual problem nowadays, in case of active virtual and remote engineering technologies and globalization progress. These laboratories are available at any time from every part of a world for all students and

developers who want to study and make researching in the area of home automation systems.

38.4 Work related analysis

Analysis of MSc and PhD curriculums, as well as the results of research of colleagues from University of Coimbra (Portugal) [8], Newcastle University (Great Britain) [9], University Politehnica of Bucharest (Romania) [30], Madrid Polytechnic University (Spain) [49] was carried out during the development of this section.

Today universities all over the world creates their own educational stands and laboratories for SBS studying. They can help students to have experiments with a real equipment. Madrid Polytechnic University has two real home automation laboratories and one of them is oriented on habitants that have special needs. Voice controlled home automation laboratory was also created in Cornell University (Itaka, USA) [50].

The article [4] is intended to provide developers with information on products and services that are useful and of value for smart home vertical rapid path to product edge IoT solution using the Intel® IoT Developer Kit and Grove* IoT Commercial Developer Kit.

The paper [5] presents the concept of human centered scalable ecosystem development which is driven by 5G/IoT paradigm and follows the philosophy of disruptive innovation. The development cycle includes both the process and the implementation of an ecosystem.

The authors of [6] claim that creating or transforming a building into a smart building is beneficial for both the owner and the organizations working within. These benefits range from energy savings to productivity gains to sustainability. Smart building strategies can reduce energy costs, increase the productivity of the facility staff, improve building operations, support sustainability efforts and enhance decision-making across the organization.

In [26] two categories of home automation systems are presented: all-around smart home systems, which are designed to coordinate a wide variety of smart home products, and security-focused systems, which are built around sensors and sirens.

In work [28] the issues of housing energy consumption growth against the background of the development and application of a large

number of energy-efficient devices are discussed. The problem seems to come from not only the lack of information about how to use these devices but also from the lack of willingness from inhabitants. This double assessment invites to think about support toward inhabitants' behaviors concerning to energy consumption, which is affected by both devices and values.

Authors of [29] show how with the IT technology, the traditional power grid is being upgraded to the smart grid (SG) with two-way communication and power flow between utilities and customers. The smart grid includes new technologies in distributed energy generation and distributed energy storage, advanced measurement and sensing, controls, cyber security, consumer-side energy management, and environment protection. Thus, it shows the advantages in efficiency, reliability, and security.

The problems of large amounts raw data that smart buildings generate are given in [30]. This poses significant challenges from both the data management perspective as well as leveraging the associated information for enabling advanced energy management, fault detection and control strategies. Using exploratory analysis it is argued that data mining inspired approaches allow for fast and effective assessment of building state and associated predictions.

The paper [31] is devoted to the issues of design of secure cyber-physical systems based on embedded devices. It aims to develop a generalized approach to the design of secure systems based on embedded devices. Current approaches to design secure software and embedded devices are analyzed. The design lifecycle for secure embedded devices system is proposed.

The paper [35] guides developers of wireless systems who are puzzled by the vast number of radio configuration parameters and options. The authors provide experimental data comparing power consumption of Bluetooth Low Energy (BLE), ZigBee and ANT protocols for a cyclic sleep scenario.

The goal of [37] is to give awareness of commonly used protocols/technologies in smart metering, provide basic characteristics of them and describe their deployment in smart grids and the consequent advantages/disadvantages. The authors emphasize that modern wireless technologies didn't avoid smart metering as an integral part of smart grids. They have a high flexibility and can be easily

integrated into existing installations, it is feasible to use them for communication with meters.

In [43] the advantages of ready-made platforms are presented that can be used as building blocks for rapid development of network of intelligent devices with sensing, control and Internet access. The authors show that Arduino family of boards having high popularity and large number of sold units featuring open access, reliability, robustness, standard connections and low prices, possesses large potential for implementation of autonomous remote measurement and control systems of various levels of complexity.

The book [44] helps software engineers, web designers, product designers, and electronics engineers start designing products using the Internet-of-Things approach. It explains how to combine sensors, servos, robotics, Arduino boards with various networks or the Internet, to create interactive, cutting-edge devices.

Conclusions and questions

REIoT complex for SBS prototyping brings together several subsystems to create a true Internet of Things for home automation systems. It is used for a variety of training tasks in several modes. In the first mode the complex provides the possibilities of remote experiments on each subsystem separately and with the entire system as a whole. The descriptions of the experiments and measurement results are available for users in this case. Another mode allows users to specify the logic of the system working, programming and processes monitoring.

The investigation of SBS prototype gives the valuable practical experience for the real SBS development and allows to improve systems` functionality and characteristics as well as control based of IoT technologies.

In order to better understand and assimilate the educational material that is presented in this section, we invite you to answer the following questions.

1. Why ES can be considered as the basis of the Internet of Things infrastructure?
2. What ES design technologies are exist?

3. What are the features of the approach to ES design based on remote engineering technologies?
4. What are the advantages of ready-made hardware/software platforms usage for ES design?
5. What are the differences between the Arduino and Raspberry Pi platforms?
6. What are the requirements for modern SBS?
7. What are the problems of SBS development?
8. What does the term «SBS out of the box» mean?
9. What wired and wireless technologies are used to integrate SBS components?
10. What are the features of the implementation of wireless networks and protocols for them?
11. Why are the Z-Wave and ZigBee protocols most popular for SBS creating?
12. What are the differences between existing network topologies?
13. What are the advantages and disadvantages of a heterogeneous network for SBS?
14. What are the features of the Mesh network?
15. What are the Wi-Fi modules ESP8266 or ESP32 possibilities?
16. What are the typical subsystems of the SBS?
17. What is the structure of the remote complex REIoT?
18. What remote experiments can the remote laboratory Smart House & IoT perform?
19. How did the Raspberry Pi and Arduino boards communicate in the Smart House & IoT lab?
20. What is the purpose of SBS prototyping based on REIoT complex usage?

References

1. What is the Internet of Things, IoT. [Online]. Available: <http://www.tadviser.ru/index.php/> (in Russian)
2. Internet of Things (IoT). [Online]. Available: <http://www.cisco.com/web/solutions/trends/iot/overview.html>
3. M. Porter, and J. Heppelmann, “How smart, connected products are transforming companies”, *Harvard business review*. [Online]. Available: <http://www.ptc.com/internet-of-things/harvard-business-review/download-article-2#sthash.L5wGKzcN.dpuf>
4. IoT path to product: Smart Home. [Online]. Available: <http://www.codeproject.com/Articles/1119436/IoT-Path-to-Product-Smart-Home>
5. A. Rucinski, R. Garbos, J. Jeffords, and S. Chowdbury, “Disruptive innovation in the era of global cyber-society: with focus on Smart City efforts”, Proceedings of the International Conference on Intelligent data acquisition and advanced computing systems: Technology and Applications, 2017, pp. 1102-1104.
6. P. Tracy, “What is a smart building and how can it benefit you?” [Online]. Available: <https://www.rcrwireless.com/20160725/business/smart-building-tag31-tag99>
7. Gartner survey shows connected home solutions adoption remains limited to early adopters. [Online]. Available: <https://www.gartner.com/newsroom/id/3629117>
8. A. Amílcar and M. Alves da Silva, “Epistemologia e mechanica do risco: reflexoes”, Proceedings of the II Congresso Internamonal e VI Encontro Nacwonal de RISCOS, Coimbra, 2010.
9. M. C. Morisset, K. Pierce, C. Gamble, C. Maple and J. Fitzgerald, “A multi-modelling based approach to assessing the security of smart buildings”, Living in the Internet of Things: Cybersecurity of the IoT - 2018, 2018.
10. Internet of things – Overview, [Online]. Available: <http://www.codeproject.com/Articles/833234/Internet-of-things-Overview>
11. Stage 1 - Introduction to the Internet of Things: What, why and how, [Online]. Available: <http://www.codeproject.com/Articles/832492/Stage-Introduction-to-the-Internet-of-Things>
12. A. E. Platunov, “High-level design of embedded systems. Part 1: tutorial”, SPb.: NIU ITMO, 2011, 121 p. (in Russian)
13. A. Parkhomenko, and O. Gladkova, “Complex requirements analysis for the high-level design of embedded Systems”, Bulletin of the Lviv Polytechnic National University, Series *Computer design systems. Theory and practice*, 2014, vol. 808, pp. 3–9.

14. J. Teich, “Hardware/software codesign: the past, the present, and predicting the future”, *Proceedings of the IEEE*, Germany, vol.100, 2012, pp. 1411–1429.

15. M. Abdurohman, Kuspriyanto, S. Sutikno, and A. Sasongko, “The new embedded system design methodology for improving design process performance”, *International journal of computer science and information security*, vol. 8(1), 2010, pp. 35–43.

16. V. Tero, “An embedded object approach to embedded system development”, OULU University press, 2009, 130 p.

17. W. T. Simpson and, J. T. Marion, O.L. de Weck, and K. Holtta-Otto, “Platform-based design and development: current trends and needs in industry”, *Proceedings of the International design engineering technical conferences & Computers and information in engineering*, Philadelphia, Pennsylvania, USA, 2006, pp. 1–10.

18. A. Parkhomenko, O. Gladkova, A. Sokolyanskii, V. Shepelenko, and Ya. Zalyubovskiy, “Reusable solutions for embedded systems’ design. Proceedings of the 13th International conference on Remote engineering and virtual instrumentation, Madrid, Spain, 2016, pp. 313–317.

19. A. Parkhomenko, O. Gladkova, A. Sokolyanskii, and Ya. Zalyubovskiy, “Investigation of reuse concepts for embedded systems design”, *Proceedings of the XII International conference on Perspective technologies and methods in MEMS design*, Lviv: NU “Lviv Polytechnic”, 2016, pp. 78–80.

20. S. Subbotin, O. Gladkova, and A. Parkhomenko, “Knowledge-based recommendation system for embedded systems platform-oriented design”, *Proceedings of the XIII International scientific and technical conference on Computer science and information technologies*, Lviv, Ukraine, 2018, pp. 368-373.

21. A. Parkhomenko, O. Gladkova, E. Ivanov, A. Sokolyanskii, and S. Kurson, “Development and application of remote laboratory for embedded systems design”, *International journal of online engineering*, vol.11(3), 2015, pp.27–31.

22. A. Parkhomenko, O. Gladkova, S. Kurson, A. Sokolyanskii, and E. Ivanov, “Internet-based technologies for design of embedded systems”, *Journal of control science and engineering*, vol. 3(2), 2015, pp. 55–63.

23. R. Santos, “Arduino vs Raspberry PI vs Beagle Bone Black vs PCduino” [Online]. Available: <http://randomnerdtutorials.com/arduino-vs-raspberry-pi-vs-beaglebone-vs-pcduino/>

24. A. Allan, “Which board is right for me? ” [Online]. Available: <http://makezine.com/magazine/make-36-boards/which-board-is-right-for-me/>

25. M. Leonard, "How to choose the right platform: Raspberry Pi or BeagleBone Black?" [Online]. Available: <http://michaelleonard.com/raspberry-pi-or-beaglebone-black/>
26. Best smart home systems for a connected domicile. [Online]. Available: <https://www.techhive.com/article/3206310/connected-home/best-smart-home-system.html>
27. N. Zhogov, "Communication protocols for the smart house" [Online]. Available: <https://www.ferra.ru/ru/digihome/review/SmartHome-Protocols/#1-Wire> (in Russian).
28. H. Haller, V.-B. Nguyen, G. Debizet, Y. Laurillau, J. Coutaz, and G. Calvary, "Energy consumption in Smarthome: persuasive interaction respecting user's values", Proceedings of the International conference on Intelligent data acquisition and advanced computing systems: technology and applications, 2017, pp. 804-809.
29. L. Zhang, and X. Xiong, "Optimization of the power flow in a Smart Home", *Online engineering & Internet of Things*, Lecture notes in Network and systems, Springer: Cham, vol. 22, 2017, pp. 721-730
30. G. Stamatescu, I. Stamatescu, N. Arghira, C. Dragana, and I. Fagarasan, "Data-driven methods for Smart Building AHU subsystem modelling", Proceedings of the International conference on Intelligent data acquisition and advanced computing systems: Technology and applications, 2017, pp.617-621
31. D. Levshun, A. Chechulin, I. Kotenko, "Design lifecycle for secure cyber-physical systems based on embedded devices", Proceedings of the International conference on Intelligent data acquisition and advanced computing Systems: Technology and applications, 2017, pp. 277-282.
32. V. Teslyuk, V. Beregovskiy, and A. Pukach, "Automation of the smart house system-level design", *Informatyka, Automatyka, Pomiar y Gospodarce i Ochronie Środowiska*, vol. 4, 2013, pp. 81-84.
33. B. Shevchuk, O. Ivakhiv, M. Geraimchuk, and Y. Brayko, "Efficient encoding and trasmission of monitoring data in information efficient wireless networks", Proceedings of the International symposium on Wireless systems within the conferences on Inteligent data asquisition and advanced computing systems, 2016, pp. 138-143
34. I. Zhuravska, "Ensuring a stable wireless communication in cyberphysical systems with moving objects", *Technology audit and production reserves*, 5/2(31), 2016, pp. 58–64 (in Ukrainian).
35. S. Dementyev, S. Hodges, and J.-S. Taylor, "Power consumption analysis of bluetooth low energy, ZigBee and ANT sensor nodes in a cyclic sleep scenario", Proceedings of the International wireless symposium, 2013, pp. 1-4.

36. A. Makarenko, A. Parfenova, and S. Mogilny, “Wireless technologies of data transfer Wi-Fi, Bluetooth and ZigBee”, *Bulletin of the National Technical University of Ukraine "KPI" Series Radio Engineering. Radio Apparatus Building*, vol.41, 2010, pp. 171-181.

37. L. Šťastný, L. Franek, P. Fiedler, “Wireless communications in smart metering”, *Proceedings of the 12th IFAC Conference on Programmable devices and embedded systems*, 2013, pp. 330-335

38. ESP8266 Wi-Fi solution. [Online]. Available: <https://www.espressif.com/en/products/hardware/esp8266ex/overview>

39. PainlessMesh Technical Documentation. [Online]. Available: <https://gitlab.com/painlessMesh/painlessMesh/wikis/home>

40. TOR HOME ASSISTANT: How to protect Smart House with “anonymous” network? [Online]. Available: https://moy-domovoy.ru/news/20161214/tor_home_assistant_kak_zashchitit_umnyy_dom_s_pomoshchju_anonimnoy_seti/ (in Russian).

41. Cybersecurity of Smart House [Online]. Available: http://www.bestron.ru/news/kiberbezopasnost_umnogo_doma (in Russian).

42. Smart home and cybersecurity: how to protect your data [Online]. Available: <http://aquagroup.ru/news/umnyy-dom-i-kiberbezopasnost-kak-zashchitit-svoi-dannye.html> (in Russian).

43. V. Cvjetkovic, and M. Matijevic, “Overview of architectures with Arduino boards as building blocks for data acquisition and control systems”, *International Journal of Online Engineering*, vol. 12 (7), 2016, pp.10-17

44. A. McEwen, and H. Cassim, “Designing the Internet of Things”, Wiley, 2014, 324 p.

45. Open HAB [Online]. Available: <http://www.openhab.org/>

46. REIoT [Online]. [Online]. Available: www.swed.zntu.edu.ua

47. REST API [Online]. Available: <https://github.com/openhab/openhab/wiki/REST-API>

48. FFmpeg [Online]. Available: <https://www.ffmpeg.org/>.

49. Internet of Things (IoT) [Online]. Available: <http://www.upm.es/internacional/Students/StudiesDegrees/University%20Masters/Master%20programs?id=59.7&fmt=detail>

50. A wireless, voice-controllable, household system [Online]. Available: https://people.ece.cornell.edu/land/courses/ece4760/FinalProjects/f2012/jw937_sz369/jw937-sz369/jw937_sz369.html

39. TECHNOLOGIES OF INTERACTION IN THE SMART BUILDING/CITY SYSTEMS

Assoc. Prof., Dr. O. Martynyuk, Prof., DrS O. V. Drozd

Contents

Abbreviations	285
39.1 Technologies of component interactions in systems of IoT at the level of their formal specifications	286
39.1.1 Specification of general architecture properties of domain components, structures, requirements to SBC	287
39.1.2 Specification of entities, relations, functions, data, conditions, events, actions of interactions of SBC	289
39.1.3 Modeling of entities, relations, functions, data, conditions, events, actions of interactions into flow process of SBC	293
39.2 Technologies of component interactions of Smart Building on a behavioral level	295
39.2.1 Specification of interactions into essentially static structure of Smart Building	296
39.2.2 Modelling of interactions into distributed dynamic flow process of functioning of Smart Building	300
39.3 Technologies of component interactions of Smart City at the level of process synchronization	304
39.3.1 Specification of interactions into essentially dynamical structure of Smart City	305
39.3.2 Modelling of interactions into distributed dynamic flow process of synchronization of Smart City	309
39.4 Work related analysis	313
Conclusions and questions	316
References	318

Abbreviations

AMI – Advanced Metering Infrastructure

ATS – Average Travel Speed

CPN – Colored Petri Nets

LTL – Linear Temporal Logic

PN – Petri Nets

QS – Queuing Systems

SB – Smart Building

SBC – Smart Building and City

UML – Universal Modeling Language

The purpose of the section is description of formal specification and modeling of interactions into Smart Building and City (SBC) of systems on base dynamical structural, functional and asynchronous/event representations with the use of the dynamic UML-diagrams, Queuing Systems (QS), Petri Nets (PN), linear temporal logic (LTL) and also development of skills of use of the gained knowledge in practice of constructing the system of SBC.

Section object is to understand formal dynamical spatial, structural, component, object, behavioral and temporal models of interactions for systems SBC in the form of dynamical UML diagrams, QS, PN and their compositions, expressions and conclusions of LTL.

Section subject is a formal processes of specification and modeling, of the dynamical spatial, structural, component, object, behavioral and temporal models of interactions for systems of SBC.

Tasks of the section:

1 Review of technologies, architectures, components of specification and modeling of interactions for distributed process into subsystems of SBC.

2 Formal specification and modeling of general entities, relations, conditions, events, actions of interactions into distributed process of systems of SBC on the basis of dynamical visual UML diagrams, QS, PN, LTL.

3. Formal temporal evolutionary behavioral specification and modeling of interactions into distributed process of subsystems of Smart Building with essentially static structure and hybrid communications.

4 Formal temporal multiagent behavioral specification and modeling of interactions into distributed process of subsystems of Smart City with essentially dynamical structure and wireless communications.

39.1 Technologies of component interactions in systems of IoT at the level of their formal specifications

The following objects are taken as input:

1) The specifications of the technical description of the architecture of components, subsystems of Smart Building/City (SBC), as well as such systems as a whole in analytic-text, tabular, graphical

representations, defining the entities, relations, component structure and their topological relationships, system and component functions, information objects, interfaces of topological interactions (format, dimension, type, conditions of transmission over the topological connections of the objects to be sent – parameters, data, methods and their compositions), the temporal behavior of functions and scenarios (time diagrams, graph, automaton, algorithmic representations).

2) The previously prepared, UML diagrams, QS and Petri nets, LTL-specifications, which define some parts of the architecture of components, subsystems of SBC, and also such systems, as a whole in analytic-text, tabular, graphical representations, for which partial system-wide interactive-visual specification and modeling are defined, in particular, in the Star UML, ExtendSim Demo, CPN Tools and SPIN tools environment.

The following objects are considered as output objects: the resulting full correct UML diagrams, QS, Petri nets and LTL-specifications, which represent the full architecture of components, SBC, as well as such systems in general, in analytic-text, tabular, graphical representations, for which in the corresponding instrumental environment, particular, Star UML, ExtendSim Demo, CPN Tools and SPIN, system interactive-visual specification and modeling with special results of fulfillment of conditions, parameters and scenarios, are executed.

39.1.1 Specification of general architecture properties of domain components, structures, requirements to SBC

Specification of general architecture properties of Smart Building/City (SBC) [1, 2, 4, 7, 8, 9, 10, 11, 18, 24-28], in particular, special characteristics of process interactions, define their domain components, structures, requirements.

Specification of these properties of components, objects and functions for domain subsystems of SBC and their general models include next stages and steps for future analysis:

Stage 1. Formal definition of main architectural abstract objects from the general models of subsystems of SBC by execution of specification steps for: components (Step 1); component functions and handlers (Step 2); information objects (Step 3); interfaces (Step 4);

scenarios (Step 5); conditions (Step 6); events (Step 7); actions, include interruption-exclusion-errors (Step 8); priorities (Step 9).

Stage 2. Definition of real types, features, properties and procedures of the real domain subsystems of SBC by execution of specification steps for: objects/subsystems of electricity, heat, gas, water, food supply (Step 1); illumination, temperature, humidity, ionization (Step 2); air conditioning, cooling, freezing, ventilation (Step 3); smoke, CO/CO₂ (Step 4); cleaning, washing (Step 5); security, survivability (Step 6); information (Internet, smartphone, smartTV, video surveillance, video intercom) communications (Step 7); transport (elevators, bikes, electric scooter, auto/electro transport) communications (Step 8); autonomous zone of wildlife (plants, greenhouse, animals) (Step 9); facilities and means of health (indicators and stimulants, simulators, fitness rooms and clubs, swimming pools) (Step 10).

Specification of detailed types, structures, requirements and specification of components, communications, functions, resources, consumers for specific models of subsystems of SBC include next stages and steps for future analysis:

Stage 1. Formal definition of detailed types and features for the specific models of subsystems of SBC and their components by execution of specification steps for: end-points – simple sensors and actuators, preliminary processing sensors and final processing actuators, intelligent sensors and actuators, controlled communication panel, end-point controller (Step 1); brokers/controllers/monitors/routers/wireless-access-point, in future – broker, – data brokers, processing brokers, communication and distribution brokers, combined brokers (Step 2); system servers – data servers, processing servers, communication and distribution servers, combined servers (Step 3); end-user and administrator terminals – workstations, notebooks, smartphones, special video, audio and sensor ports, panels, joysticks, wheels (Step 4).

Stage 2. Formal definition of detailed structure for the specific spatial and temporal models of subsystems of SBC and their components by execution of specification steps for: topological multilevel structures and topological graph elements – base and anti-base (input/output), nodes, chains, trees, hammocks, feedbacks, common entrances, exits, cross-level transitions of the building (Step

1); spatial, including horizontal intro-level decomposition (inside some level of OSI) (Step 2); and vertical interlevel decomposition (according to adjacent levels of OSI) (Step 3); temporal representing algorithms and diagrams of processes for components, subsystems and SBC (Step 4); all conditions, events and actions, embedded in spatial structures (Step 5); all conditions, events and actions, embedded in temporal structures (Step 6); part of static constants and long-term relationships, connections, conditions, events and actions from their domain slow processes of objects, components, subsystems of SBC (Step 7); part of dynamic instantaneous and short-term relationships, connections, conditions, events and actions from their domain quick processes for flows of objects, components, subsystems and SBC (Step 8).

Stage 3. Design definition of system constructive requirements and specification of components, subsystems and SBC by execution of specification steps for system specification, specification of requirements for: distribution, sharable, rights and attributes of subjects and objects of functioning (Step 1); mode, priority and discipline of functioning (Step 2); special SBC-technology, SBC-hardware, SBC-software, SBC-data, SBC-protocol and SBC-resource (Step 2); special characteristics, properties, methods and their values of the selected SBC-technology, SBC-hardware, SBC-software, SBC-data, SBC-protocol and SBC-resource (Step 3).

39.1.2 Specification of entities, relations, functions, data, conditions, events, actions of interactions of SBC

Specification of developed hosting environment of SBC define domain characteristics for environment of components/subsystems/system and SBC [1,2,4,7,8,9,10,11,18,24-28] generally.

Formal definition of these domain characteristics for developed and developed hosting environment of components, subsystems and SBC include next stages and steps for future analysis:

Stage 1. Specification of static objects and properties for developed hosting environment of the domain components/subsystems/system of SBC – end-points sensors/actuators, end-points auto-/semiauto-controlled communication panels, end-points controllers, zone controllers/brokers/routers/wireless-access-points, in future – zone brokers, system servers, end-user/administrator terminals

– is executed by specification steps for: identifiers and general descriptions of components/subsystems/system (Step 1); spatial topology and structure interlinks of components/subsystems/system (Step 2); external action/function syntax (input parameters/arrays/structures, output/changeable variables/arrays/structures, output errors/exceptions/interruptions) of components/subsystems/system (for – turning on/off/increased/normal/decreased/pause/sleep/motion-detect, increase/decrease of the level, set/get active/waiting/sleeping time, set/get level, measurement, recording, execution, compilation, search, sort, select, priority, addressing, unicast/anycast/multicast/broadcast routing, fragmentation, integration, detailed/complete genesis, analysis and prognosis, accumulation, storage, graphic/video/audio/text presentation) (Step 3); format, top/low dimension and priority of data, program classes and packets (input/output/internal signals, parameters, flags, arrays and structures, invoked methods, special transmitted messages and packets in accordance with the selected protocols, graphic/video/audio/text files) for components/subsystems/system (Step 4); format, top/low dimension and priority of conditions/events for components/subsystems/system (Step 5); special necessary properties/characteristics (performance, capacity, bandwidth, function time/delay/priority/errors) for components/subsystems/system (Step 6); special expected or necessary properties/laws (choice/transport/queue/service laws) for special roles of components/subsystems/system into services/resources, clients/servers, queues/buffers (Step 7); own necessary redundant special characteristics (performance, capacity, bandwidth, function time/delay/priority/errors, sequential/parallel/loopback compositions) of selected or existing hosting environment for components/subsystems/system (Step 8).

Stage 2. Specification of static objects and properties for developed hosting environment for interactions through ports/interfaces of domain components/subsystems/system of SBC is similar to component and executed by specification steps for: identifiers and general descriptions of ports/interfaces (Step 1); spatial relations of affiliation of the ports/interfaces to components/subsystems/system (Step 2); external action/function syntax of the ports/interfaces (for – buffering, transmitting, sending, receiving, priority, fragmentation,

integration, packaging) (Step 3); format, top/low dimension and priority of possible transmitted data streams, program classes and packets (signals, parameters, flags, arrays, structures, invoked methods, special input/output messages and packets, graphic/video/audio/text files) for interactions (transmission/sending/receiving, in particular, with buffering) through ports/interfaces between developed components/subsystems (Step 4); format, top/low dimension and priority of conditions, events, communicative actions and functions (into external syntax) for interactions through ports/interfaces (Step 5); special necessary properties/characteristics (capacity, bandwidth, transmission time, delay, priority, transmission errors, packet switching type) of ports/interfaces (Step 6); special expected or necessary properties (choice/transport/queue/service laws) of ports/interfaces into special roles of transmitters/senders/receivers, queues/buffers (Step 7); own necessary redundant special characteristics (capacity and bandwidth, transmission time, delay, priority, transmission errors, packet switching type, basic sequential/parallel/loopback compositions) of selected or existing ports/interfaces (Step 8).

Stage 3. Specification of dynamic atomic objects and properties of interactions for developed hosting environment of the domain components/subsystems of SBC is executed by specification steps for: internal algorithms (temporal sequences/states/actions diagrams, automata, Petri nets, LTL-specifications) of functions/procedures/scenarios with complex temporal actions into own internal functioning and interactions into collaborative external functioning of components/subsystems/system and ports/interfaces (Step 1); atomic conditions, events, actions, priorities, including errors/exceptions/interruptions of functions/procedures/scenarios of these complex temporal actions and interactions (Step 2); atomic relations of logical time (quasi-order, equivalence, tolerance, incompatibility, uncertainty, indifference) and temporal operators of LTL-specifications (next, until, eventually, always) between atomic conditions, events, actions, in particular, errors/exceptions/interruptions and priorities (Step 3).

Stage 4. Specification of basic hierarchy for developed hosting environment of the domain components/subsystems of SBC is executed by specification steps for: three-level spatial hierarchy of endpoints/zones/area, where: first level of sensors/actuators/communication-panels and their controller into

containers of corresponding controlled end-point; second level of controlled end-points and zone control broker into containers of corresponding controlled zone; third level of controlled zones and their control server into containers of corresponding served area; third level of terminal zones and their control server into containers of corresponding served area (Step 1); three-level temporal hierarchy of events/actions/procedures/scenarios, where: first level of atomic conditions/events, actions/functions; second level of basic end-point transactional procedures of measurement/processing of the some level, turning on/off, increase/decrease of levels, increased/normal/reduced/sleeping start/stop, motion detection start/stop; third level of scenarios of general functioning of subsystems of SBC and their components (Step 2); three-level spatial hierarchy of conditions/events for first three-level spatial hierarchy of end-point/zones/area and second three-level temporal hierarchy of conditions/events/procedures/scenarios (Step 3); separation spatial/temporal ordered basic structures elements – bases/anti-bases, simple sequences, trees, hammocks, cycles into first and second hierarchies (Step 4).

Stage 5. Specification of actions/functions, as formal detailed internal procedures, algorithms and scenarios, for temporal interactions into processes of components/subsystems/system of projected SBC is executed by specification steps for: dynamic data flows of sequences/structures of detailed spatial/temporal data objects and their instant values with common transmissions by process actions/functions (Step 1); machines of states, in particular, Kripke's structures, of logical transformations of detailed spatial/temporal data objects and their instant values for process actions/functions (Step 2); automata and Petri nets with states/positions are contained conditions/events and arcs/transitions are contained actions/functions for process actions/functions (Step 3); diagrams sequences of temporal sequences of general transformations/transmission of general spatial/temporal data objects and their instant values, and also conditions/events and actions/functions (Step 4).

39.1.3 Modeling of entities, relations, functions, data, conditions, events, actions of interactions into flow process of SBC

Modeling of interactions and flow processes of developed environment of SBC [1, 2, 4, 7, 8, 9, 10, 11, 18, 24-28] represent dynamic, multidimensional, multi-flow models.

Formal definition of these dynamic, compositional, multidimensional and multi-flow models for environment of components, subsystems and SBC include next stages and steps for future analysis:

Stage 1. Modelling of dynamic objects, properties and relations of compositional, fifth-dimensional, network, hierarchical (multilevel – level-complicated OSI), relational model for system of all relations of logical time and temporal operators of LTL for conditions/events and actions/functions into interactions for developed hosting environment of the domain components/subsystems of SBC by execution of specification steps for: first dimension (axis) – full spatial network model of relations for spatial network interactions of all developed hosting environment (Step 1); second dimension (axis) – full spatial hierarchical model of relations for spatial hierarchical interactions of all developed hosting environment (Step 2); third dimension (axis) – full dynamic time model of relations for temporal flow into temporal network/hierarchical interactions of all developed hosting environment (Step 3); fourth dimension (axis) – full dynamic condition-event model of relations for conditions/events into temporal network/hierarchical/time interactions of all developed hosting environment (Step 4); fifth dimension (axis) – full dynamic action-function model of relations for actions/functions into temporal network/hierarchical/time interactions of all developed hosting environment (Step 5).

Stage 2. Definition of dynamic transport data/service/resource flow characteristics and classes for interactions and flow processes of developed environment of the domain components/subsystems/system of SBC, include ports/interfaces, by execution of specification steps for: identifiers and general descriptions, subject initiating scenarios for components/subsystems/system, (Step 1); scenario flow structures (including base/anti-base (input/output – external system nodes), internal nodes, linear (chains – paths), trees, hammocks, feedbacks,

general system entrances/exits) and their basic classes (linear, tree, hammock, feedback) (Step 2).

Stage 3. Modelling of dynamic objects, properties and processes of linear dynamic transport data/service/resource flow models for interactions and flow processes of developed environment of the domain components/subsystems/system of SBC, include ports/interfaces, by execution of specification steps for: sequences of atomic relations of logical time and temporal LTL-operators for conditions, events, actions, functions of component/subsystem/system and port/interface, activating into scenario for linear dynamic transport flows according to the dynamic fifth-dimensional relational model (Step 1); sequences of functions of component/subsystem/system (measurement, recording, buffering, primary analysis and prognosis, execution, compilation, priority, addressing, personal, group and broadcast routing, search, sort, integrate, fragmentation, complete analysis and prognosis, accumulation, forecast, graphic, video, audio, text presentation) and port/interface (buffering, transmitting, sending, receiving, priority, fragmentation, integration, packaging), activating respectively for some processing and transmitting/sending/receiving into scenario for linear dynamic transport flows (Step 2); sequences of data, program classes and packets (input/output/internal signals, parameters, flags, arrays, structures, invocated methods, special input/output messages and packets, including graphic, video, audio, text files), respectively using for component/subsystem/system and transmitting/sending/receiving through port/interface into scenario for linear dynamic transport flows (Step 3); sequences of special QS-characteristics (uniform and non-uniform; regular and irregular; recurrent and not recurrent; stationary, ordinary and extraordinary, continuity, discreteness, tension, capacity for – resource and services, service device, customer and supplier, queues and buffers) of component/subsystem/system and port/interface, activating into scenario for linear dynamic transport flows (Step 4).

Stage 4. Modelling of dynamic objects, properties and processes of treelike/hammock dynamic transport data/service/resource flow models for interactions and flow processes of developed environment of the domain components/subsystems/system of SBC, include ports/interfaces, by execution of specification steps for: trees/hammocks of sequences of atomic relations of logical time and

temporal LTL-operators for conditions, events, actions, functions of component/subsystem/system and port/interface, activating into scenario for treelike/hammock dynamic transport flows (in particular, for nodes of scenario flow structures), according to the dynamic fifth-dimensional relational model (Step 1); trees/hammocks of sequences of functions of component/subsystem/system and port/interface, activating respectively for some processing and transmitting/sending/receiving into scenario for treelike/hammock dynamic transport flows (in particular, for nodes of scenario flow structures) (Step 2); trees/hammocks of sequences of data, program classes and packets, respectively using for component/subsystem/system and transmitting/sending/receiving through port/interface into scenario for treelike/hammock dynamic transport flows (in particular, for nodes of scenario flow structures) (Step 3); trees/hammocks of sequences of special QS-characteristics of component/subsystem/system and port/interface, activating into scenario for treelike/hammock dynamic transport flows (in particular, for nodes of scenario flow structures) (Step 4).

39.2 Technologies of component interactions of Smart Building on a behavioral level

The following objects are taken as input:

1) The specifications of the technical description of the architecture of components/subsystems/system of Smart Building (SB), as well as such systems as a whole in analytic-text, tabular, graphical representations, defining the entities, relations, component structure and their topological relationships, system and component functions, information objects, interfaces of topological interactions (format, dimension, type, conditions of transmission over the topological connections of the objects to be sent – parameters, data, methods and their compositions, using wired and wireless technologies), the temporal behavior of functions and scenarios (time diagrams, graph, automaton, algorithmic representations).

2) The previously prepared Petri nets, which define some parts of the architecture of components/subsystems/system of SB, and also such systems, as a whole in analytic-text, tabular, graphical

representations, for which partial system-wide behavioral specification and modeling are defined, in particular, in CPN Tools environment.

The following objects are taken as output objects: the resulting full, optimized and correct Petri nets specifications, which represent full optimized behavioral architecture of components/subsystems/system of SB, as well as such systems in general, in analytic-text, tabular, graphical representations, for which in the corresponding instrumental environment, particular, CPN Tools, system behavioral evolutionary specification and modeling, with special results of fulfillment of special evolutionary entities/relations, properties/parameters, conditions/events, actions/functions, scenarios, are executed.

39.2.1 Specification of interactions into essentially static structure of Smart Building

Specification of interactions into essentially static structure of hosting environment for general architecture of Smart Building (SB) define static, slowly changing spatial objects, properties and processes of domain components/subsystems/system of SB, their structures and requirements [5, 7, 12, 13, 14].

Proposed formal definition of spatial/temporal (spatially/temporally distributed) interactions of processes for illumination subsystem of SB and their components is executed on base simple logical and temporal real time Petri nets by execution of specification for static spatial control-data/electric-power long-time slow illumination processes of day/night/day-off, week, month, year of building life cycle.

General specifications of slow interactions and processes into components, objects and functions for static hosting environment of illumination subsystem of SB and their components use behavioral of Petri net models and include next two preprocessing and four domain stages, and also next steps:

Stage 1. Preprocessing formal definition of main objects and their properties, subjects, subject services of illumination of SB by execution of specification steps for: Petri nets for representation of functioning of resource objects/subsystems – electrical power network (Step 1); properties/functions of positions/transitions of Petri nets for representation of general subject illumination properties/characteristics – total power of sources of light, intensity of illumination, spectrum,

number, location, power, intensity and spectrum of every specific sources of light, temporal laws (Step 2).

Stage 2. Preprocessing formal definition of own hosting spatial (spatially distributed) subject disposition of components/nodes of illumination of SB by execution of specification steps for: spatial composition of Petri Nets for representation of functioning of elements of building, their existing electric power and illumination subsystems – entrance-input/exit-output, corridors and subsystem lines/paths-chains, nodes – crossing/nodes of corridors and subsystem lines, trees, hammocks, feedbacks – substructures of internode reachability, general entrances and exits, stairs and between floor crossings (cross-level transitions) (Step 1); communicative positions/transitions of Petri nets from their spatial composition for representation of special properties/characteristics of service/resource static communication and transport structures of electric power and illumination subsystem of SB – structural multilevel model, entrances/exits, rooms and floors volume/space, length/width/capacity of corridors, stairs and entrances/exits, existing building electric power tension for rooms and floors, end-point environments (in particular, lamps) (Step 2); properties/predicates/functions of positions/transitions of Petri nets from their spatial composition for representation of extremum of electric-current/voltage for lamps/lines/communication-panels/nodes, used protocols and existing solutions for power supply (Step 3);.

Stage 3 Domain formal definition of static objects, properties and processes of developed hosting environment for illumination subsystem of SB and their components – end-points sensors/actuators, end-points controllers, controllers/brokers/routers/wireless-access-points, in future – zone brokers, system servers, user/admin terminals – by execution of specification steps for: identifiers and general descriptions Petri nets for components (Step 1); communicative positions/transitions of Petri nets from their spatial composition for representation of spatial topology/structure interlinks of components (Step 2); properties/predicates/functions of positions/transitions of Petri nets from spatial composition for representation of capacity and bandwidth, transmission time, delay, priority, transmission errors, packet switching type of components, used protocols and existing solutions for control (Step 3); external syntax of predicates/functions of positions/transitions of Petri nets from their spatial composition for representation of

external action/function syntax (input parameters/arrays/structures, output/changeable variables/arrays/structures, output errors/exceptions/interruptions) of components and subsystem for – measurement, recording, execution, compilation, search, sort, select, priority, addressing, unicast/anycast/multicast/broadcast routing, fragmentation, integration, partial/complete genesis, analysis and prognosis, accumulation, storage, graphic/video/audio/text presentation, interaction/dialog (Step 4); properties/predicates of positions/transitions of Petri nets from their spatial composition for representation of format, top/low dimension and priority of data, program classes and packets (input/output/internal signals, parameters, flags, arrays and structures, invoked methods, special messages and packets, graphic/video/audio/text files) of components and subsystem (Step 5);

Stage 4. Domain formal definition, distribution and placement of spatial/temporal conditions/events for illumination subsystem of SB and their components by execution of specification steps for properties/predicates of positions/transitions of Petri nets from their spatial/temporal composition for: end-point actuators/lamps – direct user/admin-panel or/and end-point-controller control signals, in particular, lower/higher, on/off, are received (Step 1); end-point sensors – low or high level of illumination, motion in control zone, direct user/admin control panel or/and end-point-controller control signal, in particular, on/off, start-measurement, stop-measurement, measurement sent, measurement ready, are received (Step 2); end-point controllers – direct user/admin-panel or/and broker control signal are received, start-time/finish-time of end-point-scenario activation, start-time/finish-time of pause/waiting/sleeping/timeout, buffer/memory overflow, end-point measurement/processing completed, direct user/admin or/and zone broker control signal are received, measurement/processing-packet sent, measurement/processing-packet ready (Step 3); zone brokers – direct user/admin or/and server control-signal are received, start-time/finish-time of zone-scenario activation, start-time/finish-time of zone pause/waiting/sleeping/timeout, zone buffer/memory overflow, zone-measurement/processing completed, zone-measurement/processing-packet ready (Step 4); system servers – direct user/admin control-signal are received, start-time/finish-time of system-scenario activation, start-time/finish-time of system pause/waiting/sleeping/timeout, system buffer/memory overflow,

system-measurement/processing completed, system-measurement/processing-packet ready (Step 5); user/admin-panels – server control-signal are received, start-time/finish-time of panel-scenario activation, start-time/finish-time of panel pause/waiting/sleeping/timeout, panel buffer/memory overflow, panel-processing completed, panel-processing-packet ready, panel-processing-packet sent (Step 6); mutual relations of shared of conditions/events between components of illumination subsystem of SB (Step 7).

Stage 5. Domain formal definition of relations of interaction for spatial/temporal conditions/events of single-level and components of developed multi-level illumination subsystem of projected SB by execution of specification steps for relations between properties/predicates of positions/transitions of Petri nets from their spatial/temporal single-level composition for: horizontal single-level-1 – between end-point sensors (photosensors and motion sensors), end-point actuators (lamps), end-point auto-/semiauto-controlled electro power communication panels from local controlled point (Step 1); vertical two-level-1-2 – between end-point sensors/actuators, end-point auto-/semiauto-controlled-electro-power-communication-panels and their end-point controllers from local controlled point (Step 2); horizontal single-level-2 – between end-point controllers from zone, controlled by broker (Step 3); vertical two-level-2-3 – between end-point controllers of and zone smart control broker from zone, controlled by broker (Step 4); horizontal single-level-3 – between zone smart control brokers from space, monitoring by server (Step 5); vertical two-level-3-4 – between zone smart control brokers and server from space, monitoring by server (Step 6); horizontal single-level-4 – between servers (if there are several) (Step 7); vertical four-level-1-2-3-4 – between sensors/actuators, end-point controllers, zone brokers, servers and user/admin terminals (Step 8).

Stage 6. Domain formal definition, distribution and placement external syntax of spatial/temporal actions/functions/scenarios for illumination subsystem of SB and their components by execution of specification steps for predicates/functions of positions/transitions of Petri nets from their spatial/temporal composition for: end-point actuators/lamps – direct user/admin-panel or/and end-point-controller control signals, in particular, lower/higher, on/off, receive (Step 1);

end-point sensors – low or high level of illumination, motion in control zone, direct user/admin control panel or/and end-point-controller control signal, in particular, on/off, start-measurement, stop-measurement, measurement sent, measurement ready, receive (Step 2); end-point controllers – direct user/admin-panel or/and broker control signal receive, start-time/finish-time of end-point-scenario activate, start/finish of pause/waiting/sleeping/timeout, buffer/memory overflow processing, end-point measurement/processing, direct user/admin or/and zone broker control signal receive, measurement/processing-packet send, measurement/processing-packet create (Step 3); zone brokers – direct user/admin or/and server control-signal receive, start/finish of zone-scenario activate, start/finish of zone pause/waiting/sleeping/timeout, zone buffer/memory overflow processing, zone-measurement/processing, zone-measurement/processing-packet create (Step 4); system servers – direct user/admin control-signal receive, start/finish of system-scenario activate, start/finish of system pause/waiting/sleeping/timeout, system buffer/memory overflow processing, system-measurement/processing, system-measurement/processing-packet send (Step 5); user/admin-panels – server control-signal receive, start/finish of panel-scenario activate, start/finish of panel pause/waiting/sleeping/timeout, panel buffer/memory overflow processing, panel-processing, panel-processing-packet send (Step 6); mutual relations of shared of actions/functions between components of illumination subsystem of SB (Step 7).

39.2.2 Modelling of interactions into distributed dynamic flow process of functioning of Smart Building

Specification of interactions into essentially temporal structure of dynamic, rapidly changing distributed flows for dynamic process of Smart Building (SB) with hybrid communications define dynamic temporal objects, properties, processes and flows of domain components/subsystems/system of SB, their structures and requirements [5, 7, 12, 13, 14].

Proposed formal definition of spatial/temporal flows for illumination of SB and their components is executed on base simple logical and temporal real time Petri nets by execution of specification for dynamic temporal (temporally distributed) models of control-

data/electric-power data flows of the subsystem of illumination for short-time quick illumination of time intervals for subject processes.

Evolutionary specifications of interactions for, rapidly changing distributed flows of dynamic processes into components, objects and functions for illumination subsystem of SB and their components use behavioral of Petri net models and include stages and steps:

Stage 1. Domain formal definition of ascending interceptions and processing of conditions/events by actions/functions/scenarios for illumination subsystem of the projected SB and their components in accordance with relation models for conditions/events/actions/functions by execution of specification steps for relations between properties/predicates/functions of positions/transitions of Petri nets from their multilevel composition for: low-level-1-2 interception of conditions/events of sensors/actuators/electro-power-communication-panels from local controlled end-points for subsequent processing by corresponding end-point controllers (Step 1); low-level-2 processing for interceptional conditions/events of sensors/actuators/electro-power-communication-panels from local controlled end-points by corresponding end-point controllers (Step 2); middle-level-2-3 interception of conditions/events of end-point controllers from controlled zones for subsequent processing by corresponding zone brokers (Step 3); middle-level-3 processing for interceptional conditions/events of end-point controllers from controlled zones by corresponding brokers (Step 4); high-level-3-4 interception of conditions/events of zone control brokers from sets of controlled zones – served areas for subsequent processing by corresponding area servers (Step 5); high-level-4 processing for interceptional conditions/events of zone control brokers from sets of controlled zones – served areas by corresponding area servers (Step 6); intro-middle-level-3-3 interception of conditions/events of user/admin terminals from terminal zones for subsequent processing by corresponding brokers (Step 7); intro-middle-level-3 processing for interceptional conditions/events of user/admin terminals from terminal zones by corresponding control brokers (Step 8); high-level processing for interceptional conditions/events of user/admin terminals from sets of terminal zones – served areas by corresponding area servers (Step 9).

Stage 2. Domain formal definition of spatial/temporal relations of interactions for conditions/events/actions/functions/scenarios of

illumination subsystem of SB and their components by execution of specification steps for properties, communicative positions/transitions and relations between properties/predicates/functions from positions/transitions of Petri nets from their spatial/temporal composition for: feathers of relation type depending from type of spatial/temporal interactions (synchronous/asynchronous, eventfulness, sequential/parallel/loopback, immediate/with-delay, deterministic/non-deterministic, resolving/inhibiting) (Step 1); select and exchange of relation type (dependence, association, connection, interaction, expansion, generalization, inclusion, implementation, aggregation, composition) during day/night/day-off, week, month, year, full subsystem life cycle (Step 2); relations of logical time from conditions to events (Step 3); relations of logical time from actions to functions (Step 4); relations of logical time from events to actions (Step 5).

Stage 3. Modelling of dynamic objects, properties and relations of compositional, fifth-dimensional, network, hierarchical, relational model for system of all relations of logical time for conditions/events and actions/functions/scenarios into interactions for developed environment of illumination subsystem of SB and their components by execution of specification steps for relations between properties/predicates/functions of positions/transitions of Petri nets from their spatial/temporal multilevel composition for: first dimension (axis) – full spatial network model of relations for spatial network interactions (Step 1); second dimension (axis) – full spatial hierarchical model of relations for spatial hierarchical interactions (Step 2); third dimension (axis) – full dynamic time model of relations for temporal changes and flow into temporal network/hierarchical interactions (Step 3); fourth dimension (axis) – full dynamic condition-event model of relations for conditions/events into temporal network/hierarchical/time interactions (Step 4); fifth dimension (axis) – full dynamic action-function model of relations for actions/functions/scenarios into temporal network/hierarchical/time interactions (Step 5).

Stage 4. Definition of dynamic flow characteristics and classes for interactions and flow processes of developed environment for the illumination subsystem of SB, their components and ports/interfaces by execution of specification steps for special dynamic Petri nets from their spatial/temporal flow composition for: identifiers and general descriptions for subject initiating scenarios (Step 1); scenario flow

topological structures (including base/anti-base (input/output – external system nodes), internal nodes, linear (chains – paths), trees, hammocks, feedbacks, general system entrances/exits) and their basic classes (linear, tree, hammock, feedback) (Step 2).

Stage 5. Modelling of dynamic objects, properties and processes of linear dynamic flow models for interactions and flow processes of developed environment of illumination subsystem of SB, their components and ports/interfaces by execution of specification steps for properties/predicates of positions/transitions of dynamic Petri nets from their spatial/temporal linear-flow composition for: sequences of atomic relations of logical time for conditions, events, actions, functions, activating linear dynamic transport flows into scenario, according to the dynamic fifth-dimensional relational model (Step 1); sequences of functions of components (measurement, recording, buffering, primary analysis and prognosis, execution, compilation, priority, addressing, personal, group and broadcast routing, search, sort, integrate, fragmentation, complete analysis and prognosis, accumulation, forecast, graphic, video, audio, text presentation) and port/interface (buffering, transmitting, sending, receiving, priority, fragmentation, integration, packaging), activating into linear dynamic transport flows of scenario respectively for some processing and transmitting/sending/receiving (Step 2); sequences of data, program classes and packets (input/output/internal signals, parameters, flags, arrays, structures, invoked methods, special input/output messages and packets, including graphic, video, audio, text files) into linear dynamic transport flows of scenario, using for processing and transmitting/sending/receiving respectively through components and port/interface respectively (Step 3); sequences of special statistical QS-characteristics (uniform and non-uniform; regular and irregular; recurrent and not recurrent; stationary, ordinary and extraordinary, continuity, discreteness, tension, capacity for – resource and services, service device, customer and supplier, queues and buffers) of components and ports/interfaces, activating into linear dynamic transport flows of scenario (Step 4).

Stage 6. Modelling of dynamic objects, properties and processes of treelike/hammock dynamic flow models for interactions and flow processes of developed environment of the illumination subsystem of SB, components and ports/interfaces by execution of specification steps

for properties/predicates of positions/transitions of dynamic Petri nets from their spatial/temporal treelike/hammock-flow composition for: trees/hammocks of sequences of atomic relations of logical time for conditions, events, actions, functions, activating into treelike/hammock dynamic transport flows of scenario (in particular, for nodes of scenario flow structures), according to the dynamic fifth-dimensional relational model (Step 1); trees/hammocks of sequences of functions of components and port/interface, activating into treelike/hammock dynamic transport flows of scenario (in particular, for nodes of scenario flow structures) respectively for some processing and transmitting/sending/receiving (Step 2); trees/hammocks of sequences of data, program classes and packets into treelike/hammock dynamic transport flows of scenario (in particular, for nodes of scenario flow structures), using for processing and transmitting/sending/receiving respectively through components and port/interface (Step 3); trees/hammocks of sequences of special statistical QS-characteristics of components and ports/interfaces, activating into treelike/hammock dynamic transport flows of scenario (in particular, for nodes of scenario flow structures) (Step 4).

39.3 Technologies of component interactions of Smart City at the level of process synchronization

The following objects are taken as input:

1) The specifications of the technical description of the architecture of components, subsystems of Smart City (SC), as well as such systems as a whole in analytic-text, tabular, graphical representations, defining the entities, relations, component structure and their topological relationships, system and component functions, information objects, interfaces of topological interactions (format, dimension, type, conditions of transmission over the topological connections of the objects to be sent – parameters, data, methods and their compositions, using wireless technologies), the temporal behavior of functions and scenarios (time diagrams, graph, automaton, algorithmic representations).

2) The previously prepared LTL-specifications, which define some parts of the architecture of components, subsystems of SC, and also such systems, as a whole in analytic-text, tabular, graphical representations, for which partial system-wide interactive-visual

specification and modeling are defined, in particular, in SPIN tools environment.

The following objects are taken as output objects: the resulting full, correct LTL-specifications, which represent the full dynamic optimized temporal architecture of components/subsystems/system of SC, as well as such systems in general, in analytic-text, tabular, graphical representations, for which in the corresponding instrumental environment, particular, SPIN, system temporal multiagent specification and modeling with special results of entities/relations, properties/parameters, conditions/events, actions/functions, scenarios, are executed.

39.3.1 Specification of interactions into essentially dynamical structure of Smart City

Specification of interactions into essentially dynamic properties/characteristics and structure of hosting environment for general architecture of Smart City (SC) define static, slowly changing spatial objects, properties and processes from subsystems of SC, in particular, auto/electro transport subsystem, in future – transport subsystem, their stationary components, structures and requirements [6, 15, 16, 17, 19-23].

Formal definition of spatial/temporal (spatially/temporally distributed) transport subsystem of SC and their components, using Linear Temporal Logic (LTL) expression/equation generate specifications of static spatial/temporal LTL-structures for long-time, slow transport infrastructure (road lanes/junctions/intersections, traffic signs/lights/rules-laws) processes, during the day/night/day-off, week, month, year, subsystem-life-cycle.

General specification of static atomic objects and properties of interactions for developed hosting environment of the auto/electro transport subsystem of SC and their components is proposed by specification third general stages for: atomic conditions, events, actions, including interruptions/exceptions/errors, into complex temporal interactions (Stage 1); atomic temporal LTL-operators (next, until, eventually, always) of LTL-expression between atomic conditions/events and actions/functions (Stage 2); internal spatial/temporal dependencies into spatial/temporal sequences/structures/machine-of-states of changes of conditions/events

and execution of actions/functions/scenarios, that are defined by Kripke-structures/Buchi-automata of temporal LTL-expressions/ /equations for complex temporal collaborative functioning with their processes and interactions into transport subsystem and their components (Stage 3).

Specifications of slow interactions and processes into components, objects and functions for hosting infrastructure environment of transport subsystem of SC use LTL-expression and include next stages and steps:

Stage 1. Preprocessing formal definition of main objects and their properties, subjects, subject services of transport subsystem of SC by execution of specification steps for: identifiers of roads-(sets-of-lanes)/lanes/junctions/intersections/levels/ of road network, traffic signs/lights/rules-laws for this network (Step 1); general properties/characteristics of traffic – roads/lanes/junctions/ /intersections/dead/parking length/capacity/traffic-direction, number, topological adjacency (Step 2).

Stage 2. Preprocessing formal definition of spatial (spatially distributed) subject disposition of components of transport subsystem of SC by execution of specification steps for: spatial multilevel models and their elements of road network, their existing transport subsystems – external entrance-input/exit-output, dead/parking, lanes/roads and, node – junction/intersection of lanes/roads and cross-level transitions of levels, trees, hammocks, feedbacks – substructures of internode reachability, lane/road/node/dead/parking levels and interlevel crossings (cross-level transitions) (Step 1); special properties/characteristics for static structures of transport subsystem of SC and their entrance/exit/dead/parking/lane/road/junction/ /intersection/level/cross-level-transitions – topological ordered adjacency and general spatial topological multilevel model, length/capacity/traffic-direction/maximum-traffic-speed/priority, (Step 2); extremum of length/capacity/traffic-direction/maximum-traffic-speed/priority for entrance/exit/dead/parking/lane/road/junction/ /intersection/level/cross-level-transitions (Step 3); placement (into spatial model) and distribution (between components) traffic signs/lights/rules-laws-solutions (Step 4).

Stage 3 Domain formal definition of static objects, properties and processes of developed environment for transport subsystem of SC and

their components – end-points sensors-camera/actuators-traffic-lights, end-points controllers, zone (for the whole component) controllers/monitors/brokers/routers/wireless-access-points, in future – zone brokers, system servers, user/admin terminals – by execution of specification steps for: identifiers and general descriptions of components (Step 1); spatial topology/structure interlinks of components (Step 2); capacity and bandwidth, transmission time, delay, priority, transmission errors, packet switching type of components (including transport units as special protocol packets), used protocols and existing solutions for control (Step 3); external action/function syntax (input parameters/arrays/structures, output/changeable variables/arrays/structures, output errors/exceptions/interruptions) of components and subsystem for – measurement, recording, execution, compilation, search, sort, select, priority, addressing, unicast/anycast/multicast/broadcast routing, fragmentation, integration, partial/complete genesis, analysis and prognosis, accumulation, storage, graphic/video/audio/text presentation, interaction/dialog (Step 4); format, top/low dimension and priority of data, program classes and packets, including transport units as special protocol packets, (input/output/internal signals, parameters, flags, arrays and structures, invoked methods, special messages and packets, graphic/video/audio/text files) of components and transport subsystem (Step 5);

Stage 4. Domain formal definition, distribution and placement of spatial/temporal (spatially/temporally distributed) conditions/events for transport subsystem of SC and their components by execution of specification steps for: end-point sensors-camera/actuators-traffic-lights – control signals from direct user/admin-terminal or/and end-point-controller, in particular, lower/higher, on/off, are received (Step 1); end-point sensors – low or high rate of observation, slow/normal/quick motion in control point, direct user/admin control terminal or/and end-point-controller control signal, in particular, on/off, start-observation, stop-observation, observation sent, observation ready, are received (Step 2); end-point controllers – direct user/admin-terminal or/and broker control signal are received, start-time/finish-time of end-point-scenario activation, start-time/finish-time of pause/waiting/sleeping/ /timeout, buffer/memory overflow, end-point observation/processing completed, direct user/admin or/and zone broker control signal are

received, observation/processing-packet sent, observation/processing-packet ready (Step 3); zone brokers – direct user/admin or/and server control-signal are received, start-time/finish-time of zone-scenario activation, start-time/finish-time of zone pause/waiting/sleeping/timeout, zone buffer/memory overflow, zone-observation/processing completed, zone-observation/processing-packet ready (Step 4); system servers – direct user/admin control-signal are received, start-time/finish-time of system-scenario activation, start-time/finish-time of system pause/waiting/sleeping/timeout, system buffer/memory overflow, system-observation/processing completed, system-observation/processing-packet ready (Step 5); user/admin-terminals – server control-signal are received, start-time/finish-time of terminal-scenario activation, start-time/finish-time of terminal pause/waiting/sleeping/timeout, terminal buffer/memory overflow, terminal-processing completed, terminal-processing-packet ready (Step 6); mutual relations as LTL-operators/expressions/conclusions/proofs for shared of conditions/events between components of transport subsystem of SC (Step 7).

Stage 5. Domain formal definition of relations as LTL-operators/expressions/conclusions/proofs for interaction for spatial/temporal conditions/events of single-level and components of developed multi-level transport subsystem of SC by execution of specification steps for: horizontal single-level-1 – between end-point sensors (camera and motion sensors), end-point actuators (traffic-lights), end-point auto-/semiauto-controlled communication panels from local controlled point (Step 1); vertical two-level-1-2 – between end-point sensors/actuators, end-point auto-/semiauto-controlled-communication-panels and their end-point controller from this local controlled point (Step 2); horizontal single-level-2 – between end-point controllers from zone, controlled by some broker (Step 3); vertical two-level-2-3 – between end-point controllers of and zone control broker from zone, controlled by this broker (Step 4); horizontal single-level-3 – between zone control brokers from space, monitoring by some server (Step 5); vertical two-level-3-4 – between zone control brokers and server from space, monitoring by this server (Step 6); horizontal single-level-4 – between servers (if there are several) (Step 7); vertical four-level-1-2-3-4 – between sensors/actuators, end-point controllers, zone brokers, servers and user/admin terminals (Step 8).

Stage 6. Domain formal definition, distribution and placement external syntax of spatial/temporal actions/functions/scenarios for transport subsystem of SC and their components by execution of specification steps for: end-point actuators-traffic-lights – direct user/admin-panel or/and end-point-controller control signals receive, in particular, red/yellow/green, on/off, timer, receive data (Step 1); end-point sensors-camera – low/normal/high level of observation, motion in control zone, direct user/admin control terminal or/and end-point-controller control signal receive, in particular, on/off, observation, observation-sent, send/receive data (Step 2); end-point controllers – direct user/admin-terminal or/and zone-broker control signal receive, start-time/finish-time of end-point-scenario activate, start/finish of pause/waiting/sleeping/timeout, buffer/memory overflow processing, end-point observation/processing, direct user/admin or/and zone broker control signal receive, observation/processing-packet send, observation/processing-packet create (Step 3); zone brokers – direct user/admin or/and server control-signal receive, start/finish of zone-scenario activate, start/finish of zone pause/waiting/sleeping/timeout, zone buffer/memory overflow processing, zone-observation/processing, zone-observation/processing-packet create (Step 4); system servers – direct user/admin control-signal receive, start/finish of system-scenario activate, start/finish of system pause/waiting/sleeping/timeout, system buffer/memory overflow processing, system-observation/processing, system-observation/processing-packet send (Step 5); user/admin-terminals – server control-signal receive, start/finish of terminal-scenario activate, start/finish of terminal pause/waiting/sleeping/timeout, terminal buffer/memory overflow processing, terminal-processing, terminal-processing-packet send (Step 6); mutual relations as LTL-operators/expressions/conclusions/proofs for shared of actions/functions between components of transport subsystem of SC (Step 7).

39.3.2 Modelling of interactions into distributed dynamic flow process of synchronization of Smart City

Specification of interactions into essentially temporal structure of dynamic, rapidly changing distributed flows for dynamic process of Smart City (SC) with essentially wireless communications define dynamic temporal objects (including transport units as special protocol

packets), properties, processes and flows of transport subsystem of SC, their components, structures and requirements [6, 15, 16, 17, 19-23, 29].

Domain formal definition of spatial/temporal flows for transport subsystem of SC and their components on base LTL-operators/expressions/conclusion/proofs by execution of specification for dynamic temporal (temporally distributed) models of flows of the transport subsystem for short-time quick tyraffic of time intervals for subject processes.

Specifications of interactions for rapidly changing distributed flows of dynamic processes into components, objects and functions for transport subsystem of SC, using system of LTL-operators/expressions/conclusion/proofs, define temporal requirements for components and transport subsystem of SC.

Stage 1. Formal definition of ascending interceptions and processing of conditions/events by actions/functions/scenarios of the projected transport subsystem of SC and their components in accordance with relations as subsystem of LTL-operators/expressions/conclusion/proofs for conditions/events/actions/functions by execution of specification steps for: low-level-1-2 interception of conditions/events of sensors/actuators/communication-panels from local controlled end-points for subsequent processing by corresponding end-point controllers (Step 1); low-level-2 processing for interceptional conditions/events of sensors/actuators/communication-panels from local controlled end-points by corresponding actions/functions/scenarios of end-point controllers (Step 2); middle-level-2-3 interception of conditions/events of end-point controllers from controlled zones for subsequent processing by corresponding zone brokers (Step 3); middle-level-3 processing for interceptional conditions/events of end-point controllers from controlled zones by corresponding actions/functions/scenarios of brokers (Step 4); high-level-3-4 interception of conditions/events of zone control brokers from sets of controlled zones – served areas for subsequent processing by corresponding area servers (Step 5); high-level-4 processing for interceptional conditions/events of zone control brokers from sets of controlled zones – served areas by corresponding actions/functions/scenarios of area servers (Step 6); intro-middle-level-3-3 interception of conditions/events of user/admin terminals from terminal zones for

subsequent processing by corresponding brokers (Step 7); intro-middle-level-3 processing for interceptional conditions/events of user/admin terminals from terminal zones by corresponding actions/functions/scenarios of control brokers (Step 8); high-level processing for interceptional conditions/events of user/admin terminals from sets of terminal zones – served areas by corresponding actions/functions/scenarios of area servers (Step 9).

Stage 2. Domain formal definition of spatial/temporal relations as system of LTL-operators/expressions/conclusion/proofs of interactions for conditions/events/actions/functions/scenarios of transport subsystem of SC and their components by execution of specification steps for: feathers of relation type depending from type of spatial/temporal interactions (synchronous/asynchronous, eventfulness, sequential/parallel/loopback, immediate/with-delay, deterministic/non-deterministic, resolving/inhibiting) (Step 1); select and exchange of relation type (dependence, association, connection, interaction, expansion, generalization, inclusion, implementation, aggregation, composition) during day/night/day-off, week, month, year, full subsystem life cycle (Step 2); relations as subsystem of LTL-operators/expressions/conclusion/proofs from conditions to events (Step 3); relations as system of LTL-operators/expressions/conclusion/proofs from actions to functions (Step 4); relations as system of LTL-operators/expressions/conclusion/proofs from events to actions (Step 5).

Stage 3. Modelling of dynamic objects, properties and relations of compositional, fifth-dimensional, network, hierarchical, relational model for system of all relations as system of LTL-operators/expressions/conclusion/proofs for conditions/events and actions/functions/scenarios into interactions for developed environment of transport subsystem of SC and their components by execution of specification steps for: first dimension (axis) – full spatial network model of relations for spatial network interactions (Step 1); second dimension (axis) – full spatial hierarchical model of relations for spatial hierarchical interactions (Step 2); third dimension (axis) – full dynamic time model of relations system of LTL-operators/expressions/conclusion/proofs for temporal changes and flows into temporal network/hierarchical interactions (Step 3); fourth dimension (axis) – full dynamic condition/event model of relations as subsystem of LTL-

operators/expressions/conclusion/proofs for conditions/events into temporal network/hierarchical/time interactions (Step 4); fifth dimension (axis) – full dynamic action/function/scenarios model of relations as subsystem of LTL-operators/expressions/conclusion/proofs for actions/functions/scenarios into temporal network/hierarchical/time interactions (Step 5).

Stage 4. Definition of dynamic transport flow characteristics and classes for interactions and flow processes of developed environment for transport subsystem of SC, their components and ports/interfaces by execution of specification steps for: identifiers and general descriptions for subject initiating scenarios (Step 1); scenario flow topological structures (including base-input/anti-base-output (external system nodes of transport subsystem), internal nodes (junctions, intersections, cross-level-transitions), linear (chains – lanes, roads), substructures (trees, hammocks, feedbacks, levels), sets of basic classes (linear, tree, hammock, feedback) (Step 2).

Stage 5. Modelling of dynamic objects, properties and processes of linear dynamic flow models for interactions and flow processes of developed environment of transport subsystem of SC, their components and ports/interfaces by execution of specification steps for: sequences of atomic relations as system of LTL-operators/expressions/conclusion/proofs for conditions, events, actions, functions, activating linear dynamic transport flows into scenario, according to the dynamic fifth-dimensional relational model (Step 1); sequences of functions of components (observation, recording, buffering, primary genesis/analysis/prognosis, execution, compilation, priority, addressing, personal, group and broadcast routing, search, sort, integrate, fragmentation, complete genesis/analysis/prognosis, accumulation, forecast, graphic, video, audio, text presentation) and port/interface (buffering, transmitting, sending, receiving, priority, fragmentation, integration, packaging), activating into linear dynamic transport flows of scenario respectively for some processing and transmitting/sending/receiving (Step 2); sequences of data, program classes and packets/transport-units (input/output/internal signals, parameters, flags, arrays, structures, invoked methods, special input/output messages and packets/transport-units, including graphic, video, audio, text files) into linear dynamic transport flows of scenario, using for processing and transmitting/sending/receiving respectively

through components and port/interface (Step 3); sequences of special statistical QS-characteristics (uniform and non-uniform; regular and irregular; recurrent and not recurrent; stationary, ordinary and extraordinary, continuity, discreteness, tension, capacity for – resource and services, service device, customer and supplier, queues and buffers) of components and ports/interfaces, activating into linear dynamic transport flows of scenario (in particular, for nodes of scenario flow structures) (Step 4).

Stage 6. Modelling of dynamic objects, properties and processes of treelike/hammock dynamic flow models for interactions and flow processes of developed environment of transport subsystem of SC, components and ports/interfaces by execution of specification steps for: trees/hammocks of sequences of atomic relations as system of LTL-operators/expressions/conclusion/proofs for conditions, events, actions, functions, activating into treelike/hammock dynamic transport flows of scenario (in particular, for nodes of scenario flow structures), according to the dynamic fifth-dimensional relational model (Step 1); trees/hammocks of sequences of actions/functions of components and port/interface, activating into treelike/hammock dynamic transport flows of scenario (in particular, for nodes of scenario flow structures) respectively for some processing and transmitting/sending/receiving of scenario (Step 2); trees/hammocks of sequences of data, program classes and packets/transport-units into treelike/hammock dynamic transport flows of scenario (in particular, for nodes of scenario flow structures), using for processing and transmitting/sending/receiving respectively through components and port/interface (Step 3); trees/hammocks of sequences of special statistical QS-characteristics of components and ports/interfaces, activating into treelike/hammock dynamic transport flows of scenario (in particular, for nodes of scenario flow structures) (Step 4).

39.4 Work related analysis

The organization of interaction of components in IoT and IoE the systems of the smart building and smart city begins at a stage of coordination of the specifications in processes of their verification and modeling with the use of techniques and tools of representation of a system and its components at the structural level. Star UML, MS Visual.NET can be carried to such techniques and tools [1, 7, 9, 11].

The following step is representation of interactions in IoT and IoE systems at the behavioural level with the use of techniques and tools of the description of scenarios, cases and processes of interactive functioning of components of the smart building and smart city, including techniques, technologies and tools: the ExtendSim Demo modeling environment, the GPSS World graphic interface, the OMNet simulator – modular library of modeling, QS-models, Time Petri Net Analyzer and CPN Tools [19-22].

G. Marques and R. Pitarma from Coimbra University Portugal presented a laboratory environment conditions supervision solution based on IoT architecture called iLabM+. The solution is composed of prototype hardware for the collection of the data environment and a Web portal for data consulting and analysis. This system allows monitoring of temperature, relative humidity, barometric pressure and air quality [31].

Issues of temporary synchronization of scenarios, cases and processes of interaction of components in IoT and IoE the systems of the smart building and smart city are solved with the use of technologies, techniques and tools of temporal logic, including the following means of representation and verification of interaction of the components regarding their synchronization: Promela language, SPIN and XSPIN tool environments [26-30].

With the expansion of smart meters, like the Advanced Metering Infrastructure (AMI), and the Internet of Things (IoT), Each smart city is equipped with various kinds of electronic devices including expansion of smart meters, like the Advanced Metering Infrastructure, and the IoT systems. Therefore, equipment and technologies enable us to be smarter and make various aspects of smart cities more accessible and applicable. An inclusive review on the concept of the smart city besides their different applications, benefits, and advantages is suggested. Most of the possible IoT technologies are introduced, and their capabilities to merge into and apply to the different parts of smart cities are discussed. The potential application of smart cities with respect to technology development in the future provides another valuable discussion. Meanwhile, some practical experiences all across the world and the key barriers to its implementation are thoroughly expressed [6].

Current issues on research and development in the area of Petri nets and modeling of concurrent systems represented at the 28th

International Conference on Applications and Theory of Petri Nets and Other Models of Concurrency, ICATPN 2007 are addressed, in particular system design and verification, analysis, synthesis, structure and behavior of nets, net theory and relations, causality/partial order theory of concurrency, semantic Web, logical and algebraic calculi, symbolic net representation, tools for nets, experience reports and case studies, educational issues, higher-level net models, timed and stochastic nets, as well as standardization of nets [19].

Networked healthcare devices which closely intertwined in the structure of the Internet of Things offer many opportunities for monitoring patients, tracking their location and condition, obtaining, analyzing, and sharing patient health data. The models of healthcare IoT system based on the queueing theory describe streams of the requests and attacks on vulnerabilities and procedure of recovery by restart and eliminating of one and/or two vulnerabilities. In addition, using the submitted models, it is possible to calculate an availability function [21].

SPIN is the world's most popular and powerful, tools for detecting software defects in concurrent system designs. The tool has been applied to everything from the verification of complex call processing software that is used in telephone exchanges, to the validation of intricate control software for interplanetary spacecraft. The tool 's specification language and theoretical foundation, and gives detailed advice on methods for tackling the most complex software verification problems, design and detailed verification models of complex systems software, the SPIN command line interface, the Xspin graphical user interface, and the TimeLine editing tool, the basic theory of omega automata, linear temporal logic, depth-first and breadth-first search, search optimization, and model extraction from source code are considered [28, 29].

Ah-Lian Kor, M. Yanovsky, C. Pattinson and V. Kharchenko suggested to harness the emerging IoT technology to empower elderly population to self-manage their own health, stay active, healthy, and independent as long as possible within a smart and secured living environment. The SMART-ITEM system and services will appropriately address the smart health and care; smart quality of life and SMART-ITEM social community [32].

Real-time public transport information service infrastructure as a part of the core functionality of intelligent transport systems important in the solutions of problems of the smart city is based on the developing a

framework for real-time data acquisition and choosing an efficient model for trolleybus arrival time prediction that can be easily implemented to improve public transport services by leveraging on the GPS data and data provided by the IoT applications. An architecture model of information service infrastructure for public passenger transport was developed. As a use case of the proposed approach, eight methods combining historical average, Kalman filtering technique and Google Maps API for trolleybus arrival time prediction were implemented and tested. An assessment of models performance and their effectiveness with real-time data are investigated. The results show that combinations of average travel speed (ATS) and distance from Google Maps API and ATS and distance from Google Maps API with Kalman filtering gave the best arrival time predictions for low-speed urban transport [30].

Conclusions and questions

Specification, modeling and simulation of internal interactions are an essential part of the synthesis, analysis and verification of Smart Building and City systems (SBC), and assume a formal study of the process models and the flows of functioning of SBC components with regard to their structural, functional, data and interface features.

In the first section, the technologies of SBC-based asynchronous-event interactions, that based on the use of UML, are considered, including the processes of static hardware-software systems of the SBC, as well as data and signal flows for the dynamic processes of subsystems of the SBC.

The section presents the specifications of the architectural properties of the predefined components and structures of SBC, the basic requirements for them, defines the specifications of their entities, relations, functions, data, conditions, events, actions during interactions in SBC. Also in the section, special models of entities, relations, functions, data, conditions, events, actions in data and signal flows for processes of SBC are considered.

In the second section, technologies of behavioral component interactions of Smart Building systems, that based on the use of Petri nets, are considered. The section presents behavioral specifications of entities, relationships, functions, data, conditions, events, actions during interactions in the essentially static structure of the Smart Building, as well as behavioral models of distributed dynamic flows in the processes of functioning of Smart Building systems.

In the third section, technologies of temporal component interactions of Smart City systems, that based on the use of Linear Temporal Logic (LTL), are considered. The section presents temporary specifications of entities, relationships, functions, data, conditions, events, actions during interactions in the essentially dynamic structure of the Smart City, as well as temporal analytical models of distributed dynamic flows in the synchronization processes of Smart City systems.

1. What are the components of the overall SBC computer system architecture, that are specified?

2. What can be specified in SBC systems, using UML, QS, Petri Nets, LTL?

3. What are the features of sensors, actuators, end-point controllers, zones, brokers, servers, user and administrator terminals, that are used in SBC systems?

4. What are the basic topological structures, that are used in the analysis of SBC systems?

5. How to represent temporary processes, sequential and parallel algorithms for the functioning of SBC components?

6. What is the difference between conditions, events, actions and functions in the dynamics of interactions in the behavior of SBC components?

7. How the static hosting system of components and subsystems SBC is defined?

8. What are the features of the components and subsystems of the static system SBC?

9. How the dynamic process system of components and subsystems SBC is defined?

10. What are the objects, properties, processes SBC, that can be attributed to the dynamic?

11. How is the five-dimensional relational model of logical time relations for dynamic objects and properties is determined in the interaction of SBC components and subsystems?

12. What are the features of linear and network flow models for the processes of interaction of components and subsystems of SBC?

13. What are the features of SB and SC components and subsystems, in particular, illumination and transport subsystems?

14. How is the dynamic model of the illumination subsystem SB defined, what do Petri nets represent in it?

15. How is the dynamic model of the transport subsystem SC defined, what does LTL represent in it?

References

1. Dependable IoT for Human and Industry: Modeling, Architecting, Implementation, Vyacheslav Kharchenko, Ah Lian Kor, Andrzej Rucinski (Eds), River Publishers Series in Information Science and Technology, 2018, 450 p.

2. Internet of Things – Architecture IoT-A Deliverable D1.5 – Final architectural reference model for the IoT v3.0, 494 p. https://www.researchgate.net/publication/272814818_Internet_of_Things_-_Architecture_IoT-A_Deliverable_D1.5_-_Final_architectural_reference_model_for_the_IoT_v30

3. Ala Al-Fuqaha, Mohsen Guizani, Mehdi Mohammadi, Mohammed Aledhari, Moussa Ayyash. Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications, *IEEE Communications Surveys & Tutorials* Volume: 17 Issue: 4, 2015, pp. 2347–2376. <https://ieeexplore.ieee.org/document/7123563/references>

4. Alberti A. M., Singh D. Internet of Things: Perspectives, Challenges and Opportunities, International Workshop on Telecommunications (IWT2013), June 2013. Secure layers-based architecture for Internet of Things. Available from: https://www.researchgate.net/publication/303941011_Secure_layers_based_architecture_for_Internet_of_Things [accessed Jul 11 2018].

5. Dilshat Salikhov, Kevin Khanda, Kamill Gusmanov, Manuel Mazzara, Nikolaos Mavridis Microservice-based IoT for Smart Buildings 2017 31st International Conference on Advanced Information Networking and Applications Workshops. https://www.researchgate.net/publication/317071842_Microservice-Based_IoT_for_Smart_Buildings

6. Saber Talari, Miadreza Shafie-khah, Pierluigi Siano, Vincenzo Loia, Aurelio Tommasetti and João P. S. Catalão. A Review of Smart Cities Based on the Internet of Things Concept, *Energies* 2017, 10, 421. 23 p. <http://www.mdpi.com/1996-1073/10/4/421/pdf>

7. Rumbaugh James The unified modeling language reference manual – 2-nd edition / James Rumbaugh, Ivar Jacobson, Grady Booch. Addison-Wesley on Web: <http://www.awprofessional.com> Available at: https://www.utdallas.edu/~chung/Fujitsu/UML_2.0/Rumbaugh--UML_2.0_Reference_CD.pdf [accessed Jul 11 2018].

8. Teo Eterovic, Enio Kaljic, Dzenana Donko, Adnan Salihbegovic, Samir Ribic An Internet of Things visual domain specific modeling. 2015

XXV International Conference on Information, Communication and Automation Technologies (ICAT) Available at: <https://ieeexplore.ieee.org/document/7340537/>

9. Rumbaugh James, Jackobson Ivar, Booch Grady The Unified Modeling Language. Reference Manual. Second Edition, Addison-Wesley, Boston, Mexico, 2004. 742 p. Available at: https://www.utdallas.edu/~chung/Fujitsu/UML_2.0/Rumbaugh--UML_2.0_Reference_CD.pdf

10. Hans-Eric Eriksson, Magnus Penker, Brian Lyons, David Fado. UML 2.0 Toolkit. Wisley Publishing Inc., 2004. 549 p. Available from: http://www.ecotec.edu.ec/documentacion%5Cinvestigaciones%5Cdocentes_y_directivos%5Carticulos/6008_TRECALDE_00278.pdf

11. Grady Booch James Rumbaugh Ivar Jacobson The Unified Modeling Language User Guide // Addison-Wesley Longman Inc., 1999. 391 p. Available at: <https://pdfs.semanticscholar.org/fc51/1dcebd3dae76133d5dbbda4250bebd0fb5e3.pdf>

12. *Dan Simon Evolutionary Optimization Algorithms*. Biologically-Inspired and Population-Based Approaches to Computer Intelligence. Wiley, Cleveland State University, 2013. 727 p. https://books.google.com.ua/books?hl=en&lr=&id=gwUwIEPqk30C&oi=fnd&pg=PP1&dq=computer+evolutionary-genetic+systems+pdf&ots=GLm3DqUag2&sig=UeVaj6EE41SAdXXgEuMMQ6LtUyM&redir_esc=y#v=onepage&q=computer%20evolutionary-genetic%20systems%20pdf&f=false

13. Mark Ridley Evolution. Third Edition. / Blackwell Publishing, 2004. 786 p. http://www.biologia.buap.mx/Evolution__3rd_Edition.pdf

14. Zbigniew Michalewicz Genetic Algorithms + Data Structures = Evolution Programs. Third Edition. Springer, 1996. 388 p. <http://web.ist.utl.pt/adriano.simoes/tese/referencias/Michalewicz%20Z.%20Genetic%20Algorithms%20+%20Data%20Structures%20=%20Evolution%20Programs%20%283ed%29.PDF>

15. Yoav Shoham, Kevin Leyton-Brown. Multiagent Systems. Algorithmic, Game-Theoretic, and Logical Foundations. Revision 1.1 / Shoham and Leyton-Brown, 2010. 532 p. <http://www.masfoundations.org/mas.pdf>

16. Alexander Kleiner, Bernhard Nebel Introduction to Multi-Agent Programming / Introduction to Multi-Agent Programming. 38 p. http://gki.informatik.uni-reiburg.de/teaching/ws0910/imap/01_Introduction.pdf

17. Jos'e M Vidal Fundamentals of Multiagent Systems with NetLogo Examples. 2010. 155 p. <http://jmvidal.cse.sc.edu/papers/mas.pdf>

18. Patricia Bouyer, François Laroussinie Chapter 4 Model Checking Timed Automata. *Modeling and Verification of Real-Time Systems*. pp. 111-140. Available at: http://www.iste.co.uk/data/doc_wrkszvritcbv.pdf
19. J. Kleijn and A. Yakovlev (Eds). *Petri nets and Other Models of Concurrency – ICATPN 2007*, Lecture Notes in Computer Science, vol. 4546, ISBN 978-3-54073093-4, Springer-Verlag, 2007, 515 p.
20. Jorg Desel, Javier Esparza. *Free Choice Petri Nets*. Cambridge University Press, Cambridge, 1995. 256 p. Available from: <https://www7.in.tum.de/~esparza/fcbook-middle.pdf>
21. G. Geeraerts An Introduction to Petri nets and how to analyse them. Groupe de Vérification - Département d'Informatique Université Libre de Bruxelles. 341 p. Available from: <http://www.ulb.ac.be/di/ssd/ggeeraer/Tutorial-Perti-Nets-Geeraerts.pdf>
22. Simon Meier Advancing automated security protocol verification. ETH Zurich Research Collection, 2013. 214 p. <https://www.research-collection.ethz.ch/bitstream/handle/20.500.11850/66840/eth-7011-02.pdf?sequence=2&isAllowed=y>
23. Anna Sugak, Oleksandr Martynyuk, Oleksandr Drozd. Models of the Mutation and Immunity in Test Behavioral Evolution. *Proceedings of the 2015 8th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, 24-26 September 2015, Warsaw, Poland, pp. 790-795. <http://idaacs.net/storage/conferences/2/abstracts/i17-241-423cfa0e28b012f1d05e36800c0c638c.pdf>
24. Oleksandr Martynyuk, Anna Sugak, Dmitry Martynyuk, Oleksandr Drozd. Evolutionary Network of Testing of the Distributed Information Systems. *Proceedings of the 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications*, 21-23 September 2017, Bucharest, Romania, pp. 888-893. <https://ieeexplore.ieee.org/document/8095215>
25. Anna Sugak, Oleksandr Martynyuk, Oleksandr Drozd. The Hybrid Agent Model of Behavioral Testing [Text] / *International Journal of Computing*, 2015, Volume 14, Issue 4, Ternopil, pp. 232-244.
26. Daniel Shahaf *Temporal Logics I: Theory*. Tel-Aviv University November 2007. 155 p. Available from: http://www.cs.tau.ac.il/~annaz/teaching/TAU_winter08/Seminar/daniel.pdf
27. Patricia Bouyer Model-Checking Timed Temporal Logics. LSV – CNRS & ENS de Cachan – France. 142 p. Available from: <http://www.lsv.fr/~bouyer/files/tfit08.pdf>
28. Gerard J. Holzmann *Spin Model Checker, The: Primer and Reference Manual*. Addison Wesley, 2003. 608 p. <http://www.cin.ufpe.br/~acm/esd/intranet/spinPrimer.pdf>

29. I. Skarga-Bandurova, M. Derkach, A. Velykzhanin, A Framework for Real-Time Public Transport Information Acquisition and Arrival Time Prediction Based on GPS Data. In book: Dependable IoT for Human and Industry: Modeling, Architecting, Implementation, Vyacheslav Kharchenko, Ah Lian Kor, Andrzej Rucinski (Eds.), River Publishers Series in Information Science and Technology, 2018.

30. Dinesh Kumar Saini, Kashif Zia, Arshad Muhammad. Software Architecture for Smart Cities and Technical Solutions with Emerging Technologies Internet of Things. In book: Dependable IoT for Human and Industry: Modeling, Architecting, Implementation, Vyacheslav Kharchenko, Ah Lian Kor, Andrzej Rucinski (Eds.), River Publishers Series in Information Science and Technology, 2018.

31. G. Marques, R. Pitarma. An Internet of Things Approach for Environmental Quality Management and Laboratory Activity Support. 14th Iberian Conference on Information Systems and Technologies (CISTI), 2019.

32. Ah-Lian Kor, M. Yanovsky, C. Pattinson, V. Kharchenko. SMART-ITEM: IoT-enabled smart living, 2016.

PART XI. INTELLIGENT TRANSPORTATION SYSTEMS AND IOT

40. INTELLIGENT SYSTEM FOR MONITORING THE TRANSPORT FLOWS

Prof., Dr. V. V. Kochan, Dr. O. R. Osolinskyi, Dr. D. I. Zahorodnia,
Assoc. Prof., Dr. P. Y. Bykovyy, Prof., DrS A. O. Sachenko (TNEU)

Contents

40. Intelligent system for monitoring the transport flowS	322
40.1. Studying the hardware of traffic intensity monitoring.....	324
40.1.1 General structure of IoT monitoring system.....	324
40.1.2 Used software	330
40.1.3 Formation of images database	337
40.2. Recognition and data processing of objects in a video frame.	341
40.2.1 Calibrating the camera and adjusting the resulting image by calibration outcomes	341
40.2.2 Calculating the length and width of vehicles different types	343
40.2.3 Getting and recognizing the images of vehicles different types	345
40.3. Recognizing and data processing of objects array in a video stream.....	356
40.3.1 Counting the number of vehicles different type that passed through the camera field	356
40.3.2 Determining the coefficient of road filling by vehicles different types	358
40.3.3 Processing of video stream for IoT	359
40.4 Control system of the traffic flow intensity	365
40.5 Work related analysis.....	367
Conclusions and questions.....	369
References.....	370

Abbreviations

AWS - Amazon Web Services

CCTV - Closed-circuit television

IMAQ - Institute of Mediation and Arbitration of Quebec

NI - National Instruments

SCADA - Supervisory Control and Data Acquisition

SW - Software

VI – Virtual Instrument

V2V - Vehicle-to-Vehicle

V2I - Vehicle-to-Infrastructure

40.1. Studying the hardware of traffic intensity monitoring

40.1.1 General structure of IoT monitoring system

The overall structure of the IoT system should consist of data collection and transmission modules, a server (cloud) part, and the user/administrator who requests the server and receives the required information (Fig. 40.1). In addition, if implementation permits, then the user can contact directly the devices to collect and transfer data without involving the server.

Load capacity of roads depends on the number of cars per unit of road area, and on their dimensions, maneuverability, etc. it is necessary to know the intensity of the traffic flow for its operational management. This will enable the reasonably making decisions about changing the recommended routes either changing the ratio of switching traffic lights at crossroads or creating a "green street".



Fig. 40.1 – Generalized structure of IoT-system

Different methods for determining the number of vehicles passing through the road at fixed intervals are possible. Let's consider examples:

1). Using the single infrared sensors. These sensors should be positioned across the road above it to overlap all lanes of vehicles (Fig. 40.2).

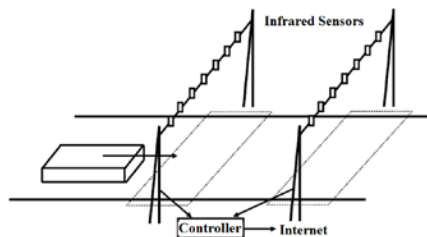


Fig. 40.2 – Placement of infrared sensors across the road

They should be placed with a certain gap that will allow the identification of individual vehicles. The main drawback of this method is the following: single infrared sensors, with a large gap between them may not be small and relatively cold vehicles. Such vehicles, when placed in the zone between the sensors, create a relatively small signal that does not exceed the threshold for sensor operation. Increasing sensor sensitivity leads to the detection of non-existing vehicles due to thermal impediments (heat fluxes that are obstructed by people, animals, sun-heated sections of the road). Also, due to the excess sensitivity of the sensors, simultaneous detection of one vehicle by several sensors may be possible. Therefore, such a method of determining the number of vehicles passing through the road at fixed intervals should be considered as the unreliable one, and its use is not feasible.

2). Using a set of integrated infrared (pyrometric) sensors.

These sensors are often used in access control systems for apartments. They should also be located across the road with a certain gap, which will ensure the recognition of vehicles across the entire width of the road (Fig. 40.3). However, the contradiction between distance and sensitivity can be bypassed. To do this, one should not recognize individual vehicles, but integrate the intensity of infrared radiation at given fixed intervals of time. This method can even take into account, to some extent, the size of vehicles. Therefore, such a method is much more promising. However, the influence of heat streams that are not derived from vehicles can not be eliminated when using this method. Although humans and animals create a relatively small heat flux (it will have little effect on the integral heat flux from vehicles with an intense

traffic flow), the heat flow that creates the sun-heated section of the road can greatly distort the results of determining the intensity of the traffic flow. Therefore, this method should be considered also as unreliable one, and its use is inappropriate.

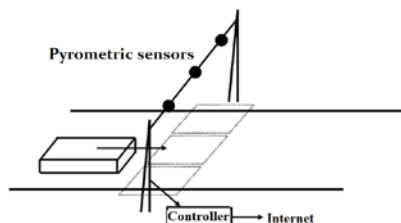


Fig. 40.3 – Placement of group of integrated passive infrared (pyrometric) sensors

3). Using the single magnetic sensors. These sensors, similar to single infrared sensors, should be positioned across and over the road so as to cover all lanes of vehicles (Fig. 40.4). They should be placed with a certain gap that will enable the identification of individual vehicles. The disadvantage of this method is that single magnetic sensors, with a large gap between them may not be able to detect small vehicles, especially those that are made using the latest technologies, that is, using plastics and lightweight (non-magnetic) materials. Such vehicles, especially when entering the zone between sensors, create a relatively small signal that does not exceed the threshold for sensor operation. Increasing the sensitivity of sensors or reducing the gap between them leads to the simultaneous detection of one vehicle by several sensors. However, the main drawback of the method is the considerable complexity of its implementation. When infrared sensors should be positioned above the road, magnetic sensors should be close to these vehicles for reliable vehicle fixation. Because the vehicles have a very different height, the magnetic sensors should be placed under the road surface. Therefore, such a method of determining the number of vehicles passing through the road at fixed intervals should be considered very labor-intensive and insufficiently reliable, and its use is not feasible.

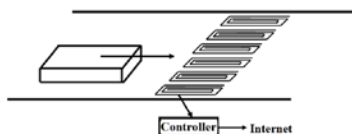


Fig. 40.4 – Placement of single magnetic sensors

4). Using the magnetic sensors. For the integrated flow of vehicles detection magnetic sensors can be used (Fig. 40.5) the same way as infrared sensors (see above). However, with some advantages, the method has a very significant disadvantage - at low speeds of vehicles magnetic sensors stop detect (the amplitude of the generated voltage of the integrated magnetic sensor - the coil of inductance, covering the entire width of the road - is directly proportional to the rate of change of the magnetic flux). Namely, in difficult traffic situations (traffic jams), when data on the intensity of the traffic flow is most needed, the speed of vehicles is reduced and the electromagnetic sensors cease to work. Therefore, such sensors can be used on highways only, where the probability of a critical reduction in the speed of vehicles is relatively small. However, the main drawback of the method - the considerable complexity of its implementation remains. Therefore, such a method of determining the number of vehicles passing through the road at fixed intervals should be considered as the very labor-intensive and insufficiently reliable one. Its use, especially at the intersection, where the likelihood of a critical reduction in the speed of vehicles or even their stops is very high, should be considered as the inappropriate one.

5). Using a Camera. In this case, the determination of the number of vehicles passing through the road at fixed intervals is reduced to the classical methods of image processing. Each vehicle is recognized, for example, by recognizing its shape using an appropriately trained neural network.

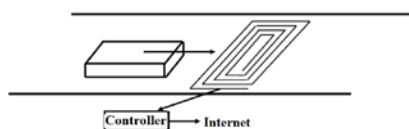


Fig. 40.5 – Placement of magnetic sensors for the integral flow

The appearance of a new vehicle is getting by the camera (Fig. 40.6). Then it is accompanied until the disappearance in the camera's field of view. The number of vehicles that have passed through the field of view of the camera at fixed intervals is also calculated. It can be also taken into account the dimensions of each vehicle by counting the number of pixels in the image that contains the contour of the vehicle. This method is relatively cheap, since modern webcams and computing devices have a relatively low price. Moreover, the introduction of such a method does not require significant costs - webcams can be placed on the back of the lantern or the wall of the house adjacent to the road.

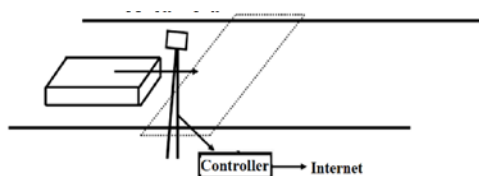


Fig. 40.6 – Webcam location

6). Using the Tracers. The most reliable and straightforward is the use of tracers - microcontrollers, which (similar to the corresponding devices in aviation), upon request, either continuously transmit the type, traffic parameters (direction and speed) and vehicle coordinates on the Internet (Fig. 40.7). It is advisable to use the known communication protocols (Zigbee, Bluetooth, etc.). Such a decision is being used already in public transport vehicles to control their passage along the route. But in order to determine the number of vehicles passing through the road at fixed intervals, such a decision requires the equipping of all vehicles with appropriate tracers. Therefore, such a decision is not yet available.

Taking into account the survey above, it is suggested to consider monitoring of transport using video cameras.

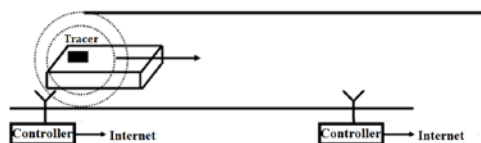


Fig. 40.7 – Use of tracers

Under the term "determining the intensity of the transport flow" we consider the number of vehicles that pass through the road at fixed intervals. For this purpose, a different hardware could be used, for example:

- A web camera that connected to the computer via USB port.
- A web camera connected via USB port to a wireless USB extender, which transmits information to computer via Wi-Fi.
- A web camera connected via a USB port to a single-board module with the ability to involve external peripherals, like Raspberry Pi. It enables transmitting the information to appropriate computer or server.
- IP-camera, which transmits images to a computer or server.

Web camera that connects via USB to a computer and web camera connecting with the Wireless USB Extender, which in turn transmits the information to a computer by means of Wi-Fi (Fig. 40.8).



Fig. 40.8 – Using the USB web camera with/ without Wireless Extender

As the intermediate option between a regular webcam with a computer and the IP camera, we can consider usage of modules with the ability to connect external peripherals and independent power supply, such as Raspberry Pi (Fig. 40.9). It was possible to install Linux OS on early Raspberry Pi models Starting from Raspberry Pi 2 and Pi 3 models, it's possible to run Windows 10 IoT Core, which enables to migrate to Raspberry the previously written Windows and debugged applications. The first (early) models of Raspberry use the single-core ARM processor Broadcom BCM2835 with a frequency of 700 MHz. A current version of Raspberry Pi 3 uses the more powerful 64-bit processor Broadcom BCM2837, which is located on 4 core ARM Cortex-A53 at 1.2 G Hz, with RAM up to 1 GB (Fig. 40.9).

Besides, it's possible to use IP cameras, which, unlike traditional analog monitoring devices, make it easy to check traffic conditions in geographically remote locations and transmit information through both wired or wireless channels (Fig. 40.10).

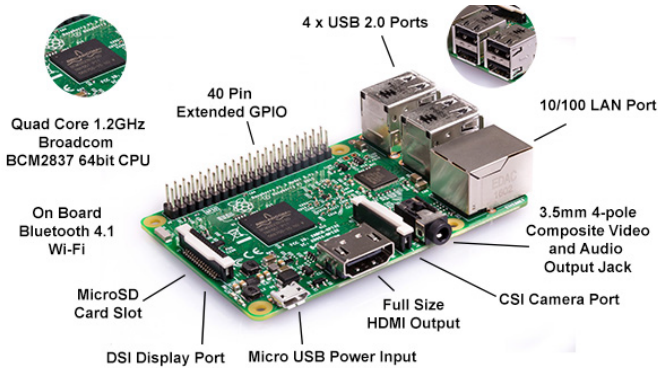


Fig. 40.9 - Raspberry Pi 3 B



Fig. 40.10 – Example of IP camera usage

40.1.2 Used software

LabVIEW is one of the National Instruments' products [1]. LabVIEW is an abbreviation that stands for Laboratory Virtual Instrumentation Engineering Workbench. It shows the orientation of laboratory studies, measurement and data collection. The process of developing a SCADA system in LabVIEW is simpler than using the "traditional" development tools.

LabVIEW software modules called "Virtual Instruments" or VI. They are stored in files with extension *.vi. VIs are "bricks", of which LabVIEW is a program. Any LabVIEW program contains at least one VI. An analogy with the function can be employed in terms of language

C, but in LabVIEW one function is contained in one file (toolbars can be created too) [2-5]. One VI can be called from another VI. In principle, each VI consists of two parts - the Block Diagram and the Front Panel. Block diagram is a program code (more precisely, a visual graphical representation of the code), and the front panel is an interface.

LabVIEW is based on the data flow paradigm [5]. In the aforementioned program, a line(called Wire) connects the constant and the terminal of the indicator. It can be called "conductor". The conductors transmit data from one element to another. This entire concept is called as Data Flow. The essence of Block Diagrams is "nodes", outputs of some nodes are attached to the inputs of other nodes. The node is activated to execute when all the necessary data comes for the job. The diagram above is two Nodi. One of them is a constant. This node is self-contained - it starts to run immediately. The second node is an indicator. It displays the data that the constant conveys (but not immediately, but as soon as the data arrives from the constant).

All elements will be executed in parallel. The developer does not need to think about how to parallelize tasks to multiple threads, which can be run in parallel on several processor cores. The latest versions enable to explicitly specify which of the processor cores must run at that or another while-loop. It should also be noted that at the disposal of the developer, a rich selection of tools for synchronizing flows - semaphores, queues, etc.

LabVIEW includes a large set of elements for building user interfaces [6,7]. The speed of creating the user interface exceeds the speed of creating the interface in Visual C ++, Visual Basic, .NET, etc.

The LabVIEW basic package includes also the blocks for working with .ini files, the registers, functions for binary and test files, mathematical functions, powerful tools for constructing graphs and the ability to call DLLs. LabVIEW enables to work with ActiveX components and .NET. A support for classes is provided, so it makes some analogy with the object-oriented SW. However, LabVIEW is not a full object-oriented language, although the main features of object-oriented languages - inheritance and polymorphism are presented there. Moreover, additional modules, such as NI Vision Toolkit - for processing images and machine vision, etc., can extend the functionality and the executable .exe file can be generated with the

Application Builder module. It's possible to work: with ftp servers using Internet Toolkit, and databases using Database Connectivity Toolkit.

Many users and developers of LabVIEW believe this is an interpreter, and block diagrams are interpreted constantly by the kernel. But this is not the case, LabVIEW is a compiler. Compilation is "on the fly" - at any point in the development process, the program is always ready to launch. LabVIEW code can also be compiled into an executable file that can be run on a computer without installing LabVIEW (requires LabVIEW Run-Time). We can also build our own installation packages without third-party tools like InstallShield.

LabVIEW Cloud Toolkit for Amazon Web Services (AWS) (Fig. 40.11) provides interfaces from Windows or LabVIEW real-time Amazon Web Services applications for storing data, publishing messages, and queuing operations.

This module provides additional storage for analytics or post-processing operations; we can use cloud services to programmatically store and retrieve any amount of data from PC-based applications or hardware modules, such as CompactRIO. Such integration with AWS cloud services offers an efficient way to store large volumes of measurements and data directly from LabVIEW, ensuring security, reliability and availability.

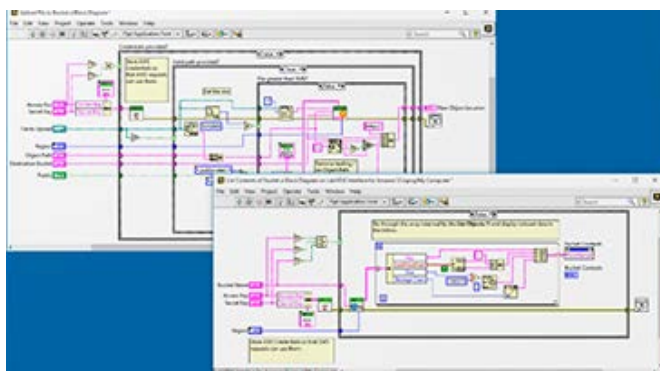


Fig. 40.11 – LabVIEW Cloud Toolkit for AWS

The toolkit supports the following services:

-AWS S3: Simple Storage

- AWS SNS: simple messaging service
- AWS SQS Simple Queuing Service
- AWS IoT Internet of Things

Image and video processing with LabVIEW and Vision Acquisition Software and NI Vision Development Module. Vision Acquisition Software is a software for capturing, displaying, registering and monitoring images from many types of cameras [8].

Vision Development Module is a set of modules for developing image processing programs that use the LabVIEW and LabVIEW NXG for Windows and real-time systems as well as C, C++ and C# for Windows systems. This package implements all popular image processing algorithms, including filters, morphologies, image matching, 3D image and classification.

To get started, it's necessary to complete a first phase configuring a webcam, or another that is connected to a PC. For this purpose we run Programs> National Instruments> Measurement & Automation Explorer (Fig. 40.12). Then we need to select Devices and Interfaces> NI-IMAQdx Devices.

After that a list of available equipment is opened, in this case cam0 USB2.0 VGA UVC WebCam for checking the equipment and its selection from the list (Fig. 40.13). Also, in this window the camera can be conFig.d according to the user's requirement.



Fig. 40.12 – Measurement & Automation Explorer

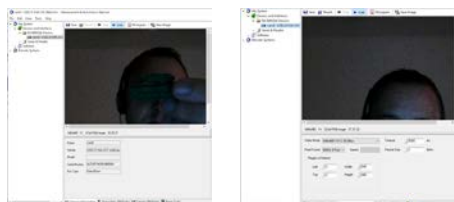


Fig. 40.13 – Camera configuration

After setting up the hardware, it is possible to carry out a second phase creating a new virtual tool in the LabView environment for image and video processing.

The *first* step of the second phase is to add the required modules in the BlockDiagram field

To do this, in the BlockDiagram field, select the Vision and Motion> NI-IMAQdx> Open Camera VI [9], Place the tool and connect a constant in the box that specifies the name of the camera to be used (cam0).

IMAQdx Open Camera VI opens the camera, surveys the camera about its capabilities, downloads the camera configuration file and creates a link to the camera.

In a *second* step of the second phase it is necessary to select in the Palette functions to choose Vision and Motion > NI - IMAQdx > Snap VI (Fig. 40.14) and connect the data elements.

IMAQdx Snap VI is employed for equipment with a low speed or for one-time capture of a frame, Snap VI by default uses cam0. If the image type does not match the video format of the camera, this VI changes the image type to the appropriate format.

The *third* step is to select Vision and Motion> Vision Utilities> IMAQ Create(Fig. 40.15) in the Function palette and connect it to Snap VI.

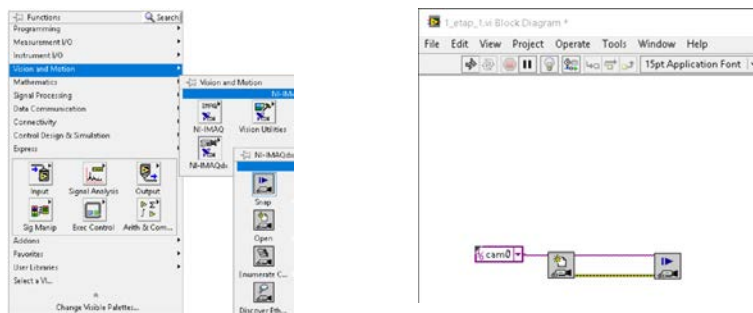


Fig. 40.14 – IMAQdx Snap VI

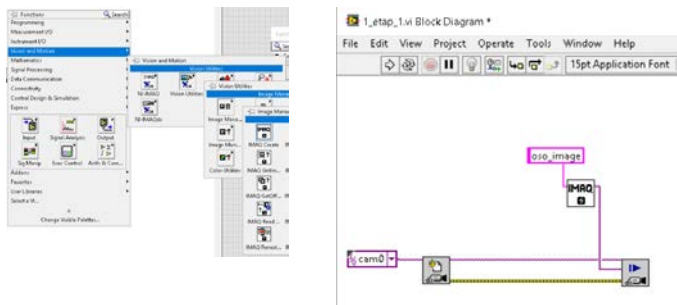


Fig. 40.15 – IMAQ Create VI

IMAQ Create VI creates a temporary memory location for an image.

In the fourth step we need to select the Vision functions in the Palette and Motion > NI - IMAQdx > IMAQdx Close Camera VI (Fig. 40.16) and connect it to the IMAQdx Snap VI element.

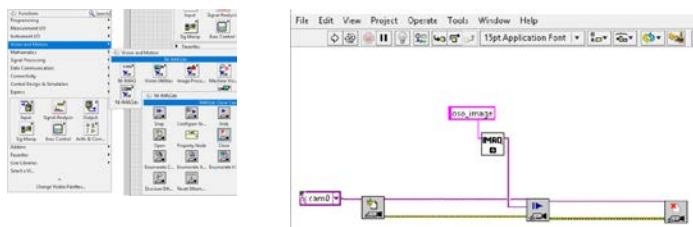


Fig. 40.16 – IMAQ Close Camera VI

To display the results, we go to Front Panel> Vision> Image Display, and in the Block Diagram panel, then connect the Image Display item with IMAQdx Snap VI(Fig. 40.17). At this stage, the program can receive only one frame from the web camera .

To display all frames, we need to select Programming> Structures> While Loop(Fig. 40.18) in the Function Palette and put our modules into it.

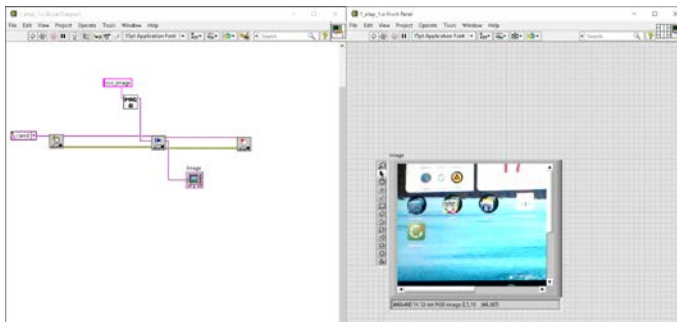


Fig. 40.17 – IMAQdx Snap VI

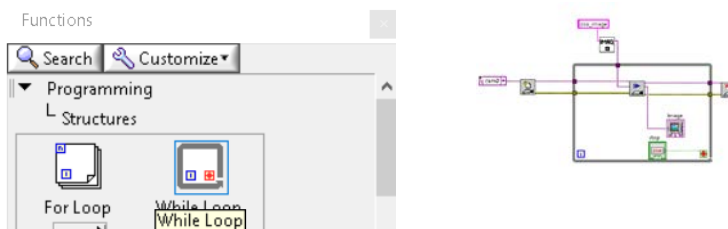


Fig. 40.18 – While Loop

After that, it will be possible to receive images from the camera in a cyclic manner (Fig. 40.19).

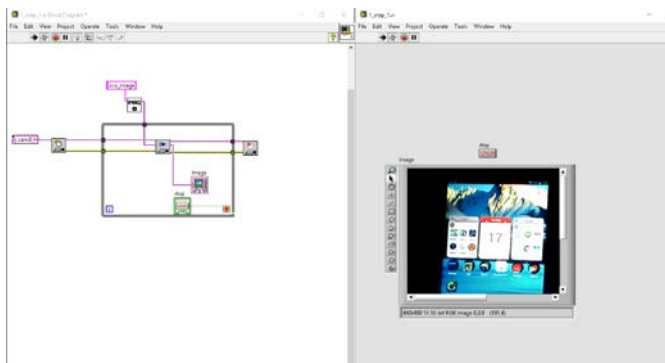



Fig. 40.19 – Retrieve Reference camera image cyclically


However, with this execution, only individual images will be in output. To get the video stream, we need to modify this schema, namely

to replace the IMAQdx Snap VI element with IMAQdx Grab VI, and after the IMAQdx Open Camera VI element it's necessary to connect the IMAQdx ConFig. Grab VI element. After these changes, a complete video stream should be received.

40.1.3 Formation of images database

To save the processing results in LabVIEW, we have to complete the following steps: (i) Modify the previous program (ii) Add the

following blocks  IMAQ AVI Create VI [8], that creates a new AVI file or overwrites the old AVI file and put it after IMAQdx Open

Camera VI  and connect according to the block diagrams (Fig.40.20, 40.21).

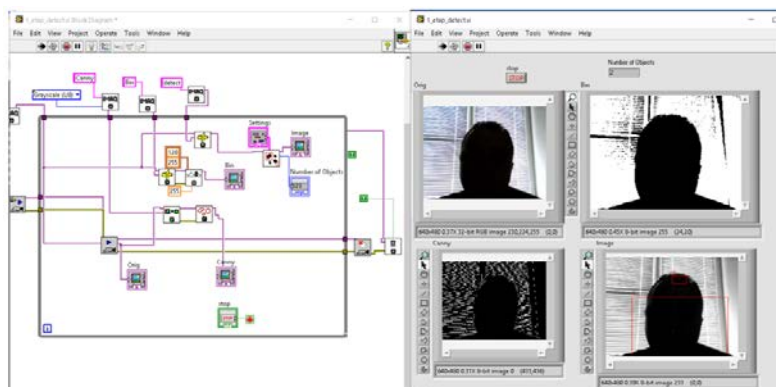


Fig. 40.20 – Program of image processing

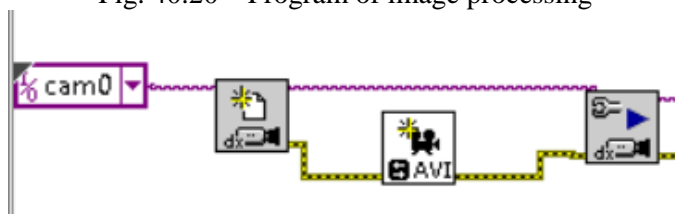


Fig. 40.21 – Improving the image processing program

When setting up IMAQ AVI Create VI it's necessary to specify

the location of the video file (Fig. 40.22).



Fig. 40.22 – The location of the video file

The next block to add to the program is IMAQ AVI Write Frame



. This block records the image into an AVI file specified by Avi Refnum, which in turn derives from IMAQ AVI Create VI. The data connection of the blocks is shown below and it is marked by red (Fig. 40.23).



Fig. 40.23 – Connection diagram of IMAQ AVI Write Frame

For correct completion of the file recording procedure, we have to

use the IMAQ AVI Close VI block  that closes the AVI file associated with AVI Refnum, which in turn gets from IMAQ AVI Write Frame VI. The combination of block data is marked by red (Fig. 40.24).

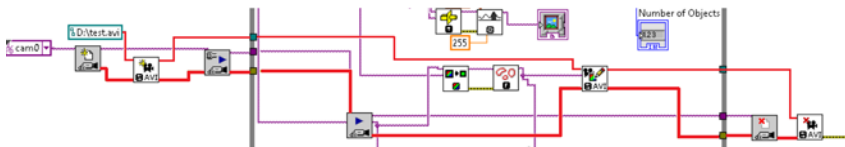


Fig. 40.24 – Connection diagram IMAQ AVI Close VI

After stopping the program, a file is created where the video streaming results are recorded. The results of the modified program are

shown in Fig. 40.25, created file with the path

D:\test.avi

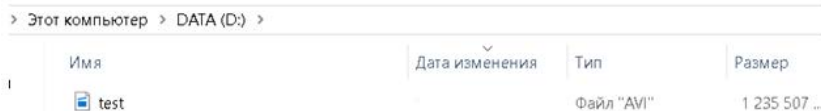


Fig. 40.25 – Result of saving

A saved video (Cany's method) is illustrated by picture (40. 26).



Fig. 40.26 – Video Result (Cany's method)

In turn, the intelligent video surveillance system is a system with its own real-time operating system, which provides high operational reliability and it uses computer resources maximally. It enables to achieve a maximum speed, the minimum reaction time to events and it has a long-term stability.

Such systems are characterized by: high speed; a large number of cameras; various modes of displaying video information on the screen; control modes; auto-visualization of channels; scalability; support for many recording formats; changing image parameters: brightness, contrast; intelligent motion detector; event logging work on schedule; catalog of recorded frames.

The first element of an intelligent video surveillance system is video sensors. Examples of video sensors can be digital or IP cameras. From the video image the sensor enters the imaging device. After that, the image is pre-processed to improve image quality and reduce the amount of video information, then it gets on the frame drive. Next, the face area is localized and contour segmentation is carried out.

Contour segmentation consists of detecting and examining a contour, and selecting characteristic points on it. When detecting the contour, it is necessary to obtain an external contour in the form of a closed curve (approximation methods are often used there). The curve

approximation method can be used for contour segmentation by selecting an analytically given curve in a set of contour preparation points. If there is information about the expected shape of the object (for vehicles), then a rectangle should be taken as an approximating curve or applied the approximation by polynomials using iterative selection methods.

Contour monitoring consists in entering the coordinates of the contour points into a two-dimensional array. Actually the algorithm itself contour resembles the behavior of the "bug". For a binary image, an imaginary "bug" begins its journey on a white field and moves towards the area of the black elements of the image. After the beetle crosses the black element, it turns left and proceeds to the next element. If this element is black, then the "bug" turns to the left again, but if the element turns white, then the "bug" turns to the right. This procedure continues until the "bug" returns to the starting point (the contour closes). The coordinates of the transition points from black to white or from white to black will be the coordinates of the contour points.

After that, the characteristic points of the contour (points on areas of significant curvature) are highlighted. Based on information about the characteristic points of the contour, a classification is carried out - the procedure of assigning the object (image) to a specific class.

To perform its functions, the vehicle recognition system uses a number of hardware and software tools, among which the main ones are video sensors and a computer. Intelligent video sensors can be programmed to perform high-level procedures such as preprocessing and image segmentation, partially or completely replacing the computer.

A computer in a vehicle recognition system is a hardware complex (microprocessor, RAM, disk drives, and others) and software (detection subsystem, vehicle recognition, vehicle database management subsystem, input and output files, and others) and performs as a rule, the high-level segmentation and image analysis procedures. A specialized hardware can be a part of recognition systems: video capture cards, network equipment for distributed recognition systems, and others [14].

40.2. Recognition and data processing of objects in a video frame

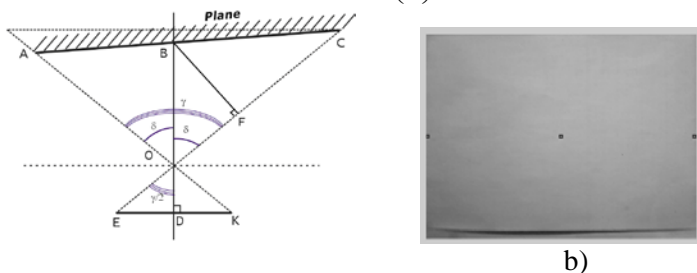
40.2.1 Calibrating the camera and adjusting the resulting image by calibration outcomes

Geometrical methods can be used to calibrate the camera. For this purpose, is necessary to determine the focal length and angle of view of a video camera by measuring its placement in the environment. The angle of view of the video camera γ and the focal length OD are unknown, they should be looked for experimentally at the stage of camera calibration. For this purpose, the video camera needs to be fixed at a certain distance of the OB relative to the plane of the AC (Fig. 40.27, a). At the same time, the plane of the AC is projected on the touch panel EK video camera through an optical lens at point A . The horizontal angle of view of the video camera γ can be determined on the basis of the angle δ with the trigonometric properties of the triangle OBC , for which by the cosine theorem:

$$\gamma = 2 * \delta = 2 * \arccos\left(\frac{OB^2 + OC^2 - BC^2}{2 * OB * OC}\right). \quad (40.1)$$

Measurement of BC , OC and OB sizes is provided on the basis of marks taken on the plane and correspond to the last positions of the image (Fig. 40.27,b). The focal length OD can be calculated from a certain angle γ and the video resolution ED in pixels:

$$OD = ED / \operatorname{tg}\left(\frac{\gamma}{2}\right).$$



a) Fig. 40.27 – Geometric representation of the camera calibration process:
a) geometric representation; b) image obtained during calibration

Another method of calibration is to lower the perpendicular and determine the angle of camera view, as well as the focal length, from right-angled triangles (Fig. 40.28)

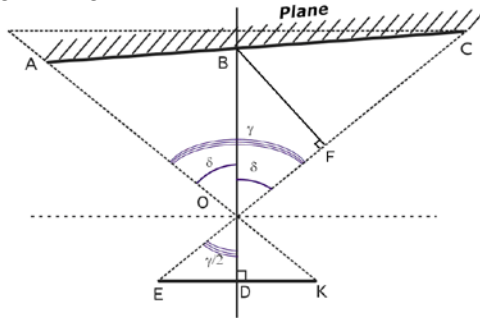


Fig. 40.28 – Geometric representation of another camera calibration method

Calibration of the internal parameters for the camera is performed using the NI Vision Development Module of LabView. Calibration Training has an independent calibration module that makes calibration more convenient and efficient. The calibration process can be divided into three stages: the first is the study of the pattern, a second one is the calibration itself, and the third step is the reading and recording the calibration results.

There are two types of calibration pattern, a first one is the square of the board, and a second one is the circular target of the calibration.

The algorithm for extracting stability and positioning accuracy of the circle center exceeds the angle extraction by a checkerboard calibration plate; a simple calibration can be performed with an array pattern of 6 x 8 points (Fig. 40.29).

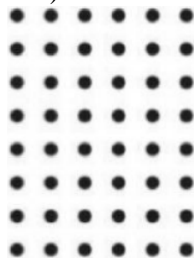


Fig. 40.29 – 6x8 dot array calibration board

The distance from the center between two adjacent points of the distance horizontally and vertically, respectively, is 24 mm.

The calibration algorithm can be described by following steps:

1. Loading the calibration image
2. Extracting the circular contour using a canny filter
3. Running the positioning using round fitting
4. Introducing the calibration image information
5. Configuring the internal camera settings
6. Adjusting the nonlinear optimization
7. Adjusting the external camera settings
8. Saving the calibration results
9. Completing the calibration.

40.2.2 Calculating the length and width of vehicles different types

To determine the length, width and distance between vehicles using LabView is necessary to create the following virtual instruments (Fig. 40.30) which will help to track objects and obtain their parameters.

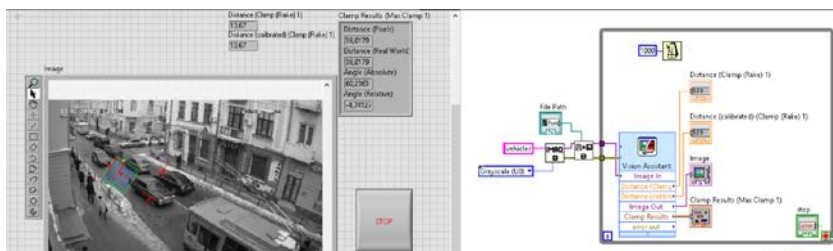


Fig. 40.30 Virtual instrument for vehicle parameters definition

To create the virtual instrument, the following blocks were used:

1. IMAQ Create VI
2. IMAQ ReadFile VI
3. While loop
4. Vision Assistant Express

IMAQ Create VI and IMAQ ReadFile VI will be described in the subchapter below.

While Loop - Repeats the sub-program inside until the condition is true or when it receives a specific logical value. The logical value depends on the behavior of while cycle. Behavior has two states: "Stop if true" or "Continue if true". Also, the errors cluster can be connected to the conditional terminal. It will allow to perform another condition: "Stop is error" or "Continue if error". The while loop (Fig. 40.31) is always running at least once.



Fig. 40.31. While loop (LabView)

Vision Assistant Express - provides the launch and rapid subsystems development for machine vision, image and video processing. Using such instrument the user can select a set of manipulations with video or image and create a macro. After that the Vision Assistant Express will automatically perform actions specified by the user. The advantage of using this module is the absence of necessity to create the new virtual instruments.

After all components selection it is necessary to adjust the Vision Assistant Express settings according to the requirements. In the first step is necessary to open the main window Vision Assistant (Fig. 40.32)

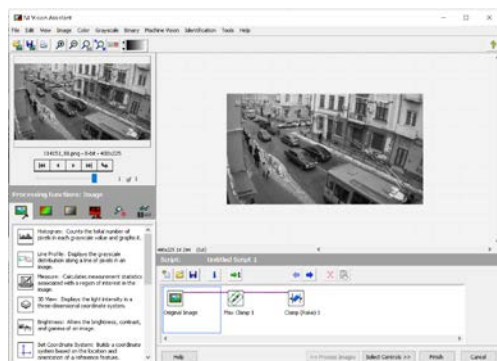


Fig. 40.32 – Main window Vision Assistant

In the second step is necessary to open the Machine Vision tab and select the Max Clamp element (Fig. 40.33).



Fig. 40.33 – Max Clamp module

This module finds the edges along the selected area (only rotated rectangle) and measures the distance between most distant opposite points on the found edges. The edges are determined by removing contours from the field of interest and by analyzing their order and geometry. If the reliable calibration information is present then a distance is measured in pixels as well as in real measurement units.

In the third step is necessary to add the next Clamp (Rake) module (Fig. 40.34). This module measures the distance in the horizontal direction from vertical sides of search area to the center of search area. The virtual instrument finds ribs along a set of parallel search lines or edges. The edges are determined basing on their contrast and tilt.



Fig. 40.34 – Clamp (Rake) module

After those three steps above, the Vision Assistant is ready to work and it can be used in the virtual instrument.

A simple algorithm for compiling a virtual tool is can be stated just in the two steps: (i) Place an IMAQ Create VI element on the chart; (ii) Set up the settings.

40.2.3 Getting and recognizing the images of vehicles different types

During the recognizing, the most informative part of the image is the contour. The contour of an object contains a large amount of

information about the shape of an object and does not depend much on the color and texture of the image.

In many cases, information about the shape of the object is sufficient for the organization of automated systems. In addition, the transition to the recognition of objects by their contours enables (for several orders of magnitude) to reduce the amount of the processed information, in addition, the contours is invariant to brightness transformations.

Since the basic information about the shape of the object is contained in the contour, the selection and description of the contour is an important task of image analysis.

After digitization, each pixel uniquely refers either to the background or to the image. There are different types of criteria for deciding whether each of the pixels belong to the background or the outline of the image.

The contour pixels differ from internal points of the image by the presence of one or several adjacent background cells. At the same time, only horizontal and vertical neighboring cells, or only diagonal cells, are considered as neighboring.

The contour of the binary image is defined by dots in the centers of the cells adjacent to each other. If half the length of the side of the square shifts the grid to the right and up, then contour points of the image will be in the nodes of the grid. As a result, the perception of the contour is simplified.

The result of the selection of contours is a contour element - a secondary image of the same size as the original one. At the initial moment, all points of this image are black, and in the process of selecting the contours, the pixels corresponding to the identified limit points of the image are painted in white.

The contour on the color image corresponds to the drop in intensity. However, this definition excludes contours associated with abrupt changes in hue color and intensity in areas with constant brightness.

Representation (coding) of the contour is a stage of obtaining a discrete signal, describes the boundaries of the digitized image.

Requirements for the contour presentation algorithms:

1. reducing the amount of used memory for storage;
2. reducing the time and complexity of further processing;

3. obtain informative features of the object.

Biological systems of visual perception, as research has shown, mainly use contours to select objects, and do not divide objects by brightness. In practice, the drops will NOT be sharp despite the degradation and the limitations imposed by video equipment. Sometimes brightness differences along the boundaries are better traced in the form of jumps of the first derivatives of brightness than by analyzing the values of the brightness itself.

To solving the problem of selecting contours is to try to find a compromise between the number of false contours and the number and size of contour breaks.

It is known that the result of the tracking operation is much less affected by small gaps. They are easier to fix than erroneous contours that are easily confused [15]. The ratio between the number of false contours and the number and size of discontinuities is determined by the noise immunity of the contour extraction method.

Any region D of the plane of a complex variable contains internal points and contour points (boundary points). The first of them have the peculiarity that not only they themselves, but also some of their neighborhoods entirely belong to domain D . The contour points are not internal, but in any small neighborhood of such points there are internal points of area D and points that do not belong to area D - external (background colors). The domain D has the property of connectedness, which consists in the fact that all its points are connected by a line that is completely in the middle of D .

A contour line of G called convex if the straight line segment connecting its two any points consists entirely of internal points of area D . A contour section is concave if such a segment includes external (background) points.

The internal element (pixel) of a binary digitized image $\omega(m_1, m_2)$ has the property of four-connectivity, that is, the adjacent elements - upper, lower, left and right, also belong $\omega(m_1, m_2)$.

To process the contour analytically, it is necessary to encode it, that is, to assign a certain number to each contour element. The sequence of such numbers is called the contour code.

On a square grid, there are eight possible standard arrangements. Let's consider some methods for encoding contours [16, 17].

1. Coding by three features: the length of the current elementary vector, the direction of rotation in the transition to the next elementary vector and the angle between adjacent elementary vectors.

2. Coding the current elementary vector three-digit binary code (numbers from 0 to 7). This code was proposed by Freeman and was widely used in image processing tasks.

3. The coding of the current elementary vector by its two projections on the coordinate axes with the origin combined with the beginning of the elementary vector is a two-dimensional code.

4. A polygonal representation of the contour, obtained by approximating it with linear segments (Fig. 40.35).

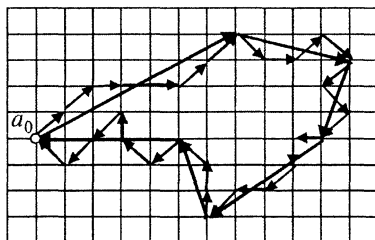


Fig. 40.35 – Polygonal representation by contour approximation of linear segments

Coding consists in fixing the coordinates of the ends of these segments.

This method due to the compactness of the obtained descriptions is widespread. This raises the problem of segmentation, similar to the problem of discretization of signals. In real cases, it is usually associated with the loss of information about the shape of images.

The methods for contour extraction can be divided into two large groups: differential and correlation extremal. In differential methods, the intensity drops are amplified by numerical differentiation, then the contour is extracted using a threshold device, after which the binary image is subjected to secondary processing, the purpose of which is to refine the contour to one pixel. The methods are simple to implement and have high speed, but have low noise immunity. The main criterion in assessing the noise immunity of the contour extraction is the position of the brightness difference.

On the other side, two approaches are used to define and describe a contour: selecting the edges or selecting the area of a point of which form an object.

The literature lists a large numbers of algorithms for the selection of contours and boundaries. The most popular methods are the operator Roberts, Sobel, Prewitt, Kirsch, Robinson, the Canny algorithm and the LoG algorithm [17, 18]. These algorithms are based on underlining sharp changes in brightness, which are characteristics of the objects contours.

LabVIEW Vision enables to read/create images files and it provides the means to manage these files. Such module has built-in functions for image analysis files (image area selection, intensity measurement, etc.). LabVIEW IMAQ enables to receive images from cameras.

A set of virtual instruments (LV-Based Vision Tools)(Fig. 40.36) for working with images and video is described below.

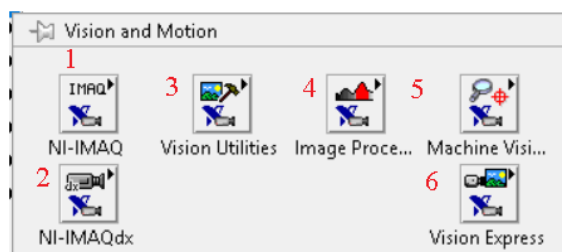


Fig. 40.36 – LV-Based Vision Tools

There are basic virtual instruments of LV-Vision Tools: Image data type, Capturing images; (2) Analyzing images; (3) Vision Utilities; (4) Image processing; (5) Machine vision.

Vision Utilities – VIs is assigned for creating and manipulating images, etc. Image Processing – provides ‘low level’ Vis. Machine Vision – groups many practical Vis for performing image analysis. For example, the “Count and Measure Objects” VI is found under this group. for analyzing images.

Vision Utilities (Fig. 40.37) is used to create and manipulate images, for example: Image management (create, dispose, etc.); file handling; image manipulation; pixel editing; etc.

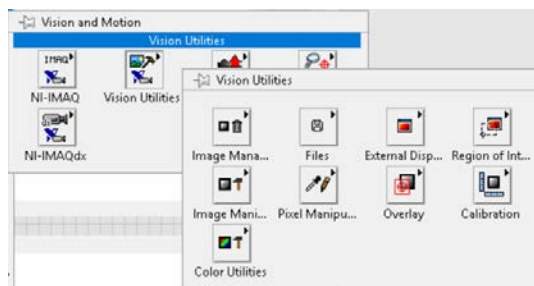


Fig. 40.37 – Vision Utilities

To determine objects (vehicles) in LabVIEW it is necessary to create the following virtual instrument. The process of its creation consist of the following steps:

Step 1. Create an empty loop where all the main elements will be placed (Fig. 40.38)

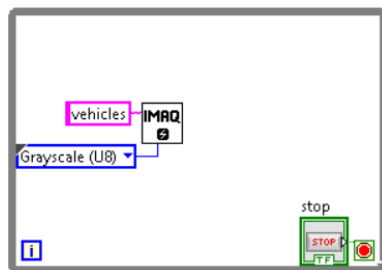


Fig. 40.38 – IMAQ Create VI

Step 2. Select and place the virtual instrument IMAQ Create VI (Fig. 40.38) into the loop. This instrument is necessary for a temporary memory allocation for images in NI Vision package. The components in Figure 40.38 run the following functions:

Border Size - specifies the size of the border around the image in pixels. The default value is 3 pixels.

Image Name - the name associated with the created image. Each created image should have a unique name.

Error in (no error) - describes the status of an error before running the virtual tool or function. If the error occurs, it transmits from one node to another and the job is not executed while a cycle is running in the idle mode.

Image Type - Sets the image type and has the following representation: grayscale (U8) (0) 8 bits per pixel; grayscale (16) (1) 16 bits per pixel; RGB (U64) (6) 64 bits per pixel and so on.

Step 3. Provide the Image Name and set the Image Type (Fig. 40.39).

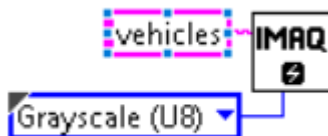


Fig. 40.39 – Setting options for IMAQ Create VI

Step 4. Add the IMAQ ReadFile VI virtual tool. Its main functions are following: reading the image files of the following formats - BMP, TIFF, JPEG, JPEG2000, PNG and AIPD or non-standard user-defined formats.

Step 5. Specify the path of the image location and connect with IMAQ Create VI according to the scheme (Fig. 40.40)

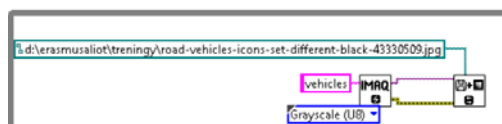


Fig. 40.40 – Opening a file

Step 6. Add the module for objects detection IMAQ Count Objects 2 VI for vehicles selection in the video or image fragment (Fig. 40.41).

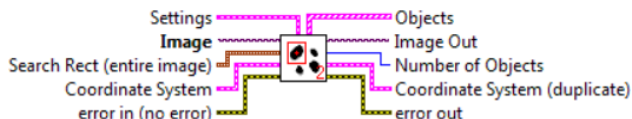


Fig. 40.41 – IMAQ Count Objects 2 VI

This module can be used to measure objects that are listed in the rectangular area. A current virtual tool uses the threshold of pixel intensity to segment objects from their background. To display results and set object search options on the Front panel it is necessary to create

the elements for displaying the results: Image display, Number of Objects and search Setting parameters (Fig. 40.42).

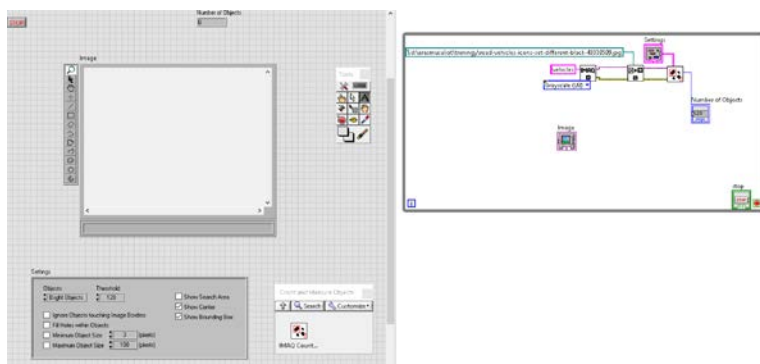


Fig. 40.42 – Connection scheme IMAQ Count Objects 2 VI

Step 7. Add the display element of error processing and connect all components according to the diagram (Fig. 40.43).

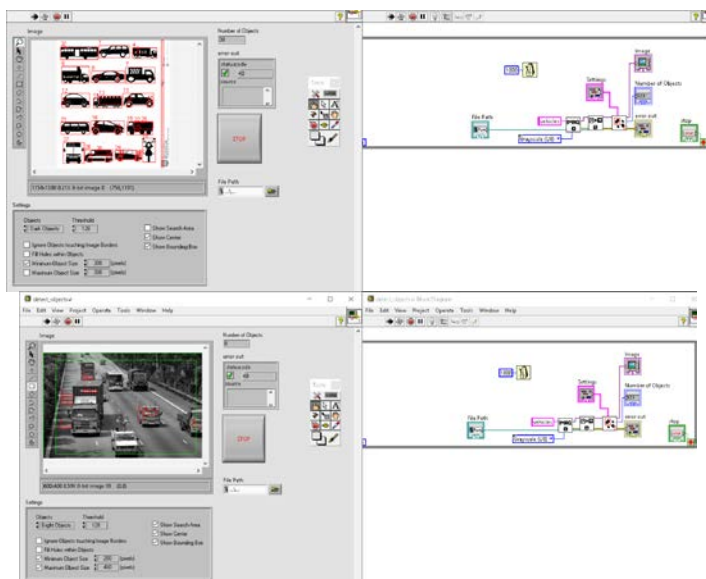


Fig. 40.43 – General view of the system

For the recognition of certain vehicle types, it is necessary to improve the previous scheme in the following way.

Firstly we create the two different objects IMAQ Create VI. The first object (Fig. 40.44, a left side) serves to open the file with cars on the road,

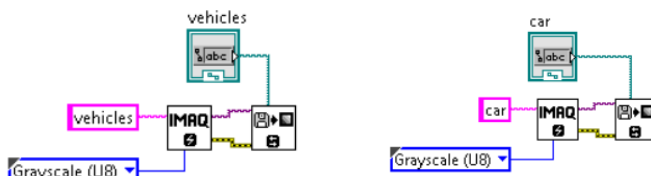


Fig. 40.44 – Improvement of the virtual tool for pattern recognition

the second one is an object of pattern search (the pattern of a particular car). To solve this problem is necessary to use a virtual tool called IMAQ Find Pattern 3 VI (Fig. 40.45).

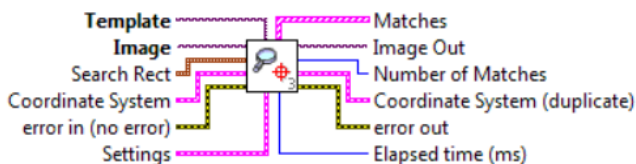


Fig. 40.45 – IMAQ Find Pattern 3 VI

This virtual tool provides a template search in an image rectangular search area. It is not necessary to connect all inputs and outputs for the system work. In this case, the following elements of this virtual tool are important:

Template - is a link to the search image during the comparison process. Template image is an image obtained from the IMAQ Learn Pattern 2 VI output data. If a template is not explored, the virtual tool is initially trained.

Image - link to the original image.

Settings - a cluster that defines the algorithm parameters for template layout and the information which is superimposed on the result image. For example, **Match** defines a technique which is used during the template search in the image and it has the following options: Shift Invariant (0) (Default) - perform a template search in the

image, assuming that it is not turned more than 4 degrees; Rotation Invariant (1) – perform the template search in the image without the rotation limitations of the template.

Number of Matches is the number of templates match found in the main image, based on the input settings.

After that, the data elements (virtual tools) are merged in a form (Fig. 40.46):

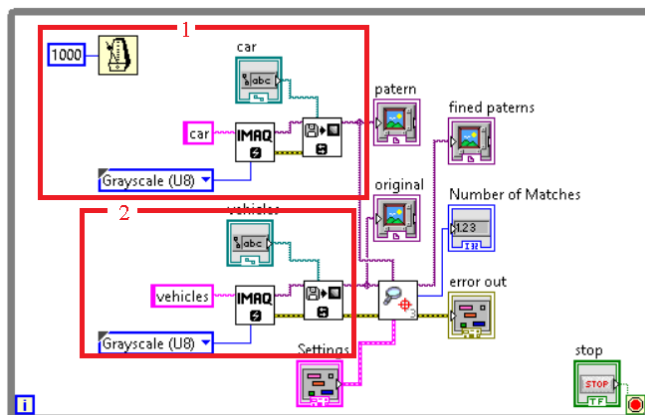


Fig. 40.46 – Connection scheme of virtual tool elements

Template - is a link to the search image during the comparison process. Template image is an image obtained from the IMAQ Learn Pattern 2 VI output data. If a template is not explored, the virtual tool is initially trained.

Image – is a link to the original image.

Settings - a cluster that defines the algorithm parameters for the template layout and the information which is superimposed on the result image. For example, **Match** defines a technique which is used during the template search in the image and it has the following options: Shift Invariant (0) (Default) - perform a template search in the image, assuming that it is not turned more than 4 degrees; Rotation Invariant (1) – perform the template search in the image without the rotation limitations of the template.

Number of Matches is the number of templates match found in the main image, based on the input settings.

After that, the data elements (virtual tools) are merged in the following way(see the Fig. 40.46):

- The processing output of template number 1 connects to the input of Template
- The processing output of the original image number 2 is connected to the input Image
- Error handling results from block 2 are connected to the error processing entry for the virtual tool IMAQ Find Pattern 3 VI
- The pattern indicator connects to Image output Out block number 1
- The original indicator is connected to the Output Image Out of Unit #2
- The fined patterns indicator is connected to Image output Out IMAQ Find Pattern 3 VI
- The Number of Matches indicator connects to the Number of Matches output of the virtual tool IMAQ Find Pattern 3 VI
- Control element Settings is connected to the input Settings of virtual tool IMAQ Find Pattern 3 VI

A Fig. 40.47 shows the results of the system's work. According to it the 3 cars were found and one car was unidentified using one template.



Fig. 40.47 – Result of cars detection on the road (images)

40.3. Recognizing and data processing of objects array in a video stream

40.3.1 Counting the number of vehicles different type that passed through the camera field

To track vehicles in a video stream it is necessary to modify previous examples above with images or create a new virtual instrument. For this purpose, the following modules should be used:

IMAQ Create - requires two modules, the first for original image obtained from the video camera, and second one for search sample.

IMAQ ReadFile VI - to open a sample file

IMAQ Setup Learn Pattern 2 VI - to establish the parameters used during the samples training phase

IMAQ Learn Pattern 2 VI - to create a description of the image pattern for which is necessary to perform search operation during the phase confirmation of pattern matching. The description details are attached to the input image template. During the phase confirmation, the template descriptor is extracting from the image template and it is used to search the template in the inspected image.

IMAQ Setup Match Pattern 2 VI – to set the parameters used during confirmation phase of the pattern match.

IMAQ Match Pattern 3 VI –to search the template or image template in the inspected image.

IMAQ Overlay Rectangle VI - to overlay rectangle into the image for the visual tracking.

IMAQdx Open Camera VI – to open the camera, survey the camera about its capabilities, download the camera configuration file and create a unique link to the camera.

IMAQdx ConFig. Grab VI – to conFig. and start frames capturing.

IMAQdx Grab VI – to read the latest frame in Image Out. This module is called only after initiating the IMAQdx ConFig. Grab VI. If the image type does not match the camera video format, this virtual instrument changes the image type into the appropriate format.

IMAQdx Close Camera VI – to stop the camera operation, remove measurement related resources and close the specified camera session.

An algorithm of assembling this virtual instrument can be described by following steps (Fig. 40.48):

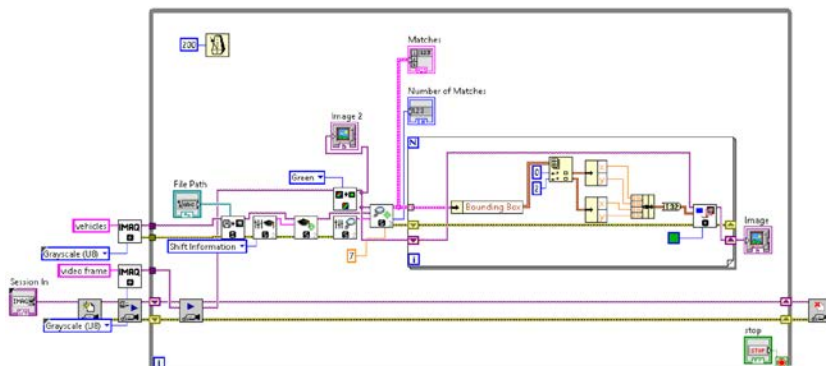


Fig. 40.48 – Block Diagram of virtual instrument for cars detection on the road (video stream)

1. Place two modules IMAQ Create and set the appropriate parameters. For this case it is the name and type of image.
2. Install IMAQdx Open Camera VI and connect it to IMAQdx ConFig. Grab VI
3. Place loop While after these elements
4. Put the element IMAQdx Grab VI into the while loop, it will merge with the element IMAQdx Close Camera VI only
5. Put elements into the while loop and connect them in the following sequence:
 - IMAQ Create VI with IMAQ ReadFile VI
 - IMAQ Create VI (for working with images from video camera) with IMAQdx Grab VI
 - IMAQ ReadFile VI with IMAQ Learn Pattern 2 VI
 - IMAQ Setup Learn Pattern 2 VI with IMAQ Learn Pattern 2 VI
 - IMAQ Learn Pattern 2 VI with IMAQ Match Pattern 3 VI
 - IMAQ Setup Match Pattern 2 VI with IMAQ Match Pattern 3 VI
 - IMAQ ExtractSingleColorPlane VI with IMAQ Match Pattern 3 VI

The interface of this virtual instrument is shown in Fig. 40.49



Fig. 40.49 – The result of the cars detection on the road (video stream)

40.3.2 Determining the coefficient of road filling by vehicles different types

To estimate the state of traffic flows through the road intersections (intensity of the transport environment) it's proposed to use a coefficient that represents a road filling by vehicles. To estimate the filling factor (a first step), is necessary to find the road area size that falls into the range of video camera:

$$S_w = L_w \cdot B_w , \quad (40.2)$$

where S_w , L_w , B_w – respectively, the area, length and width of the road section covered by video camera.

A second step is the evaluation of the area, occupied by vehicles on the road. For this purpose, the results of determination length and width of each vehicle (described in subsection 40.2.3) are used. It should be noted, that in real life vehicles cannot be too tight to each other, and therefore results, obtained in subsection 40.2.3 above, can be supplemented by the distances between vehicles. These distances depend on the speed of vehicles. However, for simplicity it is assumed that they are constant. In such case, the area occupied by vehicles on the road can be calculated by the formula:

$$S_{WEH}^{\Sigma} = \sum_{i=0}^n (L_{WEH}^i + l_{WEH}^i) \cdot (B_{WEH}^i + b_{WEH}^i) , \quad (40.3)$$

where S_{WEH}^{Σ} – the total area occupied by vehicles on the road; i – the current vehicle number assigned during the processing of current frame; L_{WEH}^i – defined in subsection 40.2.3 the length of each vehicle; B_{WEH}^i – defined in section 40.2.3 the width of each vehicle; l_{WEH}^i – distance from one vehicle to another by length (front of one car and back of another); b_{WEH}^i – distance from one vehicle to another by width (side of one car and side of another).

As it was said, values l_{WEH}^i and b_{WEH}^i are constant. Their values are determined by the method of expert evaluations.

After the definition of S_{WEH}^{Σ} and S_W the coefficient K of filling the road by vehicles

$$K = S_{WEH}^{\Sigma} / S_W . \quad (40.4)$$

Formally, it is difficult to estimate the intensity of the transport situation by the K coefficient, especially in a case the speed of passing road intersection depends not only on the "density" of vehicles on the road, but also on the condition of road surface, weather conditions, driver qualifications and other factors.

40.3.3 Processing of video stream for IoT

ThingSpeak is a web service (REST API) that collects and stores sensor data in the cloud to develop the IoT applications. This service supports a work with Arduino, Raspberry Pi and MATLAB for which corresponding libraries are implemented (Figure 40.50). In addition, it works with all kinds of programming languages, because of using the REST API and HTTP.

Figure 40.51 shows an approximate structure of this service, where ThingSpeak and LabVIEW work together.

Further, the stages of creating a virtual tool will be presented in the context of a system for analyzing a traffic on the road and transferring data to ThingSpeak in IoT environment.

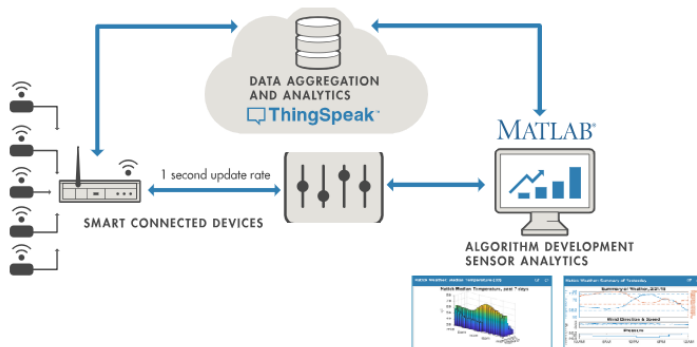


Fig. 40.50 – Structure of the service

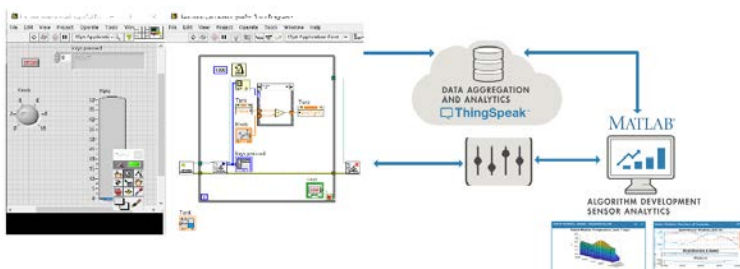


Fig. 40.51 – Structure of ThingSpeak with LabVIEW

For the beginning, it is necessary to create a virtual tool for detecting objects on the road. The creation process has been described above; the working area and the block diagram are shown at fig 40.52.

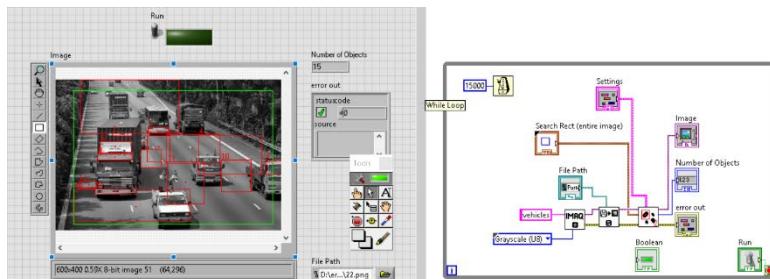


Fig. 40.52 – Car detection VI

Next operation is the registration of ThingSpeak service, after which the user window will be opened (Figure 40.53). To create a channel it is necessary to click on the New channel button, then the channel settings window will be opened. After creating the channel, a channel window opens and configures the access and data transfer on the channel.

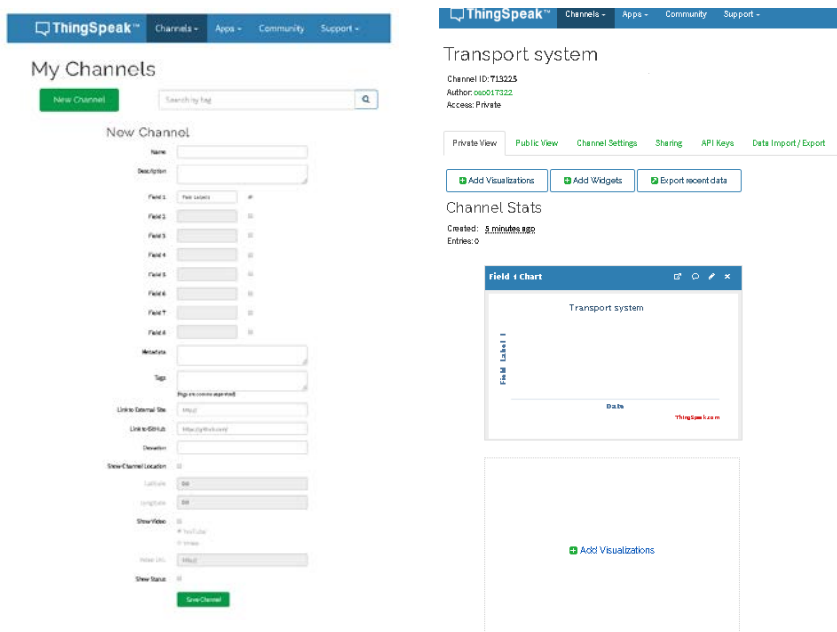


Fig. 40.53 – Channel Setup in ThingSpeak

To transfer data, it is necessary to open Data Export / Import tab (Figure 40.54) and copy the settings how to form a Get request to add data to the server.

Update a Channel Feed

```
GET https://api.thingspeak.com/update?api\_key=YK2GQ28DR44H29WQ&field1=0
```

Fig. 40.54 – GET request to add data to the server

Where the `api_key` is variable channel access key then a `field1` is a variable and the measurement values are recorded, in our case, the number of machines in the frame over a period of time.

For next operation is necessary to modify the previous virtual instrument and it enables sending data (Figure 40.55).

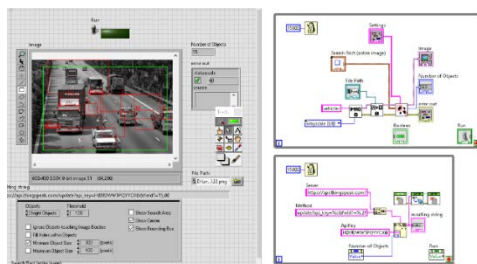


Fig. 40.55 – Modified Virtual Instrument

To do this, we create a separate parallel loop (Figure 40.56).

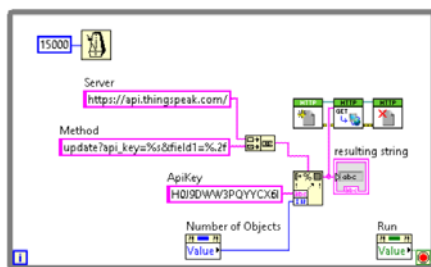


Fig. 40.56 – The separate parallel loop

Then we create a connection to the server using the following blocks OpenHandle VI, GET VI, CloseHandle VI (Figure 40.57)



Fig. 40.57 – Server Connection

OpenHandle VI - Opens the client descriptor

GET VI - Sends a web request and uses the GET method.

CloseHandle VI Closes the client descriptor and also terminates all HTTP connections and exits any authentication.

Since GET VI - Sends only a web request and does not send data, for this needs to modify the request. This is done first by dividing the request into parts (Figure 40.58).

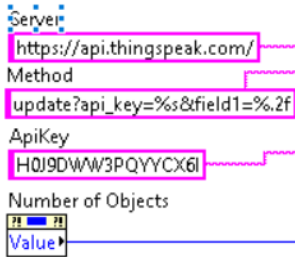


Fig. 40.58 – Split request into parts

A string "Server" contains the server address for data sent, the string "Method" contains the name of script update, the variable `api_key`, the variable `field1`. Those variables were received during creating the channel. The string "ApiKey" is the access code for the update script.

The variable "Number of Objects" contains the number of the cars per time interval.

"Concatenate Strings" and "Format Into String Function" are used functions to concatenate the strings (Figure 40.59).

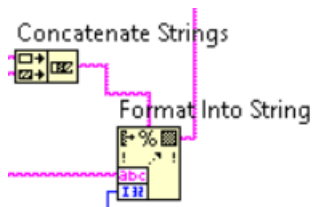


Fig. 40.59 – Concatenate Strings and Format Into String Function

"Concatenate Strings" merges the "Server" and "Method" strings, and then the "Format Into String Function" inserts the key value into "ApiKey" and number value into "Number of Objects". After that the request is concatenating and it can be sent to the server.

Then it is necessary to go to the <https://thingspeak.com/channels/694756>, channel where the number 694756 is generated. It happens when the channel is created as well as displayed in channel settings (Figure 40.60)

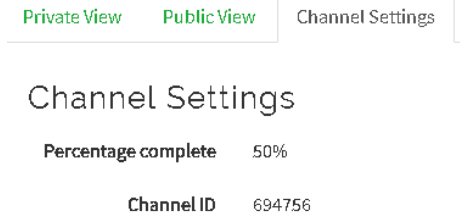


Fig. 40.60 – Channel settings

After the data are displaying, it is possible to analyze it using MatLab programs that are automatically generate, run, and show results (Figure 40.61)

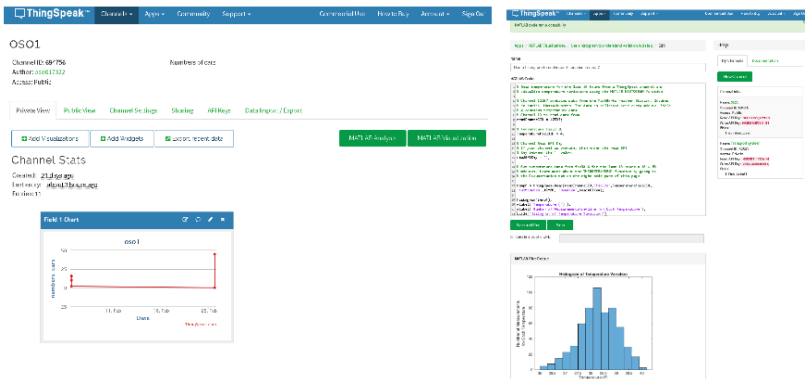


Fig. 40.61 – View the results of tracking the number of cars on the road

40.4 Control system of the traffic flow intensity

Estimate time of vehicles passing through different types of intersections

As it was noted in previous subchapter, the intensity estimation of transport situation using the coefficient K with sufficient reliability is difficult due to the influence of many additional factors. If expert estimation method is used, the different coefficients that partially take into account some factors can be used. However, the reliability of such assessment of the transport situation intensity is quite small. In particular, not all factors, which affect the speed of vehicles, are known, for example, factors of speed of passing through road crossings. At the same time, the parameters of road intersection also have a significant effect on the speed of passing vehicles.

It is suggested therefore to use the neural networks [19] trained on the results of data processing on K passing vehicles through intersections (or complex road sections) where congestion occurs, according to the coefficient of road fill of the transport environment.

At the same time, it should fulfill the following rules:

1. Each neural network can only be used for that crossroads and for the conditions for which it is taught;
2. To assess the time of vehicles passing, each junction carries out a separate group of neural networks;
3. The group of neural networks includes neural networks trained for the daytime (morning, noon, evening) for different weather conditions (sunny, cloudy, foggy, precipitation) and different seasons (with different combinations of weather conditions typical of each seasons).

For training of each neural network, the user has to create a training and test sample. It is advisable to start with a test sample. For its formation it is necessary to obtain not less than 50 marks of the crossing time of different kinds of vehicles (cars, trucks, buses and vans) at different values of the filling factor (from minimum to maximum, characteristic for this crossing). It is expedient to form the study sample by randomly extracting about 20% of vectors from the test sample.

As a neural network, three-layer perceptron should be used [19]. In this case, it is advisable to select no more than 5 hidden neurons of the hidden layer with a sigmoid activation function and one linear output neuron.

Estimate the time of traffic flow, including vehicles of the same type, intersection with the given parameters

When setting up a system that will assess the transport situation within many intersections, that is, when it is integrated into the IoT system, it is very difficult to achieve acceptable results immediately. Indeed, the speed of passage through the traffic flow of intersections (or difficult areas of the road) is strongly influenced by the composition of the traffic flow. For example, a van, when passing the intersection without changing the direction of travel, practically does not have to slow down or interfere with other vehicles. But changing the direction of motion can block a movement across the intersection (for a short time).

Therefore, it is advisable to fix a system of assessing the transport situation first on vehicles of the same type, preferably for passenger cars.

Estimate the time of traffic flow, which includes vehicles of different types, intersection with the given parameters

As it was mentioned above, it is rather difficult to take into account the fact that vehicles in the transport flow are moving, the impact of which can vary greatly at the time of passing through intersections (or complex road sections). Although the training of the neural network can be taken into account partly the difference in the time of passing through, the intersections of different types of vehicles, but the forecast errors of this time are still large. Therefore, it is advisable to take into account the aforementioned difference by setting different values of distances from this vehicle to another l_{WEH}^i and b_{WEH}^i depending on its size.

40.5 Work related analysis

This subsection is based on analysis of both research and educational activities in a field of Intelligent Transportation Systems with IoT using.

Nowadays there are plenty of IoT trends and applications. The scholarly research on the surge of connectivity between computing devices in modern society, as well as the benefits and challenges of this is presented in [20]. It helps to face with a very serious problem like Global warming. New strategies, namely automated driving and connected vehicles, are required to cope with the increased traffic congestion, fuel consumption, and CO₂ emissions. In [21] the vehicle-to-vehicle and vehicle-to-infrastructure communications and accurate positioning systems have proposed as important tools to assist the intelligent traffic management system to regulate traffic and reduce CO₂ emissions.

To optimize transport services, the business development challenges at Intelligent Transportation Systems have described at [22]. In [23] the smart city is considered as an example of context where information, communications, and technology plays the role of enabling IoT in two cases: intelligent transport system and healthcare.

The video surveillance is often used in IoT (the visual Internet of Things) where imaging sensors must achieve a balance between limited bandwidth and useful information when images contain heavy noise. In [24] authors address the problem of removing heavy noise and propose a novel hierarchical extreme learning machine-based image denoising neural network, which comprises a sparse auto-encoder and a supervised regression.

The analysis of traffic flow pattern recognition using long time CCTV image series is considered in [25]. It focuses on testing pre-trained state-of-the-art deep learning neural network systems for car detection using low quality images captured in various environmental conditions. This analysis ultimately exploits machine learning algorithms for a wider understanding of the traffic behavior variations under social events and extreme weather conditions.

The both tracking [26] and multi-target tracking [27] play an important role in many applications such as video surveillance, behavior analysis and human-computer interaction systems, which

allow locating a number of targets, retrieve their trajectories, recognize identities, etc. In [28] a novel robust multi-target tracking method by applying sparse representation in a particle probability hypothesis density of filter framework is proposed. The dictionary learning method and principle component analysis have employed to train a static appearance model offline with sufficient training data.

New types of location-acquisition and mobile sensing technologies enable tracking of vehicles trajectory. However, such applications require massive trajectory datasets. At [29] authors propose a storage method based on the recognition of trajectory patterns to reduce the storage space for the trajectory data.

An efficiency measure for transportation flows is considered in [30]. It enables to analyze large datasets of trip trajectories, and determines how much the dead mileage could be reduced in an ideal setting where the actors collaborate.

In case of wide smartphone usage, the idea of cooperative intelligent transportation systems appears. It fuses measurements and information from vehicles, pedestrians, and local infrastructure within a limited geographical area using smartphones [31].

Vehicular Ad hoc NETWORKS allow communications among vehicles, and vehicles with the roadside infrastructure, namely Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) respectively. In [32] the GreeDi based reactive routing protocol was proposed. It has aimed at selecting the most efficient route in terms of energy consumption between two nodes in Vehicular Ad hoc NETWORKS.

In addition, some universities in USA, Asia and Europe including ALIOT project partners have developed Master and PhD Programs and courses related to Intelligent Transportation Systems with IoT using. In particular, there are:

- Newcastle University, United Kingdom: MSc Programs in Transport Planning and Intelligent Transport Systems (ITS) MSc [33]. This program enables to get a critical awareness of current issues in the ITS field, supported by the latest research.

- Coimbra University, Portugal: IoT course for PhD [34];

- KTH Royal Institute of Technology, Sweden: Doctoral student in Transport Science [35] and Master program in Transport and Geoinformation Technology [36];

- New Jersey Institute of Technology, USA: Intelligent Transportation Systems (certificated program which provides the current and future ITS workforce. One of courses is TRAN 615 Traffic Studies and Capacity [37].

- Wuhan-University of Technology, China: Master in Traffic and Transportation Engineering, to cultivate high-level specialized professionals [38].

- Al-Ahliyya Amman University, Jordan: Master Program in Intelligent Transportation Systems intended to improve the transportation systems efficiency through advanced information and communications technologies and sensors [39].

Conclusions and questions

Based on the material above, it is possible to understand the structures of IoT systems, means of monitoring vehicles and software packages for creating the intelligent transport systems. In addition, we described how the vehicle monitoring systems is using the different tools, in particular:

1. single infrared sensors;
2. a set of the infrared passive sensors;
3. single magnetic sensors;
4. a set of magnetic sensors;
5. webcams;
6. special tracers.

The material above describes the basic tasks of IoT Transportation, the principles of building these systems. Moreover we explain how to create virtual instruments for setting up and calibrating a web camera, processing video stream from a camera, how to use a different image processing methods, filters, how to save processed results.

For a better study of the educational material, we suggested a list of test questions below:

1. What is the Virtual Instrument?
2. What are steps of creating the virtual Instrument for grab video frames?
3. What are steps of creating the virtual Instrument for receiving a video stream?
4. Which modules are making the saving of the video / image

processing results, and how they are connected?

References

1. J. Travis, L. K. Wells, *LabVIEW for Everyone*. Prentice-Hall, 2002, 589p.
2. P. A. Blume, *LabVIEW Style Book*. Pearson Education, 2007, 400p.
3. B. Ehsani, *Data Acquisition Using LabVIEW*. Packt Publishing Ltd, 2016, 150p.
4. B. Mihura, *LabVIEW for Data Acquisition*. Pearson Education, 2001, 480p.
5. J. Jerome, *Virtual Instrumentation Using Labview*. PHI Learning Pvt. Ltd., 2010. 416p.
6. J. Travis, *Internet Applications in LabVIEW*. Prentice Hall, 2000, 601p.
7. D. J. Ritter, *LabVIEW GUI: Essential Techniques*. McGraw Hill Professional, 2002, 562p.
8. Th. Klinger, *Image Processing with LabVIEW and IMAQ Vision*. Prentice Hall, 1 ed. (June 21, 2003), 368p.
9. C. G. Relf, *Image Acquisition and Processing with LabVIEW*, CRC Press, 2003, 264p.
10. K.-S. Kwon, S. Ready, *Practical Guide to Machine Vision Software: An Introduction with LabVIEW*. John Wiley & Sons, 2014. 296p.
11. G. Halfacree, E. Upton, *Raspberry Pi User Guide*. John Wiley & Sons, 2012, 264p.
12. S. Monk, *Raspberry Pi Cookbook*. "O'Reilly Media, Inc.", 2013, 412 p.
13. B. Horan, *Practical Raspberry Pi*. Apress, 2013, 272 p.
14. A. Karapantelakis, J. Markendahl, Challenges for ICT business development in intelligent transport systems. // Internet of Things Business Models, Users, and Networks. 2017. pp. 1-6.
15. R. O. Duda, P. E. Hart, D. G. Stork, *Pattern Classification (Pt.1) 2nd Edition*. Wiley-Interscience, 2000, 688 p.
16. Ya. A. Furman, A. V. Krevetsky, A. A. Rozhentsov, R. G. Khafizov, I. L. Egoshina, A.N. Leukhin. *Introduction to the contour analysis: applications to image and signal processing - 2nd ed.*, M. FIZMATLIT, 2003, 592 p. (In Russian)
17. R. C. Gonzalez, R.E. Woods, *Digital Image Processing*. 3rd Edition, Pearson, 2007. 976 p.
18. W. K. Pratt, *Digital Image Processing*. PIKS Scientific

Inside. 4th Edition. John Wiley & Sons, 2007, 808 p.

19. V.A. Golovko, *Neural networks: learning, organization and application*. Textbook. Editor A.I. Galushkin. M., 2001, 256 p.(In Russian)

20. P. Kocovic, M. Ramachandran, R. Behringer, R. Mihajlovic. "Emerging trends and applications of the internet of things," *Emerging Trends and Applications of the Internet of Things*, 16 March 2017, pp. 1-220.

21. L. C. Bento, R. Parafita, H. A. Rakha, U. J. Nunes, "A study of the environmental impacts of intelligent automated vehicle control at intersections via V2V and V2I communications," *Journal of Intelligent Transportation Systems*, 2019. pp.1–19.

22. A. Karapantelakis, J. Markendahl, "Challenges for ICT business development in intelligent transport systems," *Joint 13th CTTE and 10th CMI Conference on Internet of Things - Business Models, Users, and Networks*. 2018-January, pp. 1-6.

23. A. Ghanbari, A. Laya, J. Alonso-Zarate, J. Markendahl, "Business development in the Internet of Things: A matter of vertical cooperation," *IEEE Communications Magazine*. Volume 55, Issue 2, February 2017, pp. 135-141

24. Y. Yang, H. Zhang, D. Yuan, D. Sun, G. Li, R. Ranjan, M. Sun, "Hierarchical extreme learning machine based image denoising network for visual Internet of things," *Applied Soft Computing*. 2018. pp. 747-759.

25. M. V. Peppas, D. Bell, T. Komar, W. Xiao, "Urban traffic flow analysis based on deep learning car detection from CCTV image series," *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, Volume 42(4), 2018, pp. 565-572.

26. A. N. Bishop, A. V. Savkin, P. N. Pathirana, "Vision-Based target tracking and surveillance with robust set-valued state estimation," *IEEE Signal Processing Letters*. 2010 , Volume: 17 , Issue: 3. pp. 289 – 292.

27. C. H. Kuo, C. Huang, R. Nevatia, "Multi-target tracking by on-line learned discriminative appearance models," *IEEE Conference on Computer Vision and Pattern Recognition*, 2010. pp. 685–692.

28. Z. Fu, P. Feng, S. M. Naqvi, J. A. Chambers, "Robust particle PHD filter with sparse representation for multi-target tracking," *IEEE International Conference on Digital Signal Processing (DSP)*. 2016. pp. 281-285.

29. H. Wang, M. Zhang, R. Yang, X. Lin, T. Wo, R. Ranjan, J. Xu, "SMTP: An optimized storage method for vehicle trajectory data exploiting trajectory patterns," *2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS)*. 2016, pp. 773-780.

30. H. Terelius, K. H. Johansson, “An efficiency measure for road transportation networks with application to two case studies,” *2015 IEEE 54th Annual Conference on Decision and Control (CDC)*. December 15-18, 2015. Osaka, Japan. pp. 5149- 5155.
31. J. Wahlstrom, I. Skog, P. Handel, “Smartphone-based vehicle telematics: A ten-year anniversary,” *IEEE Transactions on Intelligent Transportation Systems*, 18(10), 2017, pp. 2802–2825.
32. T. Baker, J.M. García-Campos, D.G. Reina, S.Toral, H.Tawfik, D. Al-Jumeily, A. Hussain, “GreeAODV: An energy efficient routing protocol for vehicular Ad Hoc networks,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. *14th International Conference on Intelligent Computing*, ICIC 2018; Wuhan; China; 2018. Volume 10956 LNAI, 2018, pp. 670-681.
33. *MSc Programmes in Transport Planning and Intelligent Transport Systems (ITS) MSc* [<http://128.240.233.142/postgraduate/courses/transport-planning-intelligent-transport-systems-i/#profile>]
34. *Doctoral Program in Transport Systems* [<https://apps.uc.pt/courses/EN/course/2041>]
35. *Doctoral student in Transport Science*, KTH Royal Institute of Technology, Dept. of Urban Planning and Environment [<https://www.kth.se/en/om/work-at-kth/lediga-jobb/what:job/jobID:274787/type:job/where:4/apply:1>]
36. *Master's programme in Transport and Geoinformation Technology* [<https://www.kth.se/en/studies/master/transport-and-geoinformation-technology>]
37. *New Jersey Institute of Technology Intelligent Transportation Systems (ITS)*, TRAN 615 Traffic Studies and Capacity 37. <https://www.njit.edu/graduatestudies/degree-programs/graduatecertificates/intelligent-transportation-systems-cert/>
38. *Master in Traffic and Transportation Engineering*, Wuhan-University of Technology, China. <https://www.masterstudies.com/Master-in-Traffic-and-Transportation-Engineering/China/Wuhan-University-of-Technology/>
39. *Master in Intelligent Transportation Systems (ITS)*, Al-Ahliyya Amman University, Jordan. <https://www.masterstudies.com/Master-in-Intelligent-Transport-Systems/Jordan/Al-Ahliyya-Amman-University/>

41. IOT FOR PUBLIC TRANSPORT INFORMATION SERVICE DELIVERING

Prof., DrS. I. S. Skarga-Bandurova, PhD Student M. V. Derkach
(EUNU)

Contents

Abbreviations	374
41.1 Public transport (PT) systems	376
41.1.1. Automatic vehicle location	376
41.1.2 Demand responsive transport and IoT	378
41.1.3 PT priority systems and innovations in transport delivery and operation	378
41.2 Tools and techniques for real-time public transport information acquisition and arrival time prediction based on GPS data	380
41.2.1 Real-time PT information service infrastructure	381
41.2.2 Objective and challenges	384
41.2.3 Arrival time prediction models	385
41.3 PT monitoring, analysis, and management	388
41.3.1 General strategy of PT information service delivering and sharing	389
41.3.2 Information boards, ETA/ETD on bus-stops	389
41.3.3 Implementation of ITS to support the principles of demand management	391
41.3.4 Cases	392
41.4 Work related analysis	395
Conclusions and questions	397
References	399

Abbreviations

IoT – Internet of Things

ITS – Intelligent transport system

GPS – Global position system

GSM – Global System for Mobile Communications

CDMA – Code Division Multiple Access

API – Application programming interface

ATS – Average travel speed

RFID – Radio Frequency Identification

RPM – Red Hat Package manager

ISO – International Organization for Standardization

TR – Technical Reports

VPN – Virtual Private Network

ETA – Estimated Time of Arrival

ETD – Estimated Time of Departure

HTTP – Hypertext Transfer Protocol

MAE – Mean absolute error

MAPE – Mean absolute percentage error

RMSE – Root-mean-square error

APE – Absolute percentage error

AD – Absolute deviation

TANS – Trolleybus arrival notification system

cURL – Client Uniform Resource Locator

ID – IDentification

SMS – Short Message Service

Road traffic requires accurate and up-to-date information about the current situation and available services. The enhancement of the road conditions is essential to all infrastructures. However, only this improvement cannot meet the continually growing demands for safe, convenient, cost-effective, and comfortable road services.

In this context, public transport information service is one of the essential parts of intelligent transport systems (ITSs) aimed to make transportation system safer and more efficient. It provides the real-time travel information according to the people needs through appropriate tools. As mentioned in [1], applying ITS delivers several benefits by increasing traveler safety, improving the operational performance of the transportation network, mainly by reducing the traffic jam, enhancing personal convenience, providing better environmental conditions, and expanding economic and employment growth.

The emergence of the Internet of Things (IoT) adds new zest to ITS. IoT deals with different physical objects merging their data in a network in one form or the other. It mainly deals with RFID, infrared sensors, global positioning systems (GPSs), and laser scanners.

Electronic recorders in the vehicles can track and record the acceleration, speed, engine RPM (rotational speed of the crankshaft of the engine), and other parameters, and this information generated by traffic IoT and collected on all roads can be presented to fleet managers, travelers, and other users. Hence, ITSs, as well as IoT in ITSs, allow deploying the advanced transport systems that enable vehicles to share data about their positions so that the passengers aware the availability of their buses and trains in real time [2]. However, dependable and real-time communication in the scope of developing intelligent transport infrastructure is still a critical challenge and needs to be tackled for the success of its applications.

The current engineering practice for the development of such systems includes a set of different methodologies and therefore needs carefully designed approaches. Construction public transport information service infrastructure requires enforcement of existing standards in data collection, transmission, processing, and dissemination of information, and ensuring consistent service quality, which is fundamental to their convenient usage by people.

41.1 Public transport systems

The public transportation (PT) information service infrastructure is a part of the core functionality of intelligent transportation systems (ITS). The definition public transport includes three main groups of public transportation [3]:

- general public transportation that is offered to all people based on timetables and routes;
- special public transportation offers services to a specific group of people (e.g. pupils, people with disabilities);
- tourist and charter traffic that is offered to all citizens.

It is possible to categorize public transportation into local, regional and interregional traffic. Public transportation can be operated with road-based vehicles (buses, trolleybus), rail-bound vehicles (e.g. trams, trains, metro), on water (e.g. ferries) or air.

Thus, not only bus and rail networks, stations and vehicles are part of a PT system but also the information and organization. Both the journey itself and the pre-trip planning take place within the PT system. The term therefore also includes information such as in timetables, web based travel planners, announcements in vehicles or at stops or other strategically and tactical information about how to use PT.

41.1.1. Automatic vehicle location

Automatic Vehicle Location (AVL) Systems give an agency the ability to track, record, and analyze how vehicles are performing in real time [4]. These features lead to improvements in public service through better on-time performance and quicker response time to emergencies.

Currently there are four types of AVL systems in service that have been utilized for locating vehicles. They are:

- global positioning satellites;
- signpost technology;
- ground based radio;
- dead-reckoning.

The most popular Automatic Vehicle Location system, based on data supplied by the Federal Transit Administration, is Global Positioning Systems.

Automatic vehicle location systems are comprised of three elements. The first element is locating hardware, which is the component necessary to identify the position of a vehicle on the earth's surface. The next is the communication package, which takes the positional data and relays it back to the central office. In addition, the final element is the computer display system, which reveals the location of the vehicle as it travels in real time. Communication packages used in AVL systems consist of one of the following classifications:

- analog radio;
- digital radio;
- analog cellular;
- digital cellular;
- satellite technology.

The most commonly used of these communication systems is trunk analog radio. Although it is more cost effective when compared to the other types of communication packages it currently requires longer transmission times and additional hardware when used in an AVL system.

Computer display systems assist in the transformation of raw data from the field to a graphical representation in the office. Many of these systems perform additional features that further improve the reliability and usefulness of an AVL package. These include the best route or shortest path features, turn-by-turn route guidance instruction, and interpolating field data to match mapped streets. The last feature takes a vehicle's position and matches it to the closest street. This eliminates the errors that normally might place a vehicle in the middle of a block and not on the roadway.

Automatic vehicle location systems are also part of a group of technologies called Advanced Public Transportation

Systems or APTS. These are components that when used alone or with an AVL systems provide additional services to riders and the agency. The following is a list of the individual categories that these technologies fall under, including:

- fleet management and operation systems;
- traveler information systems;
- electronic fare collection systems;
- traffic management systems.

41.1.2 Demand responsive transport and IoT

A vehicle in a Demand Responsive Transport (DRT) is shared among passengers who decide where it stops to pick up or drop off users [5, 6]. The original goal behind DRT was to help disabled or elderly people, but nowadays can be regarded as a viable means to increase access and flexibility in public transport for the whole community. Bus routes acquire dynamicity and flexibility as the passengers can decide them. The only bus stops to be visited could be only those where the travelers want to exit and those where people are actually waiting. This would ensure more sustainability due to improved coverage and higher accessibility.

The public transport alternatives enabled by DRT could, in the long run, lead to a reduction in indirect emissions, this being be the consequence of a more attractive and adaptive service capable of acquiring more users. Emissions could be potentially reduced by appropriately implementing the service in such a manner as to allow buses to take shortcuts, hence avoiding stops without awaiting users, or to employ smaller and fuel-efficient buses when demand is expected to be low.

The implementation could also consider advising passengers to reach the closest bus stops to minimize their waiting time or to catch a fast transport service. IoT can be fully leveraged only if, in addition to the public transport operator, also a variety of other different actors are involved, such as telecommunication operators, sensor data providers, data storage providers, end-user service providers, public authorities, and the travelers themselves.

IoT not only benefits traditional public transport operators through enabling innovative services and better decision making, but might also create opportunities for transport-related services.

41.1.3 PT priority systems and innovations in transport delivery and operation

Public Transport Information and Priority System (PTIPS) enhance bus service reliability by providing traffic signal priority; and

informing passengers and service providers with real-time bus information, performance and their location [7].

PTIPS consists of global positioning systems and radio data communications that deliver information about buses and their location. This information is used to forecast the arrival time of buses at traffic signals. If a bus is running late, it can be given priority by altering the timing of the traffic signals using user defined business rules built into PTIPS.

PTIPS is an integral part of enhancing public transport performance and enabling passengers to make informed and easier journey decision-making.

Buses are tracked via satellite and their locations are then displayed on a map in real time. This recorded information can then be played back at any time. There is also a wide range of alerts available within the system to help improve service delivery. The system is highly customizable to suit the needs of individual users.

The bus tracking information can also be filtered according to the intended audience.

For example, bus operations can only see buses in their region of operation, whereas PTIPS enables a more global approach where all buses in the network can be tracked.

When a bus is running late, it can be given priority over other traffic by giving it a green display at traffic signals. This is done in conjunction with the Sydney Coordinated Adaptive Traffic.

The rules that allow priority are fully configurable, but at no time is traffic signal ever compromised.

The benefits of PTIPS include:

- enabling buses to maintain their scheduled timetable;
- giving bus passengers a more reliable service;
- keeping bus passengers informed of delays or cancellations;
- enabling bus operators to schedule their buses more effectively;
- service delivery planning.

As a result, such innovative solutions are being introduced:

- Transportation Systems and Services: providing intelligent transportation that creates operational efficiencies for Electronic Toll

Collection, Commercial Vehicle Operations and Motor Vehicles Services;

– Public Transport: Fare Collection Solutions for advanced technologies including smart card applications, ticket vending machines, and bank card solutions for mass transit;

– Parking and Safety Solutions: Customized for On and Off-Street Parking and Photo Enforcement to efficiently manage programs and strategies for municipal programs.

41.2 Tools and techniques for real-time public transport information acquisition and arrival time prediction based on GPS data

Everyone is in hurry to reach their destination in this fast life. In this case waiting for the buses is not reliable. People who rely on the public transport their major concern is to know the real time location of the bus for which they are waiting for and the time it will take to reach their bus stop. This information helps people in making better travelling decisions. Current position of the bus is acquired by integrating GPS device on the bus and coordinates of the bus are sent by either GPRS service provided by GSM networks. Nowadays, by the use of wireless communication, global positioning system and other devices, passengers are able to get information about the arrival time of the transit vehicle.

As a GPS tracking system, Wialon Hosting is used. Wialon is a fleet management system [8], also served for tracking moving and stationary objects, observing dynamic changes their parameters, e.g., travel speed, voltage, temperature, etc. Information about geographic coordinates of a vehicle, travel speed, and sampling time in coordinated universal time is displayed in real time and saved in the database. The row of the database table corresponds to the point on the map. The fields in this row are latitude, longitude, speed (m/s), time, and route number. An example row is:

```
'38.4522149 ', '48.9351065', 5, '09: 00: 53 ', '6 '
```

These data are used for further calculations. It is assumed that a system provides measurements with a maximum error of 10 m under fair weather conditions and when the GPS receiver can acquire the signal from a minimum of four satellites

For working with Wialon RemoteApi, the library cURL can be deployed. It provides functions for generating requests for the vehicle identifier on spatial and temporal coordinates and entry them into the database. A new entry is done as follows:

```
$result = $wialon_api->login($token);
$json = json_decode($result, true);
if(!isset($json['error']))
{
$result=$wialon_api-
core_search_item('{ "id":14157051,"flags":1024}');
$jn_result = json_decode($result, true);
$jn_x = $jn_result['item']['pos']['x'];
$jn_y = $jn_result['item']['pos']['y'];
$jn_s = $jn_result['item']['pos']['s'];
$time = date('H:i:s');
$result = mysqli_query ($db, "INSERT INTO tr
(id,x,y,s,time)
VALUES('14157051','$jn_x','$jn_y','$jn_s','$time)");
$wialon_api->logout();
}
else echo WialonError::error($json['error']);
```

41.2.1 Real-time PT information service infrastructure

As a part of the core functionality of ITS, a real-time public transport information service infrastructure includes fleet management, dispatching and scheduling services, emergency alerts, security services, and passenger information services. Figure 41.1 shows how the different subsystems are organized and interact with each other.

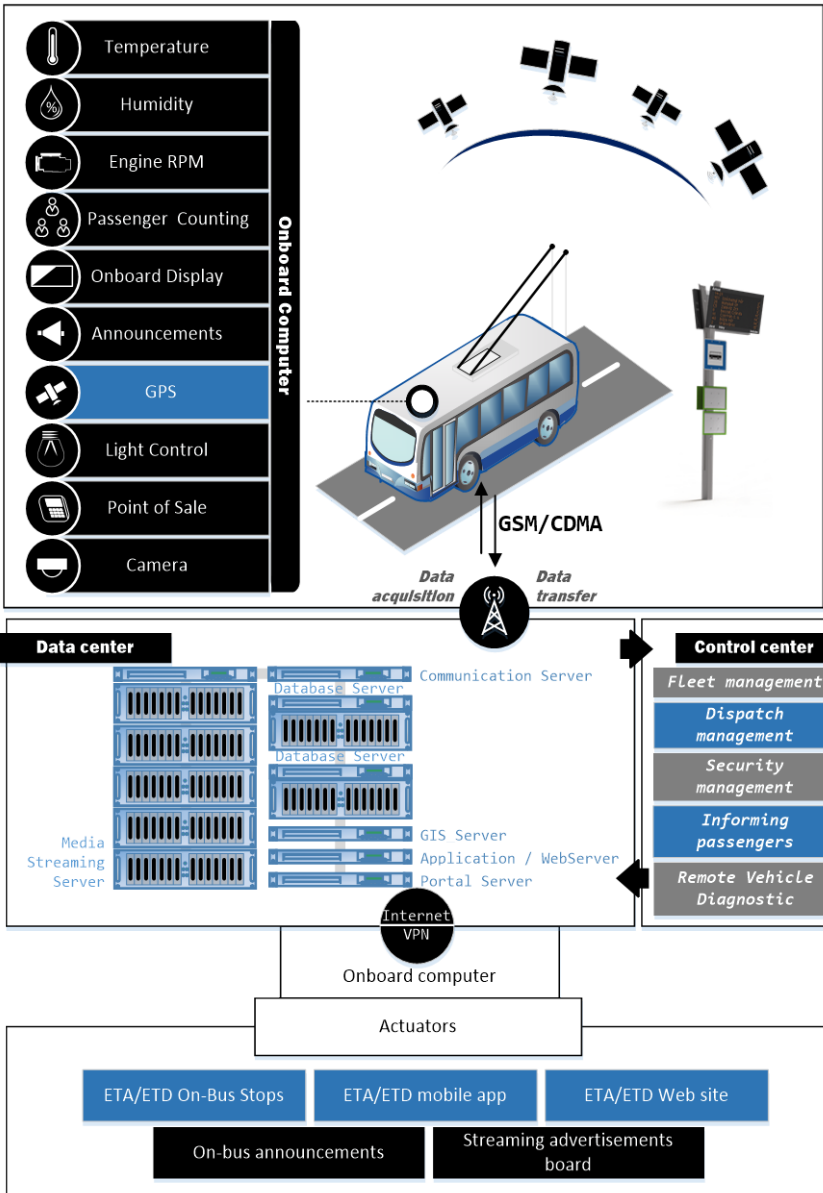


Fig. 41.1 – Real-time public transport information service infrastructure

The model is based on international ITS architecture model standards ISO/TR 14813-2:1999(E) and ISO 14813-1:2015 and provides a framework for the constant enhancement of these systems, giving desirable properties such as dependability, flexibility, and integration [9–11]. This infrastructure is designed to enhance the passenger information services and realize the people-centered paradigm by focusing on services for passengers.

Passenger information services include message boards and kiosk boards at bus stops, web-based information services to deliver information about the public transport routes, scheduling, ticket information, estimated time of arrival/estimated time of departure, on-bus announcements, etc.

Figure 41.2 shows the interaction between the forecasting system and the overall ITS infrastructure. It includes the layer for GPS data acquisition from the sensors installed in the vehicle; the data processing, and data analysis layer where the calculations of the predicted arrival time are performed; and means for delivering information to passengers by information boards and smart-phones.

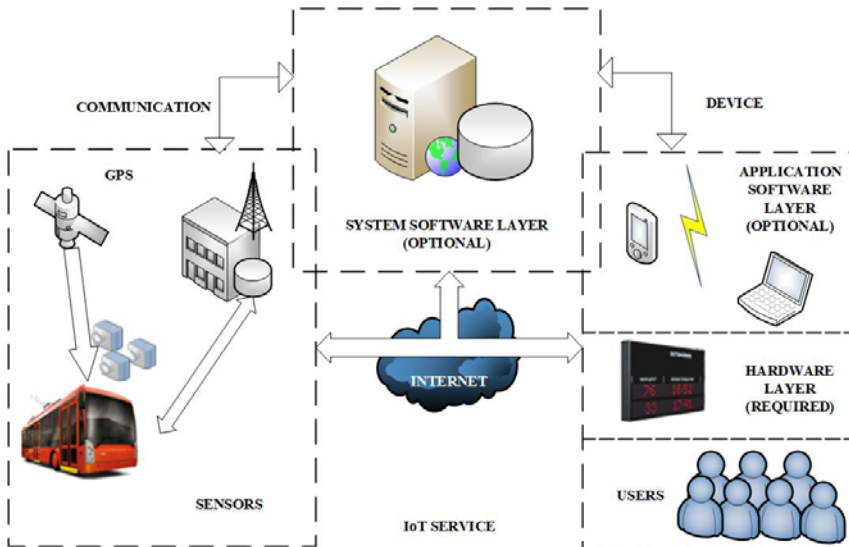


Fig. 41.2 – The interaction between the forecasting system and the overall ITS infrastructure

Providing an accurate arrival time is a fundamental task for efficient operation of public transport companies. The punctuality brings a vast improvement in public transport services. However, it is still a challenging task to find the best method to predict the accurate vehicle arrival time and as with anything better is a matter of the particular application.

41.2.2 Objective and challenges

The main tasks are:

- collection of GPS data from sensors installed in the vehicle;
- processing and analysis of data, where the calculations of the predicted time of arrival;
- providing information to passengers with information boards and smartphones.

Tasks are limited by requirements — real-time data processing, data availability, security, predictability, low power consumption, and many others.

The data acquisition, information processing and displaying strategies are described in the following flow chart (Fig. 41.3).

For our purposes, we can introduce the concept of a segmentation that is represented by the distance between two adjacent checkpoints (stops) with one or several bus stops. Thus, the segment notion provides a useful flexibility of real-time information to the passengers. The prediction of trolleybus arrival time at a certain checkpoint, in this case, is equal to the forecast of travel time as follows

$$T_{a,j} = T_{d,i} + t_{ij} \quad (41.1)$$

where $T_{a,j}$ denotes trolleybus arrival time at a certain checkpoint (stop) j ; $T_{d,i}$ is the time of departure from the checkpoint i ; t_{ij} is travel time between checkpoint i and checkpoint j . It is assumed that, there may be one or several bus stops between i and j . The remaining calculations are performed in accordance with proposed methodology in next section.

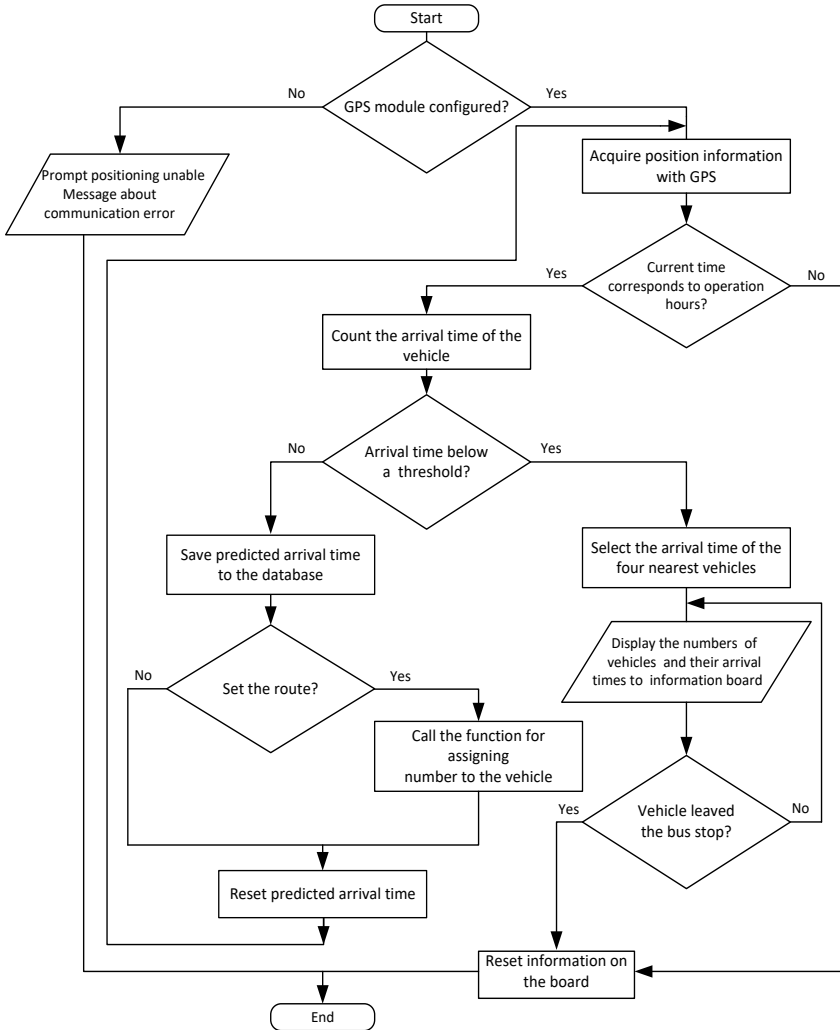


Fig. 41.3 – The algorithm of data acquisition and calculating the arrival time prediction of the vehicle

41.2.3 Arrival time prediction models

The following technique is proposed for predicting arrival time.

1. Fix the number of time slots n , passed by the vehicle during the traveling time from the start point to the current location:

$$n = \frac{T - T_0}{I}, \quad (41.2)$$

where T is a real-time value, T_0 is a time of departure, I is a unit of measured time-span.

2. Determine the average travel speed between two consecutive stops

$$s = \frac{\sum_{i=1}^n s_i}{n}, \quad (41.3)$$

where s_i is an actual speed of vehicle at a point in time i , i denotes a current time slot, n is a number of time slots throughout vehicle movement from the start point up to the current time slot.

3. Compute the distance from vehicle current location to the bus stop.

Information about vehicle position is acquired from a GPS module, and then these values can be used to calculate the distance between the current and a fixed waypoint. The distance between current locations and a bus stop can be computed at least in two ways via haversine formula [12, 13] and Vincenty's method [14]. The current approach suggests that the distance d between two consecutive points can be computed from a haversine formula as follows

$$d = \Delta\sigma \cdot R, \quad (41.4)$$

where R is the radius of Earth (6378.1 km), $\Delta\sigma$ is the angular difference.

When it comes to measuring relatively short linear distances between two geographic positions, the angular difference $\Delta\sigma$ is calculated by using haversine formula as

$$\Delta\sigma = 2 \arcsin \left\{ \sqrt{\sin^2 \left(\frac{\varphi_2 - \varphi_1}{2} \right) + \cos \varphi_1 \cos \varphi_2 \sin^2 \left(\frac{\Delta\lambda}{2} \right)} \right\}, \quad (41.5)$$

where $\varphi_1, \lambda_1; \varphi_2, \lambda_2$ indicate the latitude and longitude of point 1 and point 2, respectively; $\Delta\lambda$ – is the longitude difference between two consecutive points.

Haversine formula ensures a more straightforward computation, but it does not provide the high accuracy. The Vincenty's method can be utilized as an alternative to haversine, providing sufficient accuracy for any pair of points but it is also more computationally intensive and, therefore, performs slower and increase battery usage. That why the haversine formula may be considered as a basis for calculating the distance between two points for IoT applications. In Android, the haversine formula is used in Google Map Utils [15].

The second way is to utilize the Google Maps API. It provides information about the real-time location, the distance calculation providing mapping GPS coordinates and getting routes between numbers of points on a map. It is available for Android, iOS, web browsers and via HTTP. In particular, Service Google Maps Directions API allows you to calculate routes between two known points using the HTTP request [16]. However, the Google API does not allow determining the external boundary based on time or distance from a location.

4. Calculate the expected arrival time of the vehicle to the particular bus stop according to the values of distance and speed obtained at the previous stages

$$t = \frac{d}{s}, \quad (41.6)$$

where t denotes the expected arrival time of the vehicle, d is a distance between two points, s is averaged speed of vehicle.

The remaining distance is divided by the speed previously measured to roughly estimate the arrival time.

Since the distance between the control points of the route often can not be measured as the length of the straight line between these points, each route has been broken into smaller segments with the additive lengths, getting the distance between the control points

$$d = \sum_{i=1}^N d_i, \quad (41.7)$$

where d_i denotes the distance between additional points in d , i is a segment index, N is a number of control points.

41.3 PT monitoring, analysis, and management

Public transport is a service available on sharing basis for the benefit of general public. It includes city buses, trolleybuses, trams, passenger trains, ferries and rapid transit like metro and subways.

The main reasons why the people choose public transportation over other modes of transport are its subsidized rates, environment-friendly attributes and easy accessibility.

Firstly, public transport is very economical allowing a large population to have access to it. Using a bus or a train to commute is comparatively cheaper than using a private car.

Secondly, public transport can preserve the environment by reducing the amount of pollution.

With an increase in the use of public transportation, there will be a reasonable dip in the number of private vehicles on the road, therefore, improving the environment and in addition, solving the traffic congestion issue [17, 18].

Taking into consideration the other aspects of public transportation, there are some downsides to this service as well. Public transportation, by its very nature, is far more time consuming than any other mode of transportation. Most trains and buses run in accordance with a scheduled timetable.

However, these time schedules are seldom followed. There is always an uncertainty regarding the arrival of a bus. Often, buses break down causing further problem to commuters. Another pitfall we see is that public transportation often lacks organization.

The opportunities to improve existing public bus transportation by embedding advanced technology into real time transport system is provided by internet of things.

Internet of things is interred -networking of physical devices with electronics and network connectivity that control these objects to collect and exchange data. IoT is not only used to sense the information but also to interact with the physical world. IoT can assist in integration of communication, control and information processing across various

transportation systems. Internet of things is used to provide Interaction between the passenger and bus by means of internet.

41.3.1 General strategy of PT information service delivering and sharing

In order to provide necessary bus data to all passengers, we propose an information system where all relevant information of the bus will be gathered, processed, and presented to the user [18].

New application and business are created continuously with the help of technology through internet. With the development of wireless technology and internet of things, smart devices are more popular in our daily life than ever before.

We use these devices recording our daily life, monitoring personal status, and tracking objects.

To adjust and ensure the availability of information system, the following steps are required:

1. Ensure the remote access to the GPS for obtaining spatial and temporal coordinates of the vehicle.
2. Collect information from the sensors on the location and travel speed of each vehicle included to the system. Add sensor data to the database. The sensors are surveyed during the working day.
3. Assign the routes to vehicle (once at the start of working time).
4. Calculate the predicted arrival time of the specific vehicles for the specified bus stops (check-points). This task is performed for each vehicle, and the result is recorded in the database by their route.
5. Display the information about nearest vehicles at the bus stop information board. The vehicle number and minimum arrival time for the bus stop are taken from the database concerning their predicted values.

41.3.2 Information boards, ETA/ETD on bus-stops

Information board is a central point of alert passengers about the time of arriving public transport to the bus stops. As a rule it displays the time; destinations and bus numbers or routes of vehicles arriving at the particular stop; they help to orient in space, plan your trip, taking

into account the traffic in the city, save the time and improve orientation of people in the city.

The IoT boards working in real-time mode are activated by prior detection of arriving vehicles to the stop and can display predicting arrival / departure time [19].

After collecting and analyzing the data, the prediction of the arrival time is stored in the database on the server, for output of which the information board formerly generates a request to the forecasting server through the Wi-Fi module based on ESP8266 and Internet punctures, the response is parsed.

To make the simplest information board you need the following components (see Fig. 41.4):

- LED modules (320×160 mm, 32×16 dots, IP65, 2000 nt);
- Wi-Fi module based on ESP8266;
- power supply 5V 40A 200W.

To manage this simple information board, you need to write a sketch using the ArduinoIDE software, and then embed it into the microcontroller's internal memory.

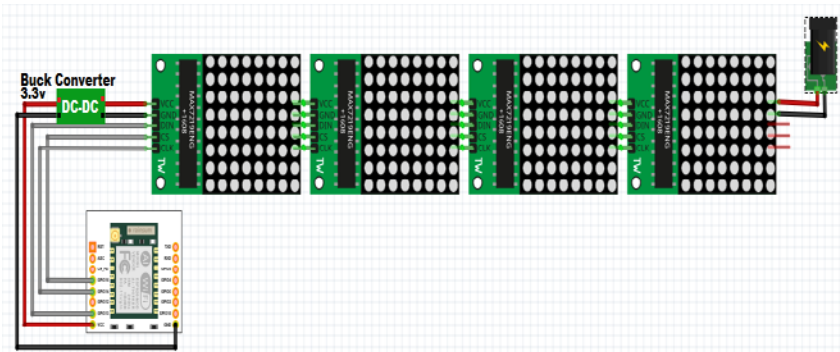


Fig. 41.4 – Wiring diagram of the information board components

Since the interaction between the server and the client, such as web application and the information board microcontroller, is performed using HTTP requests, the client application forms a request and sends it to the server.

The server software processes this request, forms a response and sends it back to the client.

The following snippet demonstrates the initiating this request:

```
void getTime()
{
  WiFiClient client;
  if (!client.connect("www.google.com", 80)) {
    Serial.println("connection to google failed");
    return;
  }
  client.print(String("GET / HTTP/1.1\r\n") +
              String("Host: www.google.com\r\n") +
              String("Connection: close\r\n\r\n"));
  int repeatCounter = 0;
  while (!client.available() && repeatCounter < 10) {
    delay(500);
    //Serial.println(".");
    repeatCounter++;
  }
}
```

41.3.3 Implementation of ITS to support the principles of demand management

Intelligent Transportation Systems (ITS) domains include many areas as public transportation control framework, road traffic management and the application of traffic control [20]. Vehicle monitoring and transportation management systems fall under the category of ITS.

Intelligent transportation systems enable various technologies to be applied in management of transportation and are defined as the use of information and communication technologies to collect, process, and transmit traffic data to transport users and operators. Vehicle monitoring systems, however, only take vehicles into account; for example, autolocation systems can be applied to vehicle monitoring, vehicle control, and vehicle management.

Public transport companies use the provision of real-time information through innovative information systems. As a result, receive customer satisfaction. Opportunity to increase income can be a long-term gain if measures lead to increased demand for public

transport. In addition to information about vehicles, these systems can also be used for fleet management.

41.3.4 Cases

As a part of public transport arrival notification system, an experimental study has been conducted in Severodonetsk, Ukraine. A multifunctional system for monitoring mobile and stationary objects based on GLONASS and GPS satellite navigation systems, the Wialon system, is under development now. First stage will be finished soon for trolleybus fleet. It is already equipped with GPS devices. This pilot project is designed to enhance the passenger information services realizes the people-centered paradigm by focusing on services for passengers. Passenger information services include message boards and kiosk boards at bus stops, web-based information services to deliver information about the public transport routes, scheduling, ticket information, Estimated Time of Arrival / Estimated Time of Departure, on-bus announcements, etc.

Let's assume that mathematical model of the city's street layout transport network is given by a graph:

$$G=(U, E), \tag{41.8}$$

with set of nodes:

$$U = U_1 \cup U_2 \cup U_3 \cup U_4, u = |U|, \tag{41.9}$$

set of arcs:

$$e = |E|, \tag{41.10}$$

where U1, U2, U3, U4 - set of nodes first, second, third and fourth type, u - number of nodes, e - number of arcs, |.| - power sign set.

Arcs are sections of roads between nodes, which in turn form a route. Routes are given by the matrix:

$$R = \left\| r_{i,j} \right\|_{u \times u}$$

$$i, j = \overline{1, u}$$

$$i \neq j, \tag{41.11}$$

and allows assigning the route to the trolleybus when it gains the specific zone.

The assignment of the route is very simple and is as follows. In the first route, at the beginning of the working day, arrival time calculations are not performed. The objective of this phase is to fill an array of data with trolleybus IDs and numbers of geo-zone rooms where they have entered.

When a vehicle crosses a specific geo-zone, it is assigned a route. The assignment algorithm is shown in Figure 41.6.

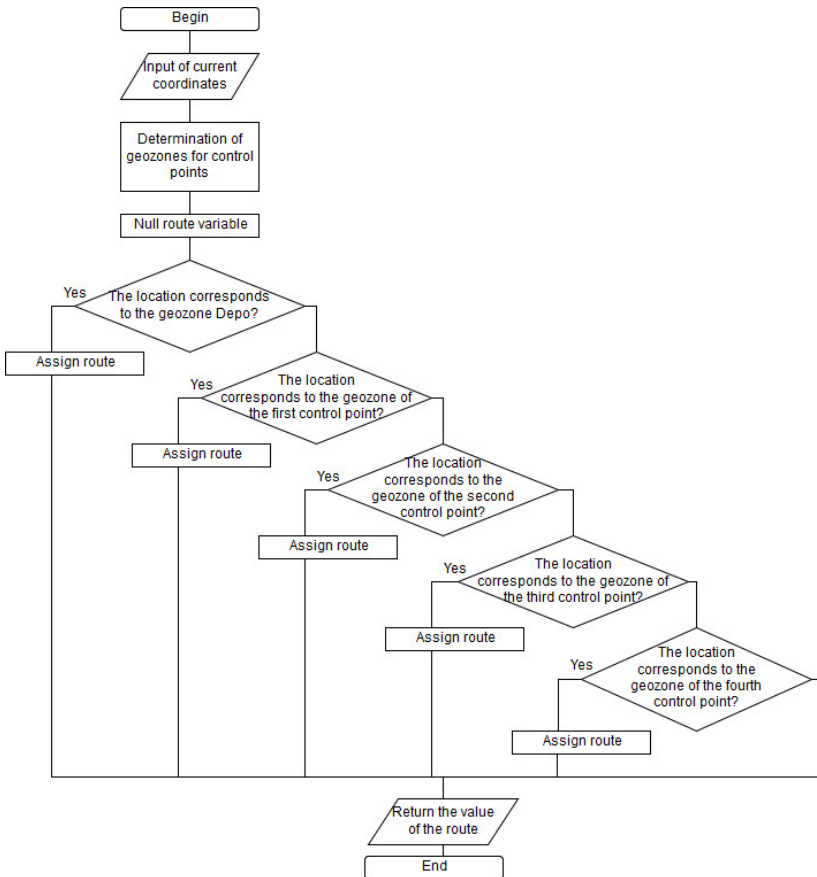


Fig. 41.6 – The algorithm for setting route number to the vehicles

The trolleybus number and minimum arrival time for the bus stop are taken from the database concerning their predicted values. The bus stop information board is limited to 4 rows; thus it seems reasonable to display four nearest incoming trolleybuses.

To better prediction accuracy, it is necessary to keep calculations updated every 15-30 seconds as the new information received.

41.4 Work related analysis

Information systems based on real-time forecasting models are widely used all around the world many of these systems have been deployed throughout the Europe and USA. London Buses' Countdown system began their operation in the early 1990s providing different information services for passengers; the algorithm for time estimation of arrival of the public transport was deployed in Blacksburg, Virginia; the Department of Transportation of Los Angeles has developed a forecasting algorithm within the framework of rapid transit services, called Metro Rapid; in Washington DC, an ad-hoc algorithm was developed for predicting the arrival for King County Metro (Seattle); the Singapore Land Transport Authority (LTA) uses drivers' smart-phones as traffic sensors to deliver personalized real-time traffic information.

Many universities worldwide, including ALIOT project partners, conduct research in the framework of the direction of the Internet of Things and Intelligent Transport Systems. The dynamics of work can be observed on the basis of the works of researchers. Developing traffic control strategies taking explicitly into account the route choice behavior of users has been widely recognized, as a very complex problem, which is considered by scientists of the University of Luxembourg and KU Leuven. In paper [21], the authors proposed an extended decomposition scheme for the anticipatory traffic control problem, based on our previous contributions, which are aimed at:

- reducing the computational complexity of the problem, approaching it on a “controller-by-controller” fashion;
- internalizing specific constraints in the objective function that guide the optimization process away from non-significant minima, such as flat regions.

The article [22] presents the research of authors from the University of Newcastle upon Tyne, aimed at identifying features that make In-vehicle navigation systems user-friendly and suitable for older drivers. The study of navigation characteristics is focused on using information about routes, current location, and estimated time of arrival at the next destination on the most appropriate method of presenting information (audio only, visual only or combination of audio and video). It also assesses potential gender differences that may arise with oriented navigation information. Another problem solved by many scientists, in particular, Erik Jenelius [23] from the KTH Royal Institute of Technology, bus crowding. The task is based on real-time vehicle location and passenger count data and evaluates the performance of a data-driven lasso regression prediction method. Another area of study of the same university is the light rail train system. The paper [24] develops and tests two forecasting schemes for railway systems that are based on building channel-specific speed profiles. The area of study also addresses the problem of crowding prediction [25] based on real-time load data and evaluates the effectiveness of several prediction methods (stepwise regression, lasso, and strengthening of tree ensembles) for metro lines. Prediction accuracy is estimated from passenger traffic and predefined discrete crowded levels. In general, a group of scientists [26] from the KTH Royal Institute of Technology is working on the use of heterogeneous data sources to analyze the multimodal effects of disruptions in the transport network. They develop a data-based systems approach that is proposed for impact analysis in relation to two aspects:

- changes in the space-time network;
- multimodal effects.

Several issues are being considered, including the definition of affected areas and the assessment of the impact on network performance, demand structure and public transport system performance. A methodology and system architecture for predicting the transit time of an integrated urban road network is also being developed based on real-time low-frequency vehicle probe data [27]. Developments include managing network traffic, routing, forecasting network transit times, and providing information using maps and the conclusion of the path, the estimated time of passage of the line by the vehicle.

Scientists from EU universities (Technical University of Denmark, KTH Royal Institute of Technology, and University of Coimbra, Massachusetts Institute of Technology) are also working together, namely, developing a Bayesian additive model with Gaussian components of the process, which combines records of smart cards from public transport with contextual information about events, which is constantly extracted from the Internet [28]. This is an efficient algorithm that uses wait-propagation and makes it possible to predict the total number of travelers by public transport, thereby creating a more adaptive transport system. Understanding public bus behavior is important for the future development of personalized transport information systems such as travel forecasting systems. This is confirmed by a study [29] which shows that there is regularity in the use of buses and that daily bus trips can be predicted with a high degree of accuracy. Also, there are spatial and temporal factors that affect the bus predictability of use. These influential factors include the frequency of use of the tire, the number of bus lines and stops used, as well as travel time. The study [30] also provides a clear proposal for effective, sustainable transport planning aimed at maintaining an environmentally friendly environment and road safety, which in turn will lead to the creation of a sustainable transport system.

Conclusions and questions

In this section, the materials for Industrial training module “IoT for intelligent transport systems” are presented. It can be used for preparation to lectures and self-learning.

Advanced public transport information services have significant benefits ensuring suitable information about services and logistics available on the road and making urban passenger transport more efficient and reliable. Real-time public transport information service infrastructure is a part of the core functionality of intelligent transport systems.

This chapter focuses on developing a framework for real-time data acquisition and choosing an efficient model for trolleybus arrival time prediction that can be easily implemented to improve public transport services by leveraging on the GPS data and data provided by the

Internet of Things applications. An architecture model of information service infrastructure for public passenger transport was developed.

As a use case of the proposed technique, we have implemented and tested model for the trolleybus arrival time prediction on the existing routes. The efficiency evaluation of the models has been performed with respect to the actual arrival time and prognosis time.

All the above results make it sure that these techniques can be easily implemented in real time to improve public transport services by leveraging on the GPS data and data provided by the IoT applications.

Information about vehicle arrival time can be disseminated via the various services, e.g., information boards and kiosks at bus stops, displays in a public transport, and smartphones through the Internet and by SMS.

These results are meant to be considered for the next series of experiments on two pilot information boards. Future work will be aimed at implementing this technology in the public transport infrastructure and validating whether it improves the passenger experience. It is also expected that follow-up study will expand on full employment of IoT technologies to improve traffic and passenger services and involve both vehicle-to-infrastructure and vehicle-to-vehicle communication along with their enhancement.

Future works can be directed to full employment of IoT technologies to improve city traffic and passenger services, involve both vehicle-to-infrastructure and vehicle-to-vehicle communication along with their enhancement.

In order to better understand and assimilate the educational material that is presented in this section, we invite you to answer the following questions.

1. List services for public transport systems.
2. Explain the principle of determining the location of the vehicle.
3. How IoT-infrastructure can meet the people needs in public transport?
4. Which public transport systems can be considered as a priority?
5. What techniques can be utilized to obtain a forecast of the arrival time of public transport? Explain the difference between them.
6. Which parameters can be considered as the input data?

7. How to perform data acquisition and calculating the arrival time prediction of the vehicle.
8. Explain the principle of the method based on haversine formulas.
9. How to perform distance calculations using Google Maps API tool.
10. Why we use different approaches, methods and services for calculating the distance between geographic coordinates?
11. What are the main modules for the manufacture of information boards?
12. How to display information about the time forecasts on an information board.

References

1. S. Ezell, "Explaining International IT Application Leadership: Intelligent Transportation Systems", *The Information Technology and Innovation Foundation*, 58, 2010.
2. G. Keramidas, N. Voros, and M. Hübner, "Components and Services for IoT Platforms: Paving the Way for IoT Standards", *Basel: Springer International Publishing*, 383, 2017.
3. K. Dziekan, "Ease-of-Use in Public Transportation – A User Perspective on Information and Orientation Aspects", *Doctoral Thesis in Traffic and Transport Planning, Infrastructure and Planning*, 2008.
4. J. Richard, A. Edward, P. Zhong-Ren, and O. Simi, "State of the art in automatic vehicle location systems", *Evaluation of the benefits of automated vehicle location systems*, 1998.
5. N. Ronald, R. Thompson, J. Haasz, S. Winter, "Determining the Viability of a Demand Responsive Transport System under Varying Demand Scenarios", *Proceedings of the 6th ACM SIGSPATIAL International Workshop on Computational Transportation Science*, November 2013.
6. The opportunities of networked telematics ("Internet of things") for an improvement of public transport's quality and its boundaries, 2017.
7. PTIPS. Available at: <https://www.scats.com.au>.
8. Wialon. Available at: <https://gurtam.com/en/wialon>.
9. A. Festag, "Cooperative intelligent transport systems standards in Europe", *IEEE Commun. Mag.*, vol. 52(12), pp. 166–172, December 2014. DOI: 10.1109/MCOM.2014.6979970.
10. B. Williams, "Intelligent Transport System Standards", *Artech House, Inc.*, 827, 2008.

11. ETSI ITS-G5 Standard. Final draft ETSI ES 202 663 V1.1.0, Intelligent Transport Systems (ITS); European profile standard for the physical and medium access control layer of Intelligent Transport Systems operating in the 5 GHz frequency band. Technical report ETSI, 2011.

12. M. Basyir, "Determination of Nearest Emergency Service Office using Haversine Formula Based on Android Platform", *EMITTER International Journal of Engineering Technology*, Vol. 5, No. 2, December 2017.

13. M. A. Berlin, "Safety Distance Calculation for Collision Avoidance in Vehicular Ad hoc Networks", *Scholars Journal of Engineering and Technology (SJET)*, vol. 4(1), pp. 63-69, January 2016.

14. C. M. Thomas, W E. Featherstone, "Validation of Vincenty's Formulas for the Geodesic Using a New Fourth-Order Extension of Kivioja's Formula", *Journal of Surveying Engineering ASCE*, February 2005.

15. Googlemaps Android-maps-utils / MathUtil.java.
[https://github.com/googlemaps/
android-maps-
utils/blob/master/library/src/com/google/maps/ android/ MathUtil. java.](https://github.com/googlemaps/android-maps-utils/blob/master/library/src/com/google/maps/android/MathUtil.java)

16. Using the Google Maps API to book the perfect ride.
[https://static.googleusercontent.com/media/enterprise.google.com/ru//maps/res
ources/UsingtheGoogleMapsAPIstobooktheperfectride.pdf.](https://static.googleusercontent.com/media/enterprise.google.com/ru//maps/resources/UsingtheGoogleMapsAPIstobooktheperfectride.pdf)

17. C. M. S. Harold and H. Kramer, "Identifying the information needs of users in public transport", *Human Aspects of Road and Rail Transportation*, pp. 31-340, 2012.

18. R. Lavanya, K. S. S. Rani, R. Gayathri, D. Binu, "A Smart Information System for Public Transportation Using IoT", *International Journal of Recent Trends in Engineering & Research (IJRTER)*, Vol. 03, Issue 04, April 2017.

19. Roads Service. Available at: <https://www.roadsni.gov.uk>.

20. I. Ashour, M. Zorkany and M. Shiple, "Design and Implementation of Transportation Management System", *In Proceedings of the 1st International Conference on Vehicle Technology and Intelligent Transport Systems (VEHITS-2015)*, pp. 11-18, January 2015.

21. M. Rinaldia, C. M.J. Tampire, F. Viti, "A global optimization heuristic for the decomposed static anticipatory network traffic control problem", *Transportation Research Procedia*, Vol. 27, pp. 648 – 655, December 2017.

22. S.J. Edwards, C. Emmerson, A. Namdeo, P.T. Blythe, W. Guo, "Optimising landmark-based route guidance for older drivers", *Transportation Research Part F*, Vol. 43, pp. 225-237, November 2016.

23. E. Jenelius, "Data-Driven Bus Crowding Prediction Based on Real-Time Passenger Counts and Vehicle Locations", 2019.

24. O. Cats, "Real-Time Predictions for Light Rail Train Systems", *The 17th International IEEE conference on Intelligent Transportation Systems (ITSC)*, October 2014.

25. E. Jenelius, "Car-Specific Metro Train Crowding Prediction Based on Real-Time Load Data", *IEEE International conference on Intelligent Transportation Systems (ITSC)*, July 2018.

26. A. Tympakianaki, H.N. Koutsopoulos, E. Jenelius, M. Cebecauer, "Impact analysis of transport network disruptions using multimodal data: A case study for tunnel closures in Stockholm", *Case Studies on Transport Policy*, June 2018.

27. M. Cebecauer, E. Jenelius, W. Burghout, "Integrated Framework for Real-time Urban Network Travel Time Prediction on Sparse Probe Data", *IET Intelligent Transport Systems*, March 2015.

28. F. Rodrigues, S. S. Borysov, B. Ribeiro, F. C. Pereira, "A Bayesian additive model for understanding public transport usage in special events", *IEEE Transactions on pattern analysis and machine intelligence*, Vol. 39. No. 11, pp. 2113-2126, December 2018.

29. S. Foell, S. Phithakkitnukoon, G. Kortuem, M. Veloso, C. Bento, "Predictability of Public Transport Usage: A Study of Bus Rides in Lisbon, Portugal", *IEEE Transactions on Intelligent Transportation Systems*, Vol. 16(5), pp. 2955 – 2960, December 2015.

30. A. Balasubramaniam, A. Paul, W.-H. Hong, H. Seo, J. H. Kim, "Comparative Analysis of Intelligent Transportation Systems for Sustainable Environment in Smart Cities", *Sustainability*, Vol. 9, April 2017.

42. IOT AND COOPERATIVE HUMAN-MACHINE INTERFACES FOR TRANSPORT SAFETY

Prof., Dr. O. O. Orekhov, Prof., DrS V. S. Kharchenko,
Dr. A. O. Stadnik A. (KhAI)

Contents

Abbreviations	403
42.1 Introduction into cooperative HMI.....	404
42.1.1 Principles of cooperative HMI design	405
42.1.2 Standard requirements to HMI for automotive systems	406
42.1.3 Standards for IoT application in automotive systems.....	407
42.1.4 Profiling of requirements to cooperative HMI and IoT.....	410
42.2 IoT based infrastructure for cooperative human-machine systems	412
42.2.1 On-board systems interaction	414
42.2.2 Communication and protocols.....	416
42.3 Development and modeling of IoT based cooperative HMI systems	417
42.3.1 Development.....	418
42.3.2 Quality and safety models	419
42.3.3 Cases for cooperative HMI for transport system.....	426
42.4 Work related analysis	429
Conclusions and questions.....	431
References	433

Abbreviations

AAM – Alliance of Automobile Manufacturers
ADASs – Advanced Driver Assistance Systems
APH – Area of potential hazard
CC – Cloud computing
CEN – European Standards Committee
CENELEC – European Committee for Electrotechnical Standardization
CHMI – Cooperative human-machine interfaces
DSS – Decision support system
IEC – International Electrotechnical Commission
IEEE – Institute of Electrical and Electronics Engineers
ESOP – European Statement of Principles on Human Machine Interface
ETSI – European Telecommunications Standards Institute
GNSS – Global Navigation Satellite System
HASTE – Human Machine Interface and the Safety of Traffic in Europe
HMI – Human-machine interfaces
IETF – Internet Engineering Task Force
I2I – Infrastructure-to-infrastructure
IoT – Internet of things
ISO – International Organization for Standardization
IT – Information technologies
ITS – Intelligent transport system
IVIS – In-Vehicle Information Systems
JAMA – Japan Automobile Manufacturers Association
RTTI – Real-Time Traffic and Travel Information
SAE – Society of Automotive Engineers
TCP – Transport communication protocol
V2V – Vehicle-to-vehicle
V2I – Vehicle-to-infrastructure

42.1 Introduction into cooperative HMI

According to forecasts of the World Health Organization by 2030 number of victims of road accidents can reach more than two and a half million people per year [1]. Active application of information and communication technologies (IT) can be considered as a strategy to improve the safety of transport infrastructure, reduce accidents, improve service quality and reduce its negative impact on the environment. All of these ITs are fully considered within the framework of unified intelligent transportation system (ITS).

ITS includes a variety of applications, such as traffic management systems, information systems of vehicles, advanced driver assistance systems in motion (ADASs - Advanced Driver Assistance Systems), as well as cooperative applications based on the exchange of information between ITS stations and transport infrastructure.

One of the main features of the ITS will be an ability to predict risks and improve the safety of the vehicle. This ability will be provided through the use of various types of models and methods of dynamic safety analysis.

The input data for these models and methods will be the data from the ITS stations of other vehicles or infrastructure on the whole. On-board software of ITS station must address problems of risk assessment, detection and forecasting of hazards, improving situational awareness of the driver in real time.

The application of these techniques in real-time for risk analysis can improve the driver's situational awareness, predict the situation, provide support for decision-making under conditions of high dynamics of the traffic situation and exchange of data within the ITS between distributed stations. It is obvious that the vehicle drivers have different awareness of the current situation. Thus, the exchange of information between ITS stations would allow a substantially increase of security and collective awareness of all road users (all about everyone else).

The aim of this work to develop new principle of cooperative human-machine interfaces (HMI) organization for ITS on basis of IoT for dynamic estimation and provisioning of vehicle safety.

42.1.1 Principles of cooperative HMI design

In the European declaration on the principles of HMI functioning [2] In-Vehicle Information Systems (IVIS) designing foundations are offered. The systems should not distract a driver, and the information they convey to the driver has to be predictable and controlled. It is important that interaction with the informational systems neither overloads the driver of the vehicle nor distracts him. The systems should give the information in a concise and comprehensive way.

Systems that need to communicate with the driver should be easy to use and always provide for the driver to do the principal task, which is driving the vehicle safely. Good HMI system reduces the informational strain on the driver helping to select the most relevant and important information.

As noted in the documents of the European Commission, safe HMI design must take into account the need to integrate nomadic devices and ensure the safety of vulnerable traffic participants (e.g. aged people). Nomadic devices include information and communication equipment such as mobile phone, navigation system, PDA, etc. All these devices are typical examples of the vehicle information systems.

Using nomadic devices may be not matched with a car, especially if their HMI is designed poorly. It should be noted that in the future the increase in the new systems with different haptic, visual and auditory methods of communication with drivers is expected. Therefore, all the risks associated with the use of such systems should be estimated.

Recommendations on the design of safe HMI of the IVIS is suggested in the project Human Machine Interface and the Safety of

Traffic in Europe (HASTE) [3]. The aim of the HASTE project is to develop methodologies and guidelines for the assessment of In-Vehicle Information Systems. It is therefore implied that such systems should have a means of communicating with the driver. This could be through one or more sensory modalities, i.e. visual, auditory or

tactile/haptic interfaces. This will also require some form of system input interface.

Among the objectives of the research program within the HASTE are the following:

- identify and explore scenarios in which safety issues are most important and relevant;
- explore the connection between the load and the risk in the context of these scenarios;
- conceive the mechanisms of risk increasing in terms of distraction and the driver situational awareness reducing;
- determine risk rates;
- apply existing risk assessment methods to real vehicles;
- consider possible causes of information systems threats related to safety and reliability.

42.1.2 Standard requirements to HMI for automotive systems

Basic design requirements for HMI are given in [4, 5]. Results of the expert analysis and ranking of these requirements are given below.

Cognitive compatibility and physiological compatibility - these requirements require physiological and psychological capabilities of the driver and the level of his training to be taken into account, when designing HMI. As main criteria, these principles allow us to estimate the quality of information, as well as ease of its perception, analysis and understanding. This is very important criteria for the human factor.

Consistency is among high priority requirement. Only mutual coherence feedback to the driver through different channels of information can allow him to make right decisions. Hierarchy of priorities of the informational sources must be clearly defined in case of conflicting data.

Situation awareness is one of the most important requirement, because it describes the ability of HMI to perform its basic function - to provide an understanding of the situation by the driver by providing him accurate information on the status of the systems.

Task Compatibility indicates that the system should meet users' requirement. This feature also is one of the most important, because the system must conform to its destination.

Error tolerance and control – priority of this requirement depends on the class of the system. For systems important to safety, this characteristic has very high priority.

Cognitive Workload – information should be fast perceived and understood. System must minimize requirements for in-mind calculations and conversions, and use some hints. The background data must be presented in a convenient form.

User Model Compatibility – all aspects of the system should be compatible with the mental users' models.

Timeliness – system design must take into consideration users' cognitive capabilities and time limits in connection with the process. The speed of the Informational stream and performance monitoring requirements, which are too fast or too slow, may lead to productivity decline.

Logical Structure – all aspects of the system (formats, terminology, sequencing, grouping, and user decision-support aids) should reflect an obvious logic based on task requirements or some other non-arbitrary rationale. The relationship of each display, control, and data-processing aid to the overall task/function should be clear. The structure of the interface and its associated navigation aids should make it easy for users to recognize where they are in the data space and should enable them to get rapid access to data not currently visible (e.g., on other display pages). The way the system works and is structured should be clear to the user.

Flexibility – the system should give the user multiple means to carry out actions and permit displays and controls to be formatted in a configuration most convenient for the task.

Feedback – the system should provide useful information on system status, permissible operations, errors and error recovery, dangerous operations, and validity of data.

Simplicity of design – the HMI should represent the simplest design consistent with functional and task requirements.

42.1.3 Standards for IoT application in automotive systems

The international standardisation process is an essential mean of ensuring the compatibility of the separate transport telematics systems.

The organisations engaged in standardisation in ITSs are as follows:

- International Organization for standardization (ISO);
- European Standards Committee (CEN);
- European Committee for Electrotechnical Standardization (CENELEC);
- International Electrotechnical Commission (IEC);
- Institute of Electrical and Electronics Engineers (IEEE);
- Society of Automotive Engineers (SAE);
- The Internet Engineering Task Force (IETF);
- European Telecommunications Standards Institute (ETSI).

The standards for ITSs are as follows:

- ISO/TR 10992:2011 Intelligent transport systems - Use of nomadic and portable devices to support ITS service and multimedia provision in vehicles;
- ISO/TR 12859:2009 Intelligent transport systems - System architecture - Privacy aspects in ITS standards and systems;
- ISO 14813-1:2007 Intelligent transport systems - Reference model architecture(s) for the ITS sector - Part 1: ITS service domains, service groups and services;
- ISO 15662:2006 Intelligent transport systems - Wide area communication - Protocol management information;
- ISO/TS 17419:2014 Intelligent transport systems - Cooperative systems - Classification and management of ITS applications in a global context;
- ISO/TS 17423:2014 Intelligent transport systems - Cooperative systems - ITS application requirements and objectives for selection of communication profiles;
- ISO/TS 17427:2014 Intelligent transport systems - Cooperative systems - Roles and responsibilities in the context of cooperative ITS based on architecture(s) for cooperative systems;
- ISO/TR 17465-1:2014 Intelligent transport systems - Cooperative ITS - Part 1: Terms and definitions;
- ISO/TS 19321:2015 Intelligent transport systems - Cooperative ITS - Dictionary of in-vehicle information (IVI) data structures;
- ISO 21213:2008 Intelligent transport systems - Communications access for land mobiles (CALM) - 3G Cellular systems;

– ISO 24978:2009 Intelligent transport systems - ITS Safety and emergency messages using any available wireless media - Data registry procedures.

Standards for the on-board interfaces.

SAE Standards and Recommended Practices from the SAE Safety and Human Factors Committee:

- SAE J2364 Navigation Function Accessibility While Driving;
- SAE J2365 Calculation of the Time to Complete In-Vehicle Navigation Tasks;
- SAE J2395 In-Vehicle Message Priority;
- SAE J2396 Definitions and Measures Related Driver Visual Behavior Using Video Techniques;
- SAE J2399 Adaptive Cruise Control (Acc) Operating Characteristics and User Interface;
- SAE J2400 Forward Collision Warning Systems: Operating Characteristics and User Interface;
- SAE J2678 Navigation Function Accessibility While Driving Rationale;
- SAE J2802 Blind Spot Monitoring System (BSMS): Operating Characteristics and User Interface;
- SAE J2808 Road/Lane Departure Warning Systems: Human Interface;
- SAE J2830 Process for Comprehension Testing of In-Vehicle Icons;
- SAE J2831 Design and Engineering for In-Vehicle Alphanumeric Messages;
- SAE J2889 Measurement of Minimum Noise Emitted by Road Vehicles.

Standards for the human-machine interface.

IEC 60447:2004 Basic and safety principles for man-machine interface, marking and identification - establishes the main principles of the human-machine interface activation that ensure the control elements to function accurately and timely as well as the safe performance of the equipment in general.

The standards in ergonomic are as follows:

- ISO 9241:2010 Ergonomics of human-system interaction - Part 210: Human-centred design for interactive systems - provides the requirements and recommendations for the human-oriented system design;

- ISO 15008:2003 Road vehicles - Ergonomic aspects of transport information and control systems - Specifications and compliance procedures for in-vehicle visual presentation;
- ISO 15005:2002 Road vehicles - Ergonomic aspects of transport information and control systems - Dialogue management principles and compliance procedures;
- ISO 17287:2003 Road vehicles - Ergonomic aspects of transport information and control systems - Procedure for assessing suitability for use while driving.

Analysis of the standards allows concluding that there are a few sets of standards containing requirements to separate groups of the cooperative HMI for IoT based ITSs.

To get the requirements to such interfaces and systems a special procedure of profiling has to be implemented.

42.1.4 Profiling of requirements to cooperative HMI and IoT

The main design manuals regarding the HMI for vehicles are the following:

- European Statement of Principles on Human Machine Interface [6],
- JAMA – Japan Automobile Manufacturers Association Guidelines for In-Vehicle Display Systems [7],
- Alliance of Automobile Manufacturers (AAM) [8].

These manuals summarize the key aspects of safety applicable for the human-machine interfaces of the automobile and communication systems.

The parameters and requirements to the cooperative HMI for the (IoT based) intelligent transport systems identified as a result of the analysis into the standards, recommendations and the context of the use are given in the table 42.1.

Table 42.1 Requirements for the HMI for the ITSs

Parameter	Requirement description	Source
Usability	<ul style="list-style-type: none"> - the feedback between the system and the driver should be timely and recognizable; - the driver should be given the information about the current state of the system and any system malfunction; - visual information should be displayed in a way that the driver can assess special details within few sights 	ESOP
	The driver should anytime have the possibility to keep at least one hand on the steering wheel when interacting with the system	ESOP JAMA
	The system should not hinder the driver's field of vision	JAMA
Safety	<ul style="list-style-type: none"> - the system should help the driver and should prevent the possible dangerous behaviour of the driver or other road users; - the system should not distract the driver and draw his attention that should be focused on monitoring the road situation; - the system should not provide the driver with the information that can cause the dangerous behavior of the driver or other road users; - the system should provide the driver with high-priority information rather than the information related mostly to the safety; - the system should not hide the vehicle control elements and the displays purposed for driving primarily 	ESOP

42. IoT and Cooperative Human-Machine Interfaces for Transport Safety

Simplicity	The system instructions should be simple, correct and easy to understand	ESOP JAMA
	The visual information should be given piece by piece to ensure the step-by-step control of the system	JAMA
Cognitive compatibility	The interface should not cause the driver's mixed reaction. The result of the drivers' actions should not be different from what he expects	
Other requirements	<ul style="list-style-type: none"> – brightness, contrast, colours and other parameters of the display should not blind the driver in the night; – the system producing sounds with the volume that can not be adjusted by the driver should not block the sound messages inside and outside the vehicle 	ESOP, JAMA

42.2 IoT based infrastructure for cooperative human-machine systems

Different vendors on IT market offer the advanced driver assistance systems [9, 10]. Such systems as a collision warning system, parking assistant, are designed for improvement of safety during the driving and reducing the driver's strain [11].

One of the development lines of such systems is the improvement of the interaction between the driver and the vehicle control system "human-machine" (Human-Machine Interaction) and the provision information about the current situation on the road in real time for driver (Real-Time Traffic and Travel Information (RTTI)).

The provision this sort of information leads to an increase of situational awareness of vehicle driver. Awareness implies existence of operational information about the vehicle state and road conditions. Sufficient level of situational awareness is required for risk assessment and hazard analysis, planning, goal-setting, etc.

Traditionally, situational awareness includes three levels: (1) the level of perception of the situation, which is provided by monitoring the status of various objects around the vehicle; (2) the level of conclusions, which determines the ability of vehicles to integrate various sources of information and to make assessments of situations on this basis (given level is provided by the decision-making about the current dangers and risks for the vehicle); (3) the level of prediction, on which the forecast of dangerous situation risks is carried out.

Undoubtedly, increasing of situational awareness leads to overall risk lowering (collisions, overturning, etc.), since it is possible to detect and predict hazardous situations, determine precautions for their reducing in real time. This way, for example, a prediction of great number of unsafe trajectories neighboring vehicles is performed, as well as dynamic risk zones, zones of "comfort" of the vehicle, etc. Great importance for enhancing of situational awareness has issues for construction of secure dynamic human-machine interfaces [12, 13].

At the same time, the point is that are two sides of the safe HMI: firstly, the development and evaluation of interfaces according to the requirements of the normative documents and safety standards, and secondly, reporting succinct information about objects in the area of the vehicle movement to the driver, which can threat him (area of potential hazard (APH)). It is also necessary to take into account the ability of an HMI to adapt to the situation on the road, to take into account the state of the driver, its features, driving experience, behavior peculiarities in critical situations, habits, etc., i.e. increasing of its adaptability.

The high amount of data used in the ITS, leads to the necessity of improvement of information access for all traffic participants. Improvement of situational awareness, risk assessment in the real-life improvement requires the use of large computing facilities for the storage, processing and analysis of data. These facilities are not always available, even for modern on-board computing equipment of vehicle.

Reliability of on-board software is also an additional safety factor in the ITS. It is necessary to consider additional precautions to enhance safety, including the possibility of using modern cloud computing for information processing in the framework of the ITS.

42.2.1 On-board systems interaction

Deployment of these systems creates prerequisites for the further vehicle intellectualization based on the newest computer technologies, satellite navigation and wireless technologies [1]. These systems are capable of warning the drivers about dangers in motion. They incorporate the systems that provide for the connection and information interchange between vehicles (V2V – vehicle-to-vehicle), between vehicle and infrastructure (V2I - vehicle-to-infrastructure) and between different parts of an intellectual transport infrastructure (I2I – infrastructure-to-infrastructure).

Intelligent transport infrastructure includes complex of equipment that secures acquisition of the almost full information about the road situation and the possibility of a quick response to the changing conditions. If necessary, these systems are complemented with the Global Navigation Satellite System (GNSS).

The infrastructure of the ITSs includes:

- the road complex of all subsystems, among them are the technical monitoring tools, tools for analysis and decision making according to the functional tasks of the subsystems, the control function implementation tools;
- the situational and operations control centers;
- wire traffic support tools the purposed to execute the functional tasks of the subsystems;
- information and telecommunication means that ensure the secure interaction with the outside information systems.

Much attention is given to the issues of human factor and HMI in the ITS [14]. HMI will be one of the major topics to which investigations in the field of transport safety are going to be devoted in the nearest future, as marked in [14]. Motorcar companies offer a whole set of advanced driver assisting systems, for example:

- collision warning system;
- pedestrian detection system
- blind spot information system;
- lane departure warning system;
- driver fatigue monitoring system;
- speed alert system;
- drunk driving prevention system.

Table 42.2 Driver help systems implementation examples

Number	System
1	Collision warning system with Auto Brake (Volvo)
2	Pre-collision System (Toyota)
3	Adaptive cruise control (Volvo)
4	Lane departure warning system (Volvo)
5	Automated Highway Driving Assist System (Toyota)

To use such systems effectively one needs an HMI that maintains human-vehicle interaction and mitigates the negative errors impact on the safety, allows avoiding misinterpretation of the information that the system provides.

Cloud computing (CC) is used to receive or transmit data over the Internet via a wireless connection. The idea of using cloud services in ITS is just beginning to gain popularity [15]. The facilities of "clouds" can also affect the increase of transport safety.

As noted above, the cooperative systems are such systems that wirelessly communicate with other cars. Therefore, under the term of a cooperative HMI we will consider an interface system, distributed among several vehicles. An additional monitor is installed on each vehicle or a compact unit is embedded into the existing HMI to provide information about safety in APH, which gives the information about the safety level. This information (risk matrix) is formed and dynamically adjusted basing on the overall situation for each car (the state of the vehicle, driver and road conditions), which is in the danger zone.

It is clear that these must be adaptive HMI, which reflect not only information about the condition of the car, but of the driver as well. If a driver starts to doze off or falls asleep, it is necessary to wake him up and inform the drivers of motor vehicles that are nearby.

The property of adaptability in the HMI becomes apparent in several forms: changes in the content of the information provided, dialogue, sharing of tasks between man and machine, the speed of adaptation [16].

One of the variants of cooperative HMI construction - is to use the technology of IoT. Fig. 42.1 shows the proposed architecture of the cooperative HMI.

Cooperative HMI provides the measure values of the parameters of vehicle and driver state in real time via the Internet into the "cloud." Here, the data from all the cars is dynamically processed and transmitted to motoring public.

Information from the HMI of one vehicle (shown as a red dashed line, Figure. 42.1) passes through the "cloud" and is displayed on the HMI of another vehicle. In turn, the information from the HMI of another vehicle (shown as a green line, Figure. 42.1), is also transferred to the HMI of the first vehicle. This information is taken into account when the risk analysis of each vehicle is performed.

There are important issues in developing of HMI: optimization of the information necessary for driver for the safe driving mode; determination of the information views, which stimulate the driver; control and prevention of the driver's distraction.

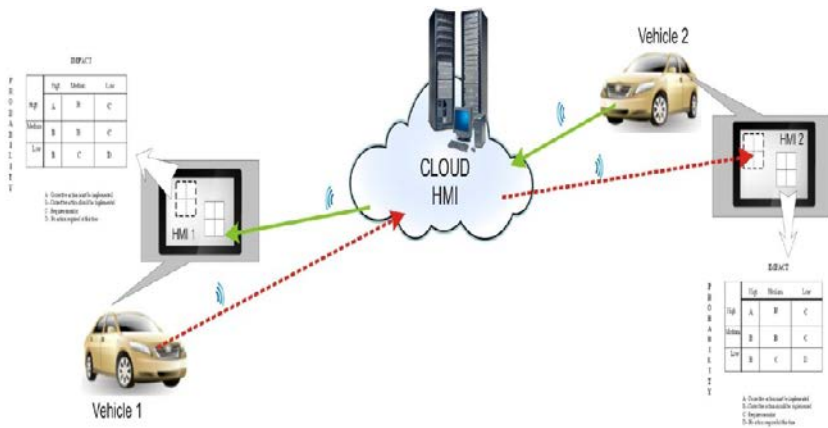


Fig. 42.1 – Architecture of the cooperative HMI based on IoT

42.2.2 Communication and protocols

The client and the server cooperate wirelessly through the module for communication. The general convenience functions and data models for packetizing can be found in the Core-project that is used by the both sides.

Since the communication protocol should provide equal rights for the client and the server, it has been agreed to implement the communication protocol based on TCP from the specification Java EE – WebSocket.

The protocol ensures the free data exchange: two equal participants exchange data, each one working independently and sending data to the other one when necessary (fig. 42.2).

The data is packetized. The packets stand for the data type from the core-project in the JSON format. The packets are formed and parsed on both sides in the communication module.

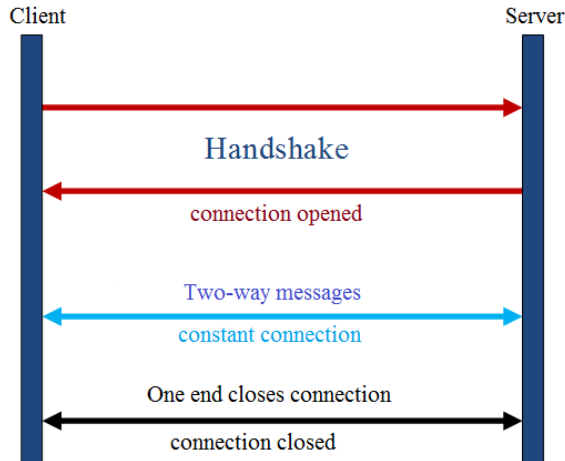


Fig. 42.2 – Work principle of the communication protocol WebSocket

42.3 Development and modeling of IoT based cooperative HMI systems

The cooperative human-machine interface for the intelligent transport systems is the client-server system based on the cloud computing. The front end is located inside the vehicle and stands for the human-machine interface for the driver to work with the system. The back-end is the decision support system based on the cloud computing.

The system “Cooperative human-machine interface for the intelligent transport systems” is designed to enhance the vehicle safety. The system monitors the driver’s state and the vehicle’s state and sends the data about the potential hazards to the other road users on a real-time basis.

42.3.1 Development

The system consists of three projects combined in a single solution:

- server end – the decision support system (DSS);
- client end – the user HMI;
- Core-project that includes data models for the communication protocol and the common utility functions.

The server end is the web-application, the core of which is the DSS. The web-application is managed by the Apache Tomcat server that supports the HTTP protocol. The protocol allows the interaction between the client and the server. The client end is implemented for the Android platform and it stands for the user interface. The ground map is the key element. The data exchange is performed wirelessly using the data types specified in the general Core-project. Java serves as the platform for creating the system in question. The figure 42.3 shows the architecture of the system.

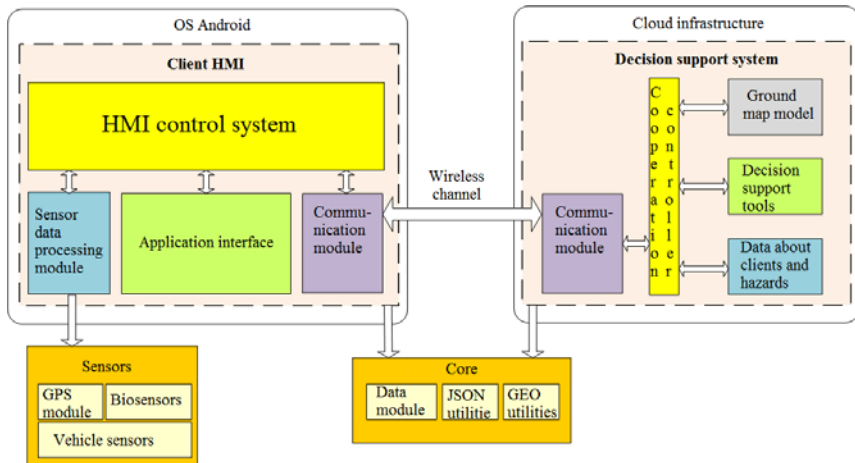


Fig. 42.3 – Architecture of the system

The vehicle's sensors data is obtained from the board computer through the wired interfaces. The requests to the biosensors can be done through wireless interfaces. The current coordinates are obtained from the GPS receiver through the wire communication channel.

The module for communication is responsible for receiving and transmitting the messages to the server. The packets are formed by the client subsystem using the data models from the Core-project.

The interface of the application includes the following modules:

1. Visual interface responsible for displaying the following elements on the monitor:

- registration page (personal data filling);
- ground map, current position and position of other participants, hazard objects on the ground map;
- indicators of the driver's state and server connection;
- hazards panel;
- signals setup control panel.

2. Speech synthesizer responsible for voice warnings generation.

3. Speech recognition responsible for voice commands recognition.

4. Sounds management responsible for sound warnings.

The HMI control system is responsible for the interaction with other modules in the system. It obtains the data from the sensor interfaces and transmits it to the communication module where packetizing takes place and the packets are sent to the server.

The user setup control module is responsible for the configuring and storing the personal data and signal parameters.

The hazard control module is responsible for the refreshing of the hazards list provided by the server.

The emulation module is responsible for the emulation of the vehicle movement and the data obtained from the biosensors.

42.3.2 Quality and safety models

The variety of software quality models were developed within the framework of program and usability engineering. Most of the models are hierarchical [17, 18].

The table 42.3 contains the most well-known models, which are applied to assess the quality of developed software and it's user interface.

The HMI model in set-theoretic can be set as a cortege of the following elements:

$$QM_{HMI\&C} = \langle G, MSC, MM, W, DATA, ART, CONT \rangle, \quad (42.1)$$

where G the interface purpose; MSC the set of characteristics; MM the set of metrics; W the set of characteristics and metrics ranks;

$DATA$ the set of data for metric measurements; ART the artefacts set; $CONT$ conditions of use.

$$MSC = MFA \cup MCR, \tag{42.2}$$

where MFA the set of factors; MSC the set of criteria.

$$CONT = \langle MUS, MTA, EN, EQ \rangle, \tag{42.3}$$

where MUS the set of users; MTA the set of tasks; EN the environment in which HMI operates (temperature, humidity etc); EQ HMI equipment.

Table 42.3 Existing Models Classification

Models Types	Hix et al. (1993)	Wixon (1997)	Dix et al. (1998)	ISO 9241-11(1998)	Lecerov et al. (1998)	Thomas (1998)	Kengeri et al. (1999)	Battleson et al. (2001)	Donyace et al. (2001)	ISO 9126-(2001)	Campbell et al. (2003)	Shneiderman (2005)	QUIM (2006)	Sauro et al. (2009)	ISO 25010 (2011)
Integrated													+		
Standardized				+						+					+
Not standardized	+	+	+		+	+	+	+	+		+	+	+	+	

Structure of HMI quality model is presented in figure 42.4.

The problem of HMI quality model development requires the consideration of new factors and criteria, based on principles. The development of new criteria is based on the introduction of new metrics, which must reflect the most important aspects of measuring attributes, and have to be rather easy.

An advantage of this model is in taking into consideration most factors that have any influence on HMI quality. It helps to avoid conflicts between different quality requirements.

Let us specify the operators to do all the interaction tasks for the HMI and build the model to assess it basing on the classical GOMS method and the assessment method for the automobile navigation systems according to the J2365 standard. The client HMI time indicators assessment model is given in the table 42.4. The table 42.5 displays the code of each operator and the duration for the young and elderly drivers.

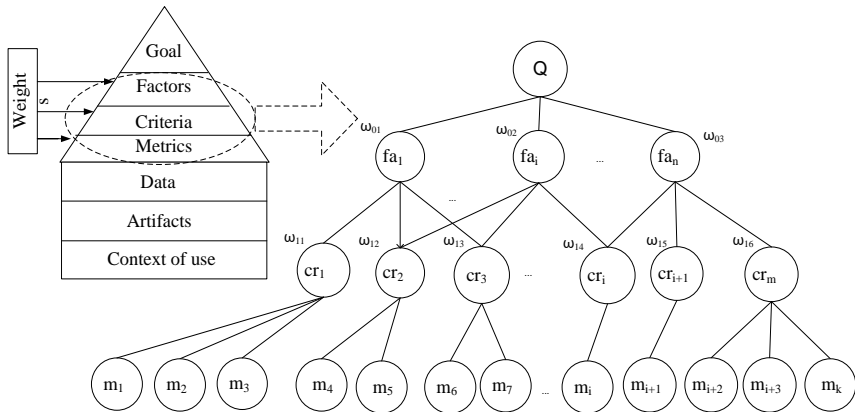


Fig. 42.4 – Structure of HMI quality model

Identification of the tasks for the work with the human-machine interface:

- 1) Pass the signal about the dangerous road section via the monitor.
- 2) Pass the signal about the dangerous road section using the voice command.
- 3) Disable the sound signals.
- 4) Request the hazard description.
- 5) Learn the road situation.
- 6) Listen to the message about the hazard.

Models development and the calculation of tasks execution.

Task 1. Pass the signal about the dangerous road section via the monitor.

- 1) M – Mental psych-up – 1.50 / 2.55.
- 2) D – Reach the monitor with the hand – 0.45 / 0.77.
- 3) Y – Move the hand (finger) to the left hazard panel – 0.80 / 1.36.

- 4) H – Get the hazard panel out – 1.2 / 2.04.
- 5) Y – Move the finger to the button of interest– 0.80 / 1.36.
- 6) H – Press the hazard button – 1.2 / 2.04.
- 7) O – Wait for a response from the system – 0.1.

The sequence:

$$M + D + Y + H + P + Y + H + O$$

Time for the young people:

$$t1 = 1.50 + 0.45 + 0.80 + 1.2 + 1.2 + 0.1 = 5.25 \text{ s.}$$

Time for the elderly people:

$$t2 = 2.55 + 0.77 + 1.36 + 2.04 + 2.04 + 0.1 = 8.86 \text{ s.}$$

Task 2. Pass the signal about the dangerous road section using the voice command.

The sequence:

$$M + G + M + G + O$$

$$t1 = 1.50 + 1.50 + 1.50 + 0.1 = 4.6 \text{ s.}$$

$$t2 = 2.55 + 1.50 + 2.55 + 0.1 = 6.7 \text{ s.}$$

Table 42.4 GOMS method adaptation for the HMI

Operator	Classical GOMS method	GOMS method according to J2365, young / elderly	GOMS for CHMI Code, time
Mental psych-up	Mental operation M = 1.35 s	Mental operation M = 1.50 / 2.55 s	Ment M = 1.50 / 2.55 s

42. IoT and Cooperative Human-Machine Interfaces for Transport Safety

Compare the hazard description with the position on the map			
Assess the most dangerous objects on the map			
Reach the monitor with the hand	Movement $D = 0.4 \text{ s}$	Reach far $R_f = 0.45 / 0.77 \text{ s}$	Reach $D = 0.45 / 0.77 \text{ s}$
Mark the position on the monitor with the finger	Mark $Y = 1.1 \text{ s}$	Cursor once $s_1 = 0.80 / 1.36 \text{ s}$	Mark $Y = 0.80 / 1.36 \text{ s}$
Find the marker on the map	-	Search $S = 2.30 / 3.91 \text{ s}$	Search $P = 2.30 / 3.91 \text{ s}$
Find the control element on the monitor	-	Search $S = 2.30 / 3.91 \text{ s}$	
Press the object on the map	Press the key $K = 0.2 \text{ s}$	Enter $E = 1.2 / 2.04 \text{ s}$	Press $H = 1.2 / 2.04 \text{ s}$
Press the button	Press the key $K = 0.2 \text{ s}$	Enter $E = 1.2 / 2.04 \text{ s}$	
Wait for a response from the interface	System response R	Response time of system-new menu $R_m = 0.50 \text{ s}$	Interface response $O = 0.1 \text{ s}$
Say the key voice command aloud	-	-	Voice command $G = 1.5 \text{ s}$
Say the signal voice command aloud	-	-	
Listen to the message about the hazard	-	-	Listen $s = 3.5 \text{ s}$
React to the situation	-	-	Rection PE

Table 42.5 Summary table of the operators

	Mental operation	Reach	Mark	Search	Press	Response	Voice command	Listen	Reaction
	M	D	Y	P	H	O	G	s	PE
Young	1.50	0.45	0.80	2.30	1.2	0.1	1.50	3.5	-
Elderly	2.55	0.77	1.36	3.91	2.04			-	

The quantitative evaluation of the HMI shows that the hazard signal is passed more effectively using the voice commands. The execution of the signal setting task should be optimized through the voice commands, and thus less time will be spent by the driver. Additionally, we can conclude that the voice description requires more time compared to the situation of the driver executing the task of the ground map assessment. However, in this case the driver pays his attention to the map far more quickly which allows him to react to the situation faster.

The functional safety of the cooperative HMI can be access using risk analysis, for example, HAZOP method. The objects of analysis are the control elements and their components, data flows, and scenarios of driver's work.

The table model for the HAZOP research is as follows:

$$Fh_t = \langle e_f, c_f, kw_f, k_f, a_f, p_f, u_f \rangle_{f=1}^F \quad (42.4)$$

where e_f – element (component, system);

c_f – feature of element;

kw_f – control word;

- k_f – failure type;
 a_f – consequences (result) of failure;
 p_f, u_f – consequences (result) of failure.

So, each combination of element and failure will correspond with n table lines, where n is the number of command words. The resulting table is given in table 42.6.

The key entities in cooperative HMI are the elements for displaying the information and data flows. The control words take a specific meaning. The examples of control words developed in this context are given in table 42.7.

Table 42.6 HAZOP Table

Component / Element	Feature of element	Control word	Failure type	Consequences of failure
---------------------	--------------------	--------------	--------------	-------------------------

Table 42.7 Examples of control words in CHMI

Control word	Data flow to CHMI	Data flow to driver
No	No information is transferred	The driver cannot receive or understand the request or establish the connection
More	Additional information is transferred	The driver understands or communicates more than intended or necessary
Less	The transferred information is not full	The driver understands or communicates less than intended or necessary
Early	The information is transferred earlier than planned	The driver makes “hasty conclusions” and provides wrong answers
Late	The information is transferred later than planned	The driver does not understand or does not send the information early

Table 42.8 demonstrates the functional safety research into the “map” element of CHMI.

To conclude, based on the CHMI, the following reasoning sequence is built:

1. The map is the key element of CHMI, so we will analyze it.
2. The feature under analysis is the “Graphic image”.
3. The command words applied to the “Graphic image” feature are LESS, MORE, NO.
4. If the information in the CHMI is not sufficient, more than needed or absent, an incorrect driver’s reaction is possible resulting in a car accident.
5. Therefore, failure severity is high and failure probability is high as well.
6. At the same time, incorrect image size is possible.
7. It is recommended to set the correct image size.

Table 42.8 Usage of HAZOP for “map” element

Element	Feature of element	Control word	Failure type	Consequences of failure
Map	Graphic image	Less	Lack of information	Incorrect driver’s reaction (distraction)
Map	Graphic image	More	Excess of information	Incorrect driver’s reaction (distraction)
Map	Graphic image	No	No necessary information	Incorrect driver’s reaction (incorrect actions)

42.3.3 Cases for cooperative HMI for transport system

The human-machine interface provides the driver with the information about the road situation, the driver’s state and the vehicle’s state.

At the first start of the client application the registration form is displayed where the driver needs to enter his personal data (nickname, age, sex).

The working area on the display is covered with the ground map (fig. 42.5).

The current state and the direction of the vehicle is marked on the map with the help of the special arrow indicator. The map is to be centered according to the current position. The position of other vehicles is displayed by means of arrows having different colours.

The connection to the server is displayed by a special indicator.

The HMI provides for the feature of manual signals to other drivers about the dangerous road stretch by pressing a button with the schematic representation of hazards types on a special board (fig. 42.6).



Fig. 42.5 – Visual interface

- 1 – current position; 2 – other vehicle; 3 – server connection indicator;
- 4 – driver's state indicator

The speech recognition has been adopted in the HMI for the voice hazard signal transfer. The command for signal transfer consists of two fields: 1 - key phrase, 2 - hazard type.



Fig. 42.6 – Hazards types

Hazards are indicated on the map with markers displaying the hazard type (table 42.9). The marker is coloured according to the hazard level.

Table 42.9 Hazard level

Hazard type	Poor road	Ice condition	Fog	Caving	Reconditioning work	Poor driver's state
Marker						

Map scale should be set according to the range of the lowest hazard level. When the hazard description is queried, an informative message with the enlarged hazard marker and the distance to the hazard object is displayed.

A new hazard occurred is accompanied by the short voice signals. If the hazard level is high, the driver is informed by the voice messages communicating the hazard.

Display brightness and contrast should be adjusted to the daytime. The voice messages volume level is to be adjusted to the noise level in the car.

The overall picture of the road is at the driver's disposal. He can see the ground map, monitor other vehicles moving on a real-time basis. The

driver's awareness is improved as the position of the cars undetected through the glass or by the mirror can be obtained. The blind spot issue is resolved. Due to the voice description of the hazards the cognitive load is reduced, the probability of the driver's distraction of the display is lowered.

42.4 Work related analysis

Reengineering the vehicle to a cloud-based technology is discussed in [16]. Vehicles with a global positioning system that are connected to the "cloud", will always "know" their location and the road conditions. Today, some of the features for vehicle are designed with innovative technology, using the IoT, for example, the communication function V2V (vehicle-to-vehicle) and V2R (vehicle-to-road).

The Volvo Car Group company is working on new car projects - exchange of information about the dangers on the road through the "cloud" and control of the driver's state [19].

The data about the slippery road parts generated basing on the vehicle sensors is passed to the Volvo Cars data base via mobile network on a real-time basis. A warning is passed to other vehicles reaching this road part instantly, thus making it possible for the driver to take prompt measures in order to prevent the critical situation.

Another example of IoT is a project where the information about the state of the road from the individual vehicles incomes into the overall system based on the "cloud." Real-time data about slippery surfaces on the road is transmitted through the mobile communication network to alert the vehicle, which are around. Warning is instantly transmitted to the other vehicles, which are close to the slippery area.

This enables drivers to take an immediate action to avoid a critical situation.

Other possible application of this technology is the remote diagnostics. Data can be transferred in advance, thus eliminating the problem in real-time [20].

Toyota Motor Corp. and Panasonic jointly develop a service that will connect cars and home appliances through the IoT [21].

The review of the systems for driver state analysis is given in the table 42.10.

Table 42.10 Driver state analyzing systems

System	Description	Sensors used	Implementation examples
DAS (Driver Attention Support) – driver’s exhaustion detection and preventing sleeping at the wheel	Driver’s exhaustion is assessed by processing multiple parameters: <ul style="list-style-type: none"> – vehicle movement (speed, forward and side acceleration, rate of yaw); – biometric indicators (heart rate, respiration rate, skin temperature); – driver’s vision (eyes opening rate and vision line); – driver’s actions (turning angle of the steering wheel, position of the foot and brake throttles); – road condition (traffic density, road covering). 	<ul style="list-style-type: none"> – IR sensor behind the steering wheel that controls the face temperature. – piezoelectric sensor in the safety belt that monitors the breathing rate; – patches at the rim of the steering wheel that measure the pulse; – IR sensor behind the steering wheel that measure the temperature of the palms; 	<ol style="list-style-type: none"> 1) Attention Assist (Mercedes-Benz) 2) Driver Alert Control (Volvo); 3) Seeing Machines (General Motors).
Physical state assessment systems	Assessment of the critical health indicators: <ul style="list-style-type: none"> – pulse; – breathing rate; – skin capacity; – blood sugar level; 	<ul style="list-style-type: none"> – heart rate sensors installed in the seat; – sensors at the rim of the steering wheel: electrodes that monitor the heart rhythm and optical sensors that assess palms capacity. 	<ol style="list-style-type: none"> 1) Driver load assessment system (Ford); 2) Aged driver’s state control system 3) Vital indicators control system (Toyota); 4) Warning technology for the diabetic drivers (BMW).

The project PRORETA [22] is a research in the area of the cooperative HMIs. The research object is the prototype of the cooperative automobile HMI that implements the scenarios of preventing collisions at the cross-roads.

The PRORETA HMI system implements a huge number of use scenarios, it does not complicate or irritate and ensures the multimode support.

The HMI provides 4 support levels – information messages, warnings, actions recommendations, automatic intervention.

A lot of EU universities including ALIOT project partners conduct research and implement education MSc and PhD programs in the Internet of Things application for transport and other domains. Development of cooperative HMI for cloud and IoT systems based on analysis of these programs and providing some of the educational topics and research directions.

In particular, the following courses and programs have been considered:

- Coimbra University, Portugal: IoT course for MSc [23]. The course represents a new stage in the digital evolution and focuses on the Internet of Things for smart transport and cities, and the development of tools to transform city infrastructure;

- KTH University, Sweden: three MSc programs including:

- a) IoT related topics in Information and Network Engineering [24],

- b) Communication Systems [25],

- c) Embedded Systems [26];

- Newcastle University, United Kingdom: MSc Programme on Embedded Systems and Internet of Things (ES-IoT) MSc [27].

Conclusions and questions

In this section, the analysis into the available solutions regarding the cooperative intelligent transport systems and their human-machine interfaces has been conducted. The standards and recommendations in the area of transport systems interfaces design have been analysed. The requirements to the HMI for the cooperative ITSs have been formulated. The features of the such interfaces have been identified.

The prototype of the system “Cooperative human-machine interface for intelligent transport systems” based on the Internet of Things has been developed.

The HMI prototype in question has been examined in the laboratory conditions. The assessment using the GOMS method has allowed to calculate the time to execute the task of user interaction with the system. The resulting data showed that the interface needs to be improved further.

The hierarchical model quality of the cooperative HMI has been suggested. The HMI prototype in question has been examined in the laboratory conditions. The assessment using the GOMS method has allowed to calculate the time to execute the task of user interaction with the system. The resulting data showed that the interface needs to be improved further.

The method of HAZOP risk analysis has been adapted for the functional safety of the cooperative human-machine interfaces of the intelligent transport systems. A new interpretation of control words has been given, the elements and features for the analysis have been selected, and the risk analysis has been performed.

The system “Cooperative HMI for ITSs” allows enhancing the vehicle safety and reducing the number of the road accidents. Safety is increased due to elimination of the following situations:

- crashing into the on-going or overtaking vehicle;
- accident caused by the “agressive” driver;
- emergency due to the poor driver’s health;
- accident caused by the drunk driver;
- possible emergency on the dangerous road section.

Safety is improved by increasing the driver’s awareness about the road situation and the possible hazards on a real-time basis through the human-machine interface.

1. What does intelligent transport system stand for?
2. What are the trends in driver assistance systems?
3. Please give examples of driver assistance systems.
4. How can the driver’s situation awareness be increased?
5. What is the effect of increased driver’s situation awareness?
6. Please name the methods used for dynamical risk assessment.
7. What are the types of connection between the transport systems and the infrastructure?
8. What does intelligent transport infrastructure stand for?

9. What are the components of the intelligent transport system infrastructure?
10. Please define the human-machine interface.
11. What are the key characteristics of HMI?
12. Please specify the requirements to the HMI for the ITSs.
13. What does the characteristic of “cognitive compatibility” stand for?
14. How does the HMI adaptivity express itself?
15. What is the key element of data representation in HMI for ITS?

References

1. V. Stepanov, “Organization of traffic. Intelligent transport and two main troubles”, *Haulier*, vol. 108, no. 9, 2009
2. European Statement of Principles, European Statement of Principles for in-vehicle information and communication systems, 1999.
3. Recommended Methodology for a preliminary safety analysis of the HMI of an IVIS, *HASTE, Deliverable 4*, 2005.
4. A. Anokhin and N. Nazarenko, “Designing interfaces”, *Biotechnosphere*, vol. 8, no. 2, pp. 21-27, 2010.
5. A. Orekhova, “Analysis of the criteria and methods for the design of safe interfaces information and control systems”, In Proc. International Conference “ICTM-2010”, vol. 2. 2010, p. 219.
6. Commission recommendation of 22 December 2006 on safe and efficient in-vehicle information and communication systems: update of the European Statement of Principles on human machine interface, *Official Journal of the European Union*. L 32/200. pp. 200-241, 2007.
7. JAMA - Japan Automobile Manufacturers Association Guidelines for In-Vehicle Display Systems, Version 3.0 Online.. Available: http://www.jamaenglish.jp/release/2005/jama_guidelines_v30_en.pdf. Accessed 18.08.2004...
8. Alliance of Automobile Manufacturers (AAM) Statement of Principles, Criteria and Verification Procedures on Driver Interactions with Advanced In-Vehicle Information and Communication Systems, Online.. Available: https://www.google.com.ua/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwiC763ntq_JAhVILHIKHS8FBM4QFggcMAA&url=http%3A%2F%2Fwww.autoalliance.org%2Findex.cfm%3Fobjectid%3DD6819130-B985-11E1-9E4C000C296BA163&usg=AFQjCNEbPAVAVmle1dSUj2

D39DOhs2_zA&sig2=n91_IEv8HWlaC_Q2o_ycLg. Accessed 26.06.2006...

9. Opel and project URBAN: improvement of safety and cost-effectiveness on moving in cities, 2014. Online.. Available: www.opel.ru/experience/ob-opel/novosti-opel.

10. What technical innovations has Volvo implemented for last 10 years? 2011. Online.. Available: www.autoconsulting.com.ua/news.

11. Toyota Motor Corporation» presents new systems of vehicle safety, 2013. Online.. Available: www.major-toyota.ru/news.html.

12. A. Orekhova, “Information technology of I&C systems human machine interfaces safety assessment”, *Information processing systems*, vol. 108, no 1, pp. 267-271, 2013.

13. A. Orekhova A., V. Kharchenko V., and V. Tilinskiy, “Safety case-oriented assessment of human-machine interface for NPP I&C system,” *Reliability: Theory & Applications*, vol. 26, no. 3, pp. 27 – 38, 2012.

14. Cars In The Future: Human Machine Interface Online.. Available: <http://www.rosopa.com/roadsafety/policy/carsinthefuture/human-machine-interface.aspx>..

15. J. Stoltzfus, “Cloud Computing for Vehicles: Tomorrow's High-Tech Car”, 2012. Online.. Available: <http://www.techopedia.com/2/28137/trends/cloud-computing/cloud-computing-for-vehicles-tomorrows-high-tech-car>.

16. Cloud Computing can Reengineer the Car Interiors, 2012. Online.. Available: <http://www.cbrdigital.com/2012/01/16/cloud-computing-can-reengineer-the-car-interiors.html>.

17. A. Rae, “Helping the operator in the loop: practical human machine interface principles for safe computer controlled systems”, In Proc. of the twelfth Australian workshop on Safety critical systems and software and safety-related programmable systems, 2007, vol. 86, pp. 61-70.

18. H.Thimbleby, P. Cairns P. and M. Jones, “Usability analysis with Markov models”, *ACM Transactions on Computer-Human Interaction*, vol. 8, no. 2, pp. 99 - 132, 2001.

19. Lynn Walford, “Volvo New Connected Car Features-Magnets”, *Real-Time Cloud Road Data & Driver Sensing*, 2014. Online.. Available: <http://www.autoconnected-car.com/2014/03/volvo-new-connected-car-features-magnets-real-time-cloud-road-data-driver-sensing/>.

20. Michael Sheehan, “ Cloud Computing Cars and Mobile

Devices”, 2011. Online.. Available: <http://scoop.intel.com/cloud-computing-cars-and-mobile-devices/>.

21. Toyota and Panasonic develop cloud service to connect cars and household appliances, 2014. Available: http://panasonic.ru/press_center/news/detail/464204.

22. E. Bauer and M. Lotz, “PRORETA 3: An Integrated Approach to Collision Avoidance and Vehicle Automation”, *At – Automatisierungstechnik*, no. 12, pp. 755-765, 2012.

23. Internet Of Things Course - Immersive Programme Master in City and Technology, Available: <https://apps.uc.pt/search?q=Internet+of+Things>.

24. Master's programme in Information and Network Engineering, Available: <https://www.kth.se/en/studies/master/information-and-network-engineering/master-s-programme-in-information-and-network-engineering-1.673817>.

25. Master's programme in Communication Systems, Available: <https://www.kth.se/en/studies/master/communication-systems/description-1.25691>.

26. Master's programme in Embedded Systems, Available: <https://www.kth.se/en/studies/master/embedded-systems/description-1.70455/>.

27. Related Programmes to Embedded Systems and Internet of Things (ES-IoT) MSc, Available: <https://www.ncl.ac.uk/postgraduate/courses/degrees/embedded-systems-internet-of-things-msc/relateddegrees.html>.

43. INTERNET OF DRONE BASED SYSTEMS

Assoc. Prof., Dr. H. V. Fesenko (KhAI)

Contents

Abbreviations	437
43.1 Introduction into Drone Fleets.....	439
43.1.1 Advantages of using a drone fleet when comparing to a single powerful drone.....	439
43.1.2 Generic architecture for a drone fleet	441
43.1.3 Fleet construction	442
43.1.4 Types of a drone fleet	443
43.2 Internet of Drones.....	444
43.2.1 Communication and Protocols.....	444
43.2.2 Data collection.....	452
43.2.3 Data delivery.....	453
43.2.4 Internet of Drone based systems examples.....	453
43.3 Case studies	456
43.3.1 IoD for surveillance tasks in smart farms	457
43.3.2 Internet access and IoT services provision in remote and peripheral areas with IoD as Fog enabler	459
43.3.3 Targeted services delivery on big events with IoD.....	461
43.4 Security, safety and reliability of Internet of Drone based systems	463
43.4.1 Security of Internet of Drone based systems	463
43.4.2 Safety of Internet of Drone based systems	465
43.4.3 Reliability of Internet of Drone based systems.....	472
43.5 Work related analysis	477
Conclusions and questions.....	479
References	481

Abbreviations

ADC – Analog- to-Digital Converter
BS – Fixed Location Transceiver
BSP – Broadcast Storm Problem
CC – Crisis Centre
CD – Drone System Interface Controller
CH – Cluster Head
CS – Sensor Controller
CU – Controller Unit
CW – Wired System Interface Controller
DAC – Digital to Analog Converter
DCR – Data Centric Routing
DF – Drone Fleet
DM – Drone Monitoring System
DR – Drone Transmission System
DSDV – Destination- Sequenced Distance Vector
DSSS – Direct Sequence Spread Spectrum
DTN – Delay Tolerant Network
EASA – European Aviation Safety Agency
E2E – End to End
FAA – Federal Aviation Authority
FANET – Flying Ad hoc Network
FMEA – Failure Mode Effects Analysis
FODA – Flight Operations Data Analysis
GCS – Ground Control Station
GFMS – Ground Flight Management System
GSM – Global System for Mobile Communication
HiRP – Hierarchical Routing Protocols
HRB – Hybrid Routing Protocol
IoD – Internet of Drones
LCAD – Load Carry and Deliver Routing
MANET – Mobile Ad-Hoc Network
Mb – Monitoring Drones
MLH – Multilevel Hierarchical Routing
MTC – Machine-Type-Communication
M2M – Machine-to-Machine

N2N – Node to Node
PRP – Proactive Routing Protocol
RFID – Radio-Frequency Identification
Rj - Transmission Drone
RRP – Reactive Routing Protocol
SATCOM – Satellite Communications
Si – Sensor
SRI – Safety Risk Index
Srv – Redundant Sensor
SS – Sensor System
SW – switching units
UANET – Underwater Ad hoc Network
UAS – Unmanned Aircraft System
UAV – Unmanned Aerial Vehicle
U2I – Unmanned Aerial Vehicle-to-Infrastructure
U2U – Unmanned Aerial Vehicle-to-Unmanned Aerial Vehicle
VANET – Vehicular Ad hoc Network
WAN – Wide Area Networks
WBAN – Wireless Body Area Networks
WFANET – Wide Flying Ad hoc Network
WS - Wired System
WSN – Wireless Sensor Networks
ZSP – Zone Service Providers

43.1 Introduction into Drone Fleets

43.1.1 Advantages of using a drone fleet when comparing to a single powerful drone

Why should a drone fleet (DF) can be preferred to single, powerful drones (also known as drones/unmanned aircraft systems (UASs)/unmanned aerial vehicles (UAVs)). The coordination of a drone fleet allows accomplishing missions that no individual drones can accomplish on its own. DF members can exchange sensor information, collaborate to track and identify targets, perform detection and monitoring activities [1], or even actuate cooperatively in tasks such as the transportation of loads. The advantages of using a DF when comparing to a single powerful drone can be categorized as follows: multiple simultaneous interventions, greater efficiency, complementarities of fleet members, reliability, technology evolution, cost. A single vehicle with the performance required to execute some tasks could be an expensive solution when comparing to several low-cost vehicles performing the same task.

As illustrated Fig 43.1, the fleet is usually composed of several smaller drones that can be equipped with different sensors or other equipments providing redundancy that can help to tolerate a certain degree of failure. In addition, a multitude of drones can cover a larger geographic area than a single one. This can be performed in a smarter way, since only required drones with useful capabilities to support the mission can be sent to specific areas while other drones perform other tasks. However, large drones and smaller versions should not be opposed since they can be used in a complementary way; for example, in a multi-level fleet in which they can serve as relay (they can also be seen as cluster heads) for the smaller drones to enable communication with a GCS or with other DFs. In Fig. 43.2, a multi-level fleet is depicted.

It is worth noting that DFs presented before always received command from the GCS.

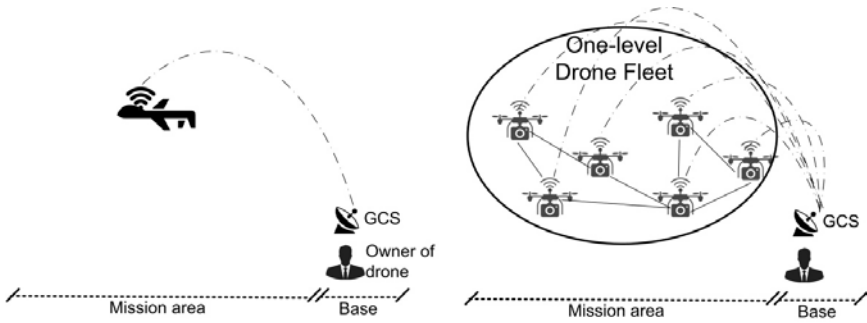


Fig. 43.1 – Single drone versus a one-level drone fleet

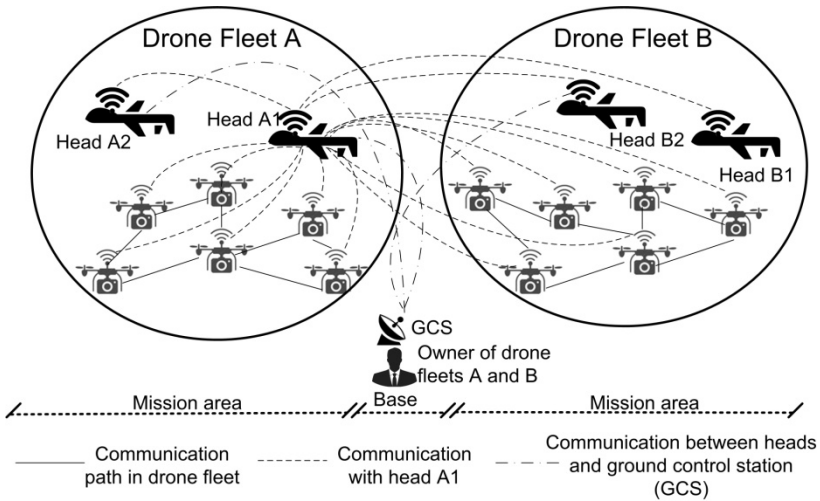


Fig. 43.2 – Multi-level drone fleet

Of course, they can have a certain degree of autonomy but a standalone DF, illustrated in Fig. 43.3 acting like swarm of animals/insects can be regarded as highly desirable for researchers and operators.

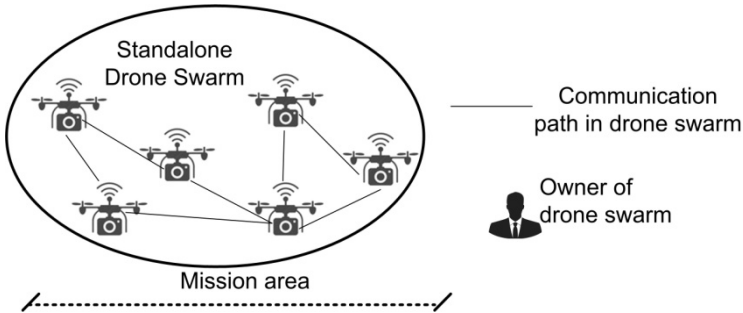


Fig. 43.3 – Standalone drone swarm

43.1.2 Generic architecture for a drone fleet

Consider generic architecture for the swarm variant of the DF. The conceptual architecture shows the set of operations in two different contexts: (1) how they are stacked in a single drone, for example, operations are that specific (or individual) to a drone and how it is related to other operations on the drone, and (2) how different operations are actually a collaborative options in which the swarm decides rather than individual drones. The architecture is divided into three layers with some duplication and each layer.

Layer 1. Drone Abstraction. This abstraction layer is focused on single drone operations, which preserves the drone as an individual entity and includes: D1 Flight Management; D2 Navigation; D3 Power and Performance Efficiency; D4 Service Level Maintenance; D5 Object Detection and Avoidance; D6 Individual Mission Objectives; D7 Security, Safety and Privacy Measures; D8 Self-Preservation.

Layer 2. Fleet Abstraction. This abstraction layer bridges between the decisions taken by individual drones on their own and the course of action that is stipulated as part of the mission brief from the DF owner, with feed in from the swarm abstraction layer in case an unexpected situation is encountered in the wild. This layer includes: F1 Flight Management; F2 Airspace Policy Management; F3 Navigation; F4 Flight Route Management; F5 Object Detection and Avoidance; F6 Mission Objectives; F7 Congestion Detection and Avoidance; F8 Secure Communication; F9 Trust Establishment and Verification; F10

Policy Consolidation and Harmonisation; F11 Power and Performance Management.

Layer 3. Swarm Abstraction. The services in this layer, similar to the other abstractions layers, are continuously running on individual drones. This layer has baseline knowledge: a collection of knowledge that is accumulation of all the DF flights managed the DF owner/operator. Therefore, learning, evaluation and decision formulation performed during a single mission then becomes part of the collaborative knowledge to improve all future missions. This layer includes comprises: S1 Swarm Community Management; S2 Security and Privacy; S3 Safety and Self-Preservation: Similarly to the S2, this service deals with safety and self-preservation of individual drones and DF as a whole; S4 Ethical Principles; S5 Mission Assessment; S6 Collaborative Learning; S7 Collaborative Evaluation; S8 Collaborative Decision Formulation; S9 Collaborative Knowledge Management.

43.1.3 Fleet construction

Based on the conceptual model, the first step is the formation of the DF at the pre-mission stage and deformation at the post-mission stage. At the pre-mission stage, DF construction process begins with the formulation of a mission – with a set of objectives. The mission control unit generates a mission brief that includes mission objectives, airspace regulations, ethical principles, security and privacy policies, organization commitments, baseline configuration (for first mission), and collaborative knowledge. The mission brief is then communicated to the ground flight management system (GFMS). After the completion of the mission, upon return of the DF participants to the base, the GFMS will connect with each drone to download the mission logs, learning/evaluation matrix and potential material that can contribute to the collaborative knowledge. The GFMS communicates this information to the mission control centre that would analyses the mission debriefing information and improves the collaborative knowledge. Fig. 43.4 shows the fleet construction process with both pre- and post-mission activities.

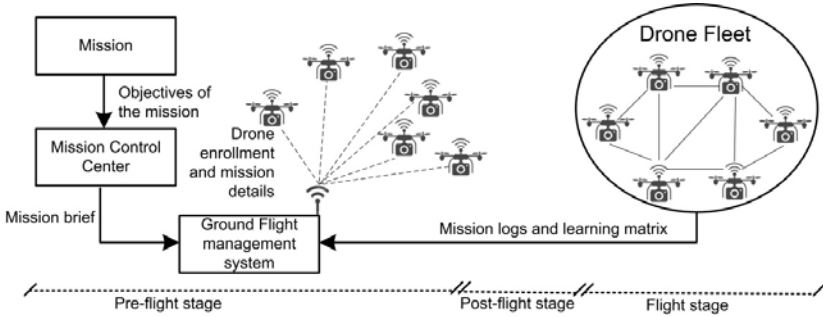


Fig. 43.4 – Drone fleet construction process – pre- and post-mission activities

43.1.4 Types of a drone fleet

Discuss three types of DF that can be potentially deployed depending upon the target environment and situation.

Static DF. The most basic type of the DF is the static DF. In this formation, the drones of the DF are pre-selected at the pre-mission stage. Fig. 43.5 shows the static DF in comparison with the dynamic DF.

Dynamic DF. In contrast to a static DF, a dynamic DF is open to the inclusion of new members along with existing members leaving the swarm at any point of time: pre-mission and/or during the mission.

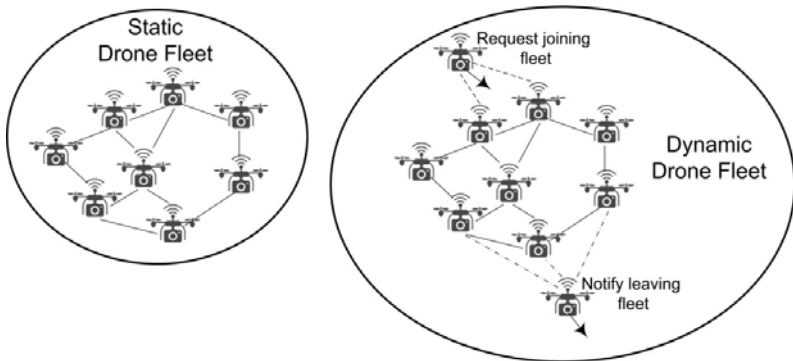


Fig. 43.5 – Static and dynamic drone fleets

Hybrid DF. This variant of a DF combines both the static and dynamic DFs together into a single collaborative unit. At the core of this DF is a static DF that behaves like one in all of its operations. Fig. 43.6 shows the hybrid DF construction.

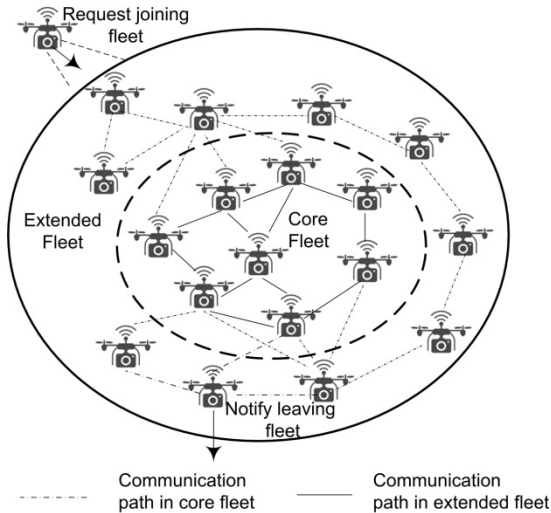


Fig. 43.6 – A hybrid swarm of drones

43.2 Internet of Drones

43.2.1 Communication and Protocols

Node-to-Node Communication. The study [2] presents different networking architectures for UAV-to-UAV (U2U) and UAV-to-infrastructure (U2I) communication that can be applied at the various layers of open system interconnection networking model. Since in-flight UAVs are highly mobile, mobile *ad-hoc* network (MANET) protocols are used for U2U communication where each UAV is considered as a mobile node in MANET. Besides, U2I refers to data exchange between UAVs and the infrastructure and the Internet. For this purpose, one of the UAVs plays the role of a gateway, where it collects the data from other UAVs (through U2U) and then relays the

collected data to the GCS. Li *et al.* [3] introduced two types of communication: 1) *centralized* and 2) *decentralized*.



Fig. 43.7 – Centralized UAV Network

Centralized communication (Fig 43.7) includes the most common topology that has a GS as the central node to which all the UAVs are connected. In this architecture, UAVs are not directly connected. The communication between two UAVs needs to be routed through the GS. On the other hand, a central node is not required in *the decentralized architecture*, where two UAVs can communicate either directly or indirectly employing a UAV as a relay. Consider three groups for decentralized communication architecture:

1) *UAV Ad-Hoc Network*: Each UAV participates in data forwarding for other UAVs of the network (Fig. 43.8).

2) *Multigroup UAV Network*: UAVs within a group construct a UAV *ad-hoc* network with its perspective backbone UAV connecting to the GS (Fig. 43.9).

3) *Multilayer UAV Ad-Hoc Network*: UAVs within an individual group construct a UAV *ad-hoc* network which corresponds to the lower layer of the multilayer *ad-hoc* network architecture. The upper-layer is composed of the backbone UAVs of all groups (Fig. 43.10).

Note that UAV *ad-hoc* network is more appropriate for a homogeneous group of UAVs, while a multilayer *ad-hoc* network is more suitable for connecting multiple groups of heterogeneous UAVs.

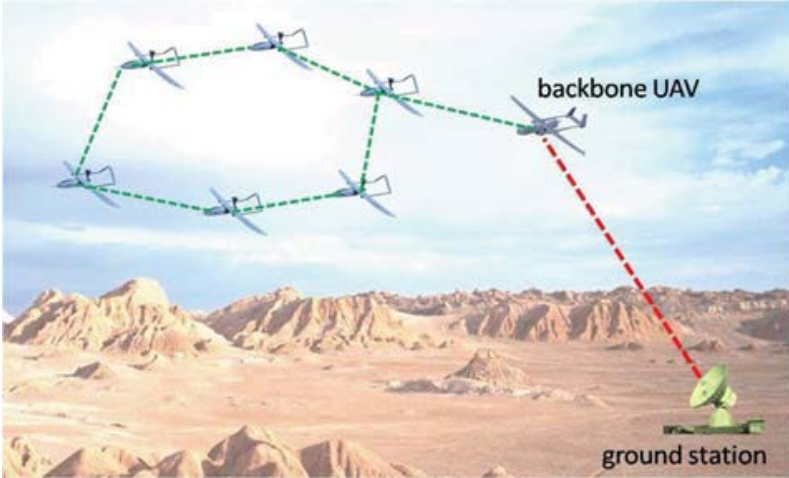


Fig. 43.8 – UAV Ad Hoc Network

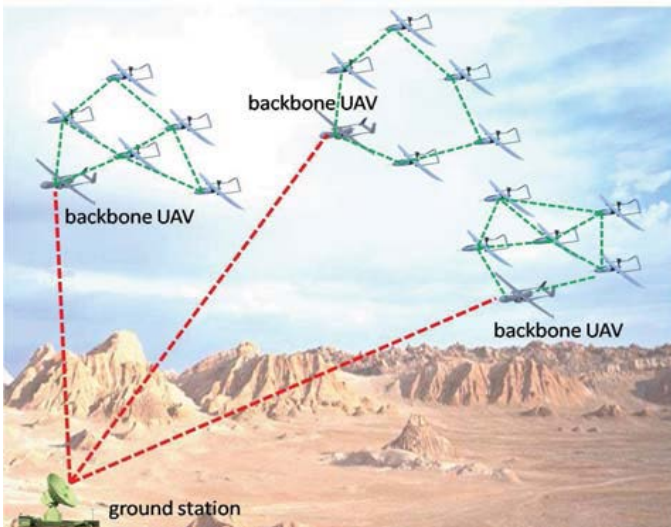


Fig. 43.9 – Multi-Group UAV Network

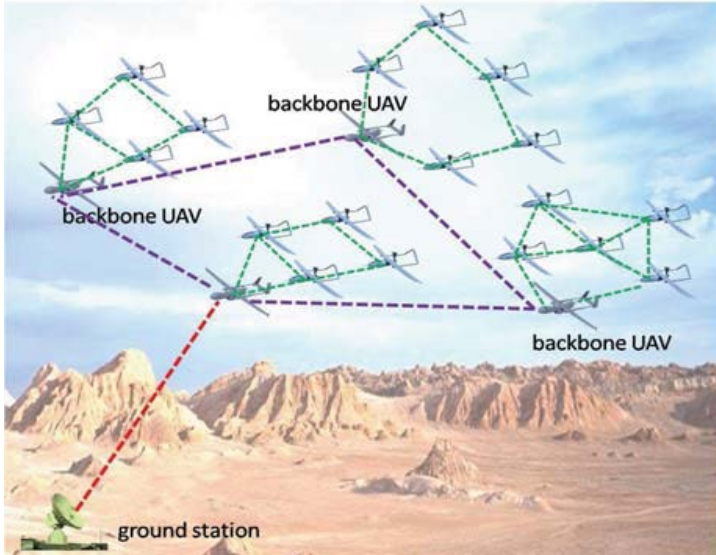


Fig. 43.10 – Multi-Layer UAV Ad Hoc Network

Mesh Networking. Mesh networking can be defined as an architecture, where every node, i.e., a UAV or GS, can act as a data relay (Fig. 43.11). Besides, communication among multiple UAVs and GS can occur over several hops through intermediate nodes [4].

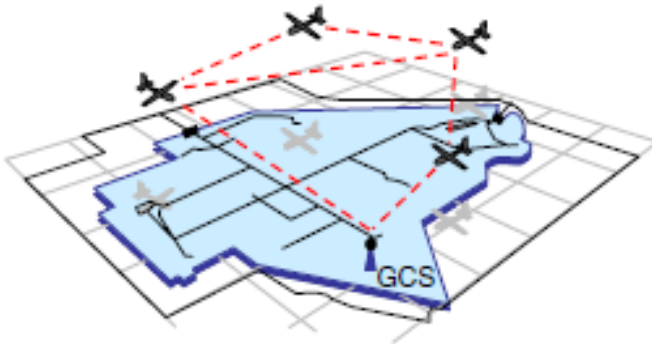


Fig. 43.11 – Mesh networking

The Delay Tolerant Network (DTN) architecture aims to provide interoperable communications between a wide range of networks that may have poor and disparate characteristics [5]. DTN architecture has been designed to address the needs of networks characterized by link intermittent connectivity, lack of end-to-end connectivity between end-users as well as high latency. In order to mitigate these problems, DTNs rely on store-and-forward message switching.

MANET/VANET/FANET Data Routing. The implementation of an ad hoc network connecting all vehicles is one of the most feasible alternatives to infrastructure-based communication. An ad hoc network is composed of nodes that also function as routers, forming a temporary network with no fixed topology or centralized administration [6]. Ad hoc networks are classified according to their implementation, utilization, communication, and mission objectives. If the nodes that compose an ad hoc network are mobile, the network is classified as MANET (Mobile Ad hoc Network). For vehicle-specific applications, MANETs are subdivided into UANET (Underwater Ad hoc Network) for aquatic vehicles, VANET (Vehicular Ad hoc Network) for terrestrial vehicles, or FANET (Flying Ad hoc Network) for aerial vehicles [7-12], as illustrated in Fig. 43.12. FANET nodes typically have higher mobility than those in other types of MANET. As a result, a FANET's network topology can change more frequently, which increases the overhead caused by connecting and routing operations.

Regarding the FANET protocols, they are classified into six major categories: 1) static; 2) proactive; 3) reactive; 4) hybrid; 5) position/geographic-based; and 6) hierarchical.

Static Routing Protocol. In static routing protocols, each UAV has a routing table that is not updated during the mission. Static routing protocols are applicable in cases when the topology of the network does not change and where the choices in route selection are limited. For example, in Load Carry and Deliver Routing (LCAD) model, a UAV store data from a source ground node, convey these valuable data by flying to a destination ground node as illustrated in Fig. 43.13. Another set of routing solutions for FANETs under static routing is the multilevel hierarchical protocols (MLH). MLH routing protocol is designed to deal with the network scalability issue. Here, the network

can be grouped into a number of clusters designated in different operation areas as illustrated in Fig. 43.14.

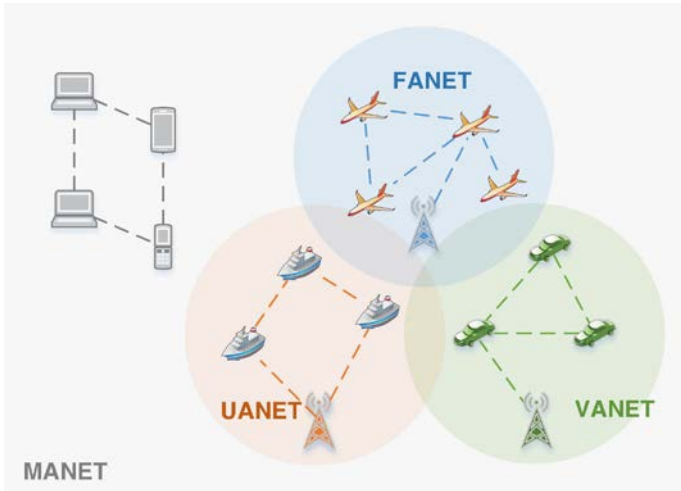


Fig. 43.12 – Relationships between different types of Mobile Ad Hoc Networks (MANET): Underwater Ad Hoc Networks (UANET), Vehicular Ad Hoc Networks (VANET), and Flying Ad Hoc Networks (FANET).



Fig. 43.13 – Load Carry and Deliver Routing



Fig. 43.14 – Multilevel Hierarchical Routing

Proactive Routing Protocol. The proactive routing protocol (PRP) is also known as a table. In this type of routing protocol, every node periodically maintains one or more tables indicating the complete topology of the network. Owing to the proactive nature, this routing protocol has advantage of having routes immediately accessible when needed.

Reactive Routing Protocol. The reactive routing protocol (RRP) is also known as on demand routing protocol, means it discovers or maintains a route on demand. The routing table here is periodically updated, when there is some data to send, if there is no connection between two nodes, there is no need to calculate a route between them.

Hybrid Routing Protocol. The hybrid routing protocol (HRB) is a combination of both proactive and reactive routing protocols, taking the best features and to overcome the limitations from both worlds. Reactive routing protocols generally need extra time to discover route and proactive routing protocols has huge overhead of control messages. These shortcomings can be mitigated by using HRP. Hybrid protocols are especially appropriate for large networks, and is based on the concepts of zones where intra-zone routing is executed with the help of proactive routing and inner-zone routing is achieved using the reactive routing approach.

Geographic/Position Based Routing Protocols. Position-based routing protocols have been proposed to assume knowledge of the geographical position information of UAVs to support efficient routing. In this type of protocols, they assume that the source UAV knows about the physical position of the communicating UAVs and sends message to the destination UAVs without route discovery..

Hierarchical Routing Protocols. In hierarchical routing protocols (HiRP) the ability of choosing proactive and of reactive routing rely on the hierarchical level of the network in which a UAV resides. This specific routing is primarily determined with some proactive planned routes and then helps the request from by triggered nodes through reactive protocol at the lower levels.

WFANETs Data Routing. The Wide FANETs (WFANETs) merge the concept of FANETs with IoT, and take wide area networks (WAN) as an inspiration to benefit from all paradigms. A visual representation is seen in Fig. 43.15, which illustrates a real scenario with WFANETs.

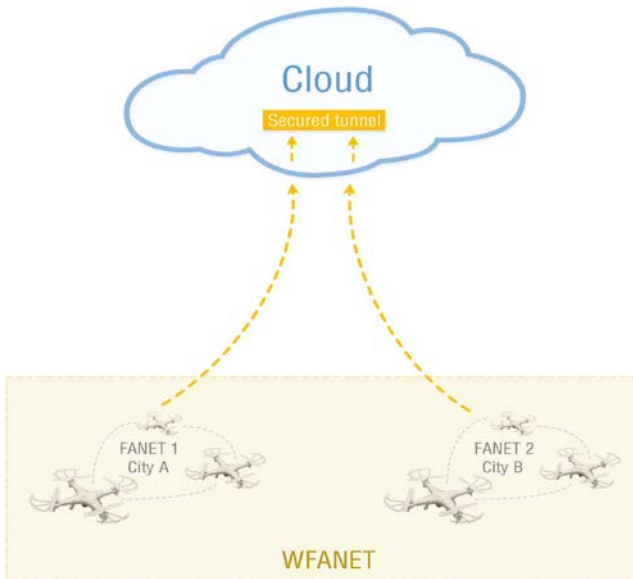


Fig. 43.17 – A Wide FANET.

WFANETs are used for different approaches and applications. A good example is big events, for example, football matches, Olympic games, and concerts, which require high security in order to manage large crowds, monitor suspicious activities, manage ongoing events, and so on. Another example of application improved by WFANETs is the pavement scanning for distress, helping the provision of better quality roads.

43.2.2 Data collection

The basic task of UAS is collecting data using onboard IoT devices and utilities. UAVs can utilize intelligent interfaces for connecting devices, machines, smart objects, smart environments, services and persons so they share their collected data from embedded sensors, actuators and other IoT member utilities. UAVs collect the data from remote locations and share them with a GS.

Data collection and reporting methods can be classified into the following [2]: time driven, space driven, space-time driven, event driven, query driven, space-query driven.

UAS could be equipped with a variety of multiple and interchangeable imaging devices including day and night real-time video cameras in order to capture real-time video. Some of these devices are video camera, digital camera, infrared cameras, multispectral and hyperspectral sensors, biological and radiological sensors. Note that some requested data needs to be collected from more than one type of sensors, like the heat index that is calculated from the temperature and humidity.

Sensors are the fundamental IoT utilities of any data collecting devices. They have an integral role in subsequent data transmission and data processing. Sensors and their associated circuits are applied to measure various physical properties. There are different types of physical quantity sensors: mechanical sensors; heat sensors; radiation sensors, chemical sensors, other types of sensors (touch, contactless, linear (analog), digital (numeric), compound, and integrated). These sensors increase the ability to measure, analyze, and aggregate data at a much localized level.

Actuators are other IoT devices applied with the UAVs. They are mechanical devices that convert energy into motion, i.e., digital data into physical actions. Some of these devices are electric servo-actuators, high performance low-weight compact servo actuator that is applied for flap control and other UAV applications.

43.2.3 Data delivery

There are the following communication technologies for UAVs: Cellular Systems, WiMAX (802.16), Satellite Communications, Wi-Fi (IEEE 802.11), Bluetooth (IEEE 802.15), Zigbee (IEEE 802.15.4).

Machine-type-communications (MTC), or alternatively machine-to-machine (M2M) communications, refers to data communication among IoT devices without any human intervention. M2M devices cover a broad variety of applications; e.g., eHealth, surveillance, and security, intelligent transport system, city automation, etc.; in a wide range of domains, influencing different markets and environments. M2M is considered as the key enabler of the IoT vision. MTC is expected to connect an enormous number of devices, where it is expected to reach 50 billion M2M devices by 2020. Usually, M2M devices can communicate either among each other directly.

43.2.4 Internet of drone based systems examples

The Internet of Drones (IoD) is an architecture designed for providing coordinated access to controlled airspace for drones.

The IoD is indeed flexible. This characteristic is important for the provision of almost every feature in such model. It helps increase overall cooperation and collaboration, is ready for real-time operations, is usually up-to-date due to the highly connected environment and easy access to the Internet, and is assisted by a powerful remote cloud and/or local fog structure. In terms of cost, since the IoD merges the benefits of two well-known paradigms, namely, IoT and UAVs, which may vary from cheap to expensive commercial off-the-shelf products, there will be an affordable and adaptive solution for most needs.

Cooperation and collaboration are desired features for most of modern computing systems. Many modern applications distribute tasks

and share information in real time, providing better results quickly. In particular, an IoT-ready environment is usually designed to be equipped with more than one way of acquiring data, interacting, and automating specific tasks. Although IoT is a scalable model, its expansion can mean high costs for relatively small returns. If an environment does not expand easily, it might have its flexibility compromised, resulting in limited cooperation and collaboration. IoD addresses this tension in different ways—such as by setting up UAVs in strategic areas serving as gateways, fog, or cloud data link providers, and also by being capable of replacing sensors and actuators in more active and inexpensive ways (for instance, if a traffic light fails, a flying thing might be used to temporarily replace its task). Moreover, real-time operations are also a priority of the model, since it can be reconfigured to meet requirements and provide the best connection to servers and services available locally or through the Internet.

The IoD integration with IoT infrastructures achieved by strategically positioning UAVs which helps the model to meet some key features. Linking to internet-based information processing can collate services from all around the world in real time, providing valuable up-to-date accurate information.

This in turn can facilitate interactive decision-making in response to dynamic situations. Those decisions can be processed in powerful datacenters available as cloud providers. The net result is to allow more reliable and more adaptive missions, maximizing their potential benefits, or broadening their applicability.

Table 43.1 summarizes these IoD features in comparison with UAVs and IoT paradigm. IoT and UAS segments are limited by their inherent infrastructure characteristics. Although they can be expanded, the setup cost, for instance, is a con that must be considered, especially if such infrastructure might end up being underused. In such case, the use of flexible flying things for sensing and actuating is an advantage.

The architecture comprises two groups of components: *Zone Service Providers (ZSP)* and *drones*. All ZSPs and drones are connected to the cloud, so communication between any two components is possible.

Consider a layered architecture for IoD. Layering provides many benefits such as the separation of concerns, scalability, maintainability

of the code base, and flexibility of modifying a layer with minimal changes needed to the other layers. The fundamental goal that the architecture is concerned with is to enable drones to perform various applications by providing common generic services for all applications.

Table 43.1 – A comparison of available features of unmanned aircraft systems, Internet of Things, and the Internet of Drones

Features	Internet of Things (IoT)	Unmanned aircraft systems (UAS)	Internet of Drones (IoD)
Cooperation	Limited by IoT infrastructure	Limited by FANET infrastructure	Includes all the IoT and FANET infrastructure capabilities
Collaboration	Limited by IoT infrastructure	Limited by FANET infrastructure	Includes all the IoT and FANET infrastructure capabilities
Real-time operations	Limited to the network coverage	Limited to the actuation areas	Reduced limitations due to increased connectivity
Connectivity	Internet connected	Locally connected by a FANET	Highly connected—not just to the Internet, but also locally connected
Up-to-date data/ services	Available	Weakly available	Available
Internet-based information processing	Available	Weakly available	Available
Interactive decision-making	Available	Available	Available with higher flexibility
Mission-assistive Multisource information providers	Available	Weakly available	Available with higher variety of sources

The proposed architecture consists of five layers as shown in Fig. 43.16

Application
Service
End to End(E2E)
Node to Node (N2N)
Airspace

Fig. 43.16 – Layers in the architecture of IoD.

1) Airspace Layer. The airspace layer is required to implement the following features along with the needed protocols and interfaces for using these features: *map; airspace broadcast and track; plan trajectory; airspace precise control; collision avoidance; weather condition*

2) Node to Node Layer. The features required for the node to node layer is as follows: *zone graph; N2N broadcast and track; plan pathway and contingency; refuel; N2N precise control; emergency; congestion notification.*

3) End to End Layer. The end to end layer must implement the following features: *interzone graph; routing; handoff; explicit congestion notification*

4) Service Layer. The service layer is an extensible layer that currently has the following mandatory feature and can be extended to add more services in the future as needs arise. The main role of the service layer is to provide a common platform where zone-related messages can be broadcast to the drones.

5) Application Layer. There is no feature requirement for the application layer. These are the applications that will be written in the future to use the architecture. The point of having a general airspace navigation and control service along with other services as is provided by the four layers of airspace.

43.3 Case studies

Three case studies will be carried out in this section exemplifying real-world applications of the IoD. The first is on smart farms

highlighting WFANETs application. The second is on the provision of Internet access and IoT-based services on remote areas, especially on rural zones and peripheries of smart cities. Finally, the third case study is on the management of big events and provision of targeted services.

43.3.1 IoD for surveillance tasks in smart farms

Although smart farms are already benefiting from IoT, they still have limited connectivity to the Internet, which usually leads to big areas with no connectivity and no surveillance. Thus, network structures that do not depend on Internet connections have been applied as temporary alternatives for monitoring animals, crop fields, forests, schools of fish, and so on. It is common to find wireless sensor network (WSN) and wireless body area networks (WBAN) spread in many fields. However, the feedback from these networks and sensors is frequently limited, delayed, and poorly updated, which leads to less dynamic operations and limited overall farm management.

The problem addressed in this case study is related to general surveillance of a smart farm, including farm borders, controlled cattle, or suspect activities within the farm field. Such problems get bigger and more complex according to the farm size and also due to the number of different tasks that demand monitoring for safety and security reasons. They can also be considered critical since high value assets are put at risk.

Discuss the hypothetical application of FANETs and WFANETs to three farm scenarios: border control, cattle monitoring, and crop monitoring. Fig. 43.17 illustrates the scenarios discussed further.

The surveillance of farm borders to identify potential threats, such as intruders (humans or not), and trigger appropriate procedures is one of the most important tasks for safety purposes. In a typical scenario, the task would be performed by human patrol and/or surveillance cameras. This solution, besides costly, is not likely to be effective, since the risk of human failure is always present.

A WFANET would provide border control at a lower cost. The UAVs would gain from the available IoT infrastructure to provide surveillance images or data in real time to a control central (e.g., for security guards, a specialized security company or a police station). The

use of UAVs would reduce the necessity of surveillance cameras installed over the property border and its required infrastructure (such as batteries or solar cells for power), again reducing the task cost. The advantages would be even bigger in bigger farms, since the use of WFANETs would allow the exchange of relevant information among more than one local FANET, in a cooperative live border monitoring.

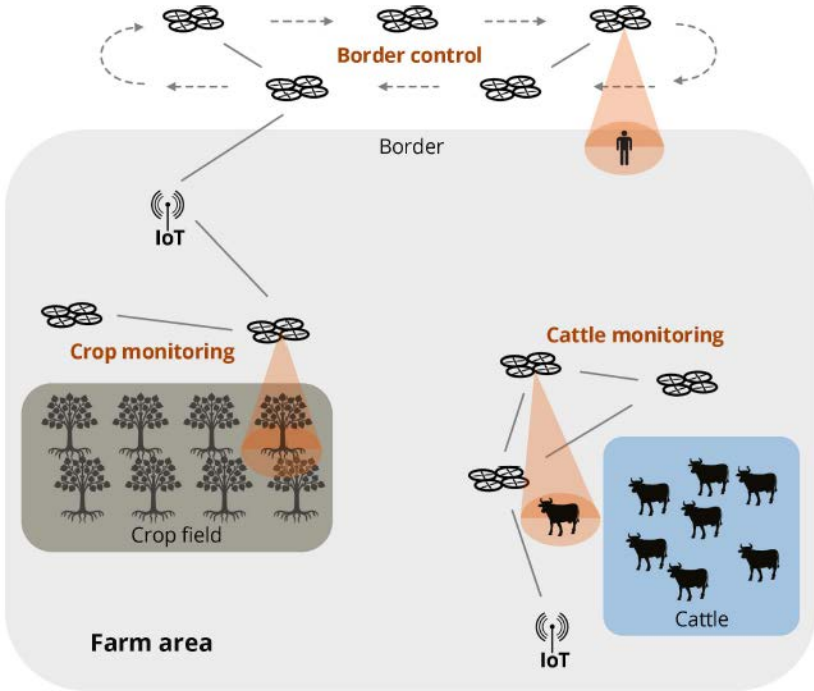


Fig. 43.17 – Surveillance situations for the study of WFANET's application in smart farms.

An IoT infrastructure would provide means of cattle tracking by installing cheap sensors in each single animal. Moreover, by surveying the area with UAVs, data acquisition would flow fast from the cattle raising area to monitoring centers, providing means of taking timely actions. As an alternative, automatic actions could also take place as soon as an unwanted behavior is identified, for example, closing

backup gates in case of cattle escape. For that, FANETs (in small areas) or WFANETs (in bigger areas) would identify and trigger the appropriate action.

The surveillance of crop fields can be motivated by several factors, such as early identification of pests and plagues, soil checking, and weather conditions monitoring. Once again, appropriate local actions could take place as soon as an atypical situation is identified. In such case, more accurate information could be acquired by starting specialized missions with FANETs and/or WFANETs based on the additional information required to precisely recognize a countermeasure. UAVs can collect data from wireless sensor networks placed on the ground at strategic frequency, being able to transmit such data in real time to monitoring centers. Moreover, such data collection frequency could be based on weather conditions, originating from both local sensor and web services.

43.3.2 Internet access and IoT services provision in remote and peripheral areas with IoD as Fog enabler

Rural areas and city peripheries might be the trickiest areas for provision of Internet/IoT-based services, especially due to the lack of appropriate infrastructure. In most of the cases, it is not worth installing a full infrastructure that will be rarely used in remote areas. The downtown of a smart city is likely to be the geographic region to first experience novel efforts and updated technologies, while the peripheries will usually be the last ones to face a full integration and also to get relevant investments. That is the natural process given a business model full of potential opportunities which focuses on highly populated areas to be profitable.

In a different context, rural areas might not need Internet connectivity at all times, but they do need to update/synchronize data at some stage. For this, data mules can be used, for example, in vehicles that physically carry computers with dedicated storage servers allowing a slow, limited, once-a-day synchronization. Although this approach can be considered inexpensive and efficient in many situations, it is poorly flexible and does not provide the benefits of a fully connected infrastructure. The same issue is experienced in emergency situations,

for example, search and rescue. A local network infrastructure does not provide the real-time support that such an operation would need to properly and efficiently do the search and also the rescue tasks. In some cases, the inexistence of cellular network coverage limits even more the connectivity, which leads to the necessity of a flexible, inexpensive, easy-to-set-up approach.

Pursuant to such issues, the IoD paradigm might be a relevant alternative of either temporarily or permanently minimizing the already discussed problems. Next subsection will discuss proposed solutions for recurrent cases demonstrating how this paradigm would solve practical cases.

Here, three main applications of this case study will be highlighted. The first investigates how an IoD network would be important for smart cities peripheries. The second addresses the environmental monitoring in rural areas helping the environmental police to identify illegal actions and take appropriate countermeasures. Last, natural phenomena and emergency operations support are discussed considering that in such situations connectivity becomes an issue due to the loss of infrastructure nearby. Fig. 43.18 illustrates the scenarios that will be discussed further.

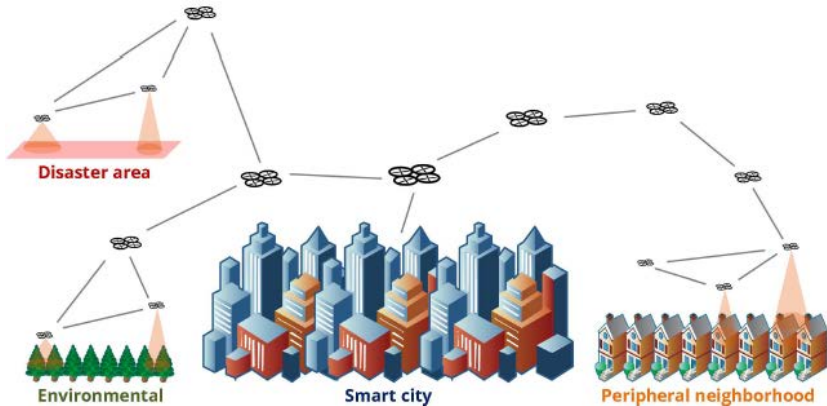


Fig. 43.18 – Applications of IoD in smart cities

By strategically moving drones to the edges of smart cities, a powerful connection to the Internet will be available for restricted areas

helping with the provision of connectivity to city peripheries. From this connection, a complete range of IoD services will be available for end users nearby for a specific period, allowing the execution of relevant tasks.

For instance, the smart city's electric power company might automate the reading process of residential energy consumption. Such task is usually performed by a person taking note about the consumption in each residence/building, which takes more time and is susceptible to misreading. Applying appropriate identifiers to each residence, which in turn will be recognizable by the IoD infrastructure, would provide means of reading the energy consumption of a big area in several minutes. That is possible due to the existence of a FANET/WFANET flying over the area, providing such class of services and being able to provide real-time information to both the customer (e.g., bad debt warnings) and the electric power company (e.g., reading issues in specific residences that would require a technical visit).

The concept of fog computing is clear in this situation, but the IoD network emerges as an enabler of the model. This model meets the requirements of environmental monitoring by governmental official agencies, which is a trend due to the global issues being reported lately. The real-time monitoring by flying things can be remotely analyzed by specialists in central offices that will be able to use updated images to identify suspicious activities. If an environmental illegal practice is taking place, the environmental police can promptly move to the region being supported by the IoD infrastructure at all times, allowing efficient redhanded operation.

IoD in emergency situations will provide connectivity for basic services provision, governmental central offices, and news agencies to be updated with recent discoveries, and the complete support for ambulances being moved to the target area.

43.3.3 Targeted services delivery on big events with IoD

In big events one of the most alarming problem is to lose people, especially children. Sometimes a cellular network signal will not be available and finding someone in a crowded area is almost an impossible mission for one person.

The applicability of IoD in the cited situations might be a simple and efficient solution. The following subsections will discuss two cases specifically. First, the application of finding people will be discussed. Second, real-time information about multiple venues in music festivals will be addressed. Figure 43.19 presents the scenario of this case study.

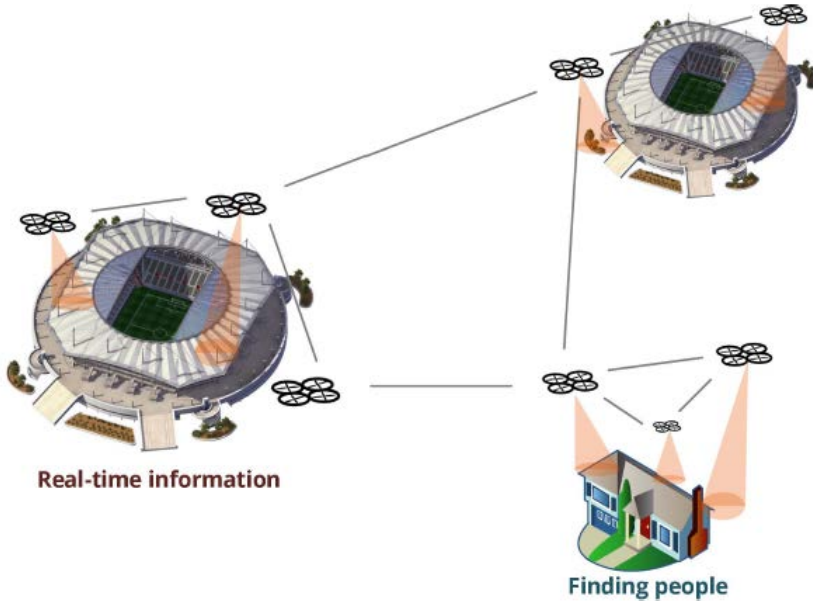


Fig. 43.19 – Applications of IoD in big events

It is common to suddenly find yourself separated from your friends or family in crowded places. If a cellular network is not available for any reason or your phone ran out of battery, then you might have a problem. Plus, the situation gets even worse if a kid is lost by any reason and the parents are desperately looking for him/her.

The identification of people using fixed cameras coupled to the infrastructure of venues is efficient most of the times. However, in crowded places the angle of the camera might be a problem. In case of lost children, it is even more problematic, since the height would negatively influence the camera coverage.

For cases like this a reasonable solution would be a drone connected to a FANET/WFANET for accurate, fast search on site.

The real-time streaming can be monitored by trained people and also relatives. Such effort would significantly reduce the chances of any hurt to an unattended child and also provide effective means to supporting families. Another relevant topic in big events, especially the ones with simultaneous attractions in multiple venues, is the possibility of getting access to information in real time. One can wonder whether a concert meant to be played at a specific time has started or is delayed. Moreover, why not have access to the audio or a video streaming to check how is the performance going or how crowded it is?

An IoD network plus fixed cameras and sensors could provide a set of information about multiple venues in real time to a central server that would redistribute such information all over the network. Personal smart phones or special stations could get access to such information, improving the delivered services during the days of the event.

43.4 Security, safety and reliability of Internet of Drone based systems

43.4.1 Security of Internet of Drone based systems

In general, security challenges are big concerns of computing systems. There are several security issues that could exist in IoD-based applications, which are mostly inherited from the underlying networks and technologies (e.g., UAS, IoT). The main security issues that could be imposed by the different network layers are listed as follows [1]:

Physical Layer. Both jamming and tampering attacks are known issues for this layer. Jamming is a well-known attack that causes interferences to the radio frequencies that network's nodes are using. It can interrupt the network if a single frequency is used throughout the network: at worst, interrupting communications with flying things; and at best causing excessive energy consumption. On the other hand, if an attacker can physically tamper nodes, a tampering attack takes place which damages, replaces, and electronically "interrogates" the nodes to acquire information GPS spoofing attacks, which happen in this layer, consist in the use of a signal that is stronger than and mimics the

attributes of a genuine GPS signal to take over a GPS receiver, have become more frequent. Such attacks can cause the aircraft to completely lose control, which is a very critical issue.

Data Link Layer. Collision, exhaustion, and unfairness are the most likely attacks at this level. A collision happens when two nodes simultaneously attempt to transmit on the same frequency, resulting in either partial or complete packet disruption, which will cause an erroneous data transmission through a communication channel. In an IoD, it is a big issue because the possibility of having an intermittent network condition is likely to cause chaos in a FANET.

Network Layer. There are several attacks found on this layer. In a selective forwarding attack, malicious nodes attempt to stop the packets in the network by refusing to forward or drop messages passing through them, which could compromise a FANET that relies on strategically placed flying things to reach all the destinations within the network. If an attacker makes the compromised flying thing look more attractive to surrounding ones, which is considerably an easy task since IoD applications usually take place in open environments, the selective forwarding attack becomes very simple. Then, through the affected flying thing, a data transfer situation may be started leading to a sinkhole attack. Another attack on network layer is the Sybil attack, in which a flying thing exhibits multiple identities to other flying things in the network.

Transport Layer. Flooding attack causes immense traffic of useless messages on the network. It may result in congestion, and eventually lead to nodes exhaustion. The desynchronization attack is made when the adversary repetitively pushes messages, which convey sequence numbers to one or both of the endpoints. The GPS spoofing may help attackers to hijack flying things, which is another issue that is strongly related to situations where an attacker secretly relays and possibly alters the communication between two parties, also known as man-in-the-middle attacks. This kind of attack allows an attacker to land the flying thing in an unauthorized place, and taking advantage of its legitimate network access. However, such problem can be neutralized by the high connectivity in IoD environments: In most cases, a solution lies in techniques that check the accuracy of GPS signals by comparing to the ones provided by access points and other fixed known infrastructures.

Perception Layer. This layer is mainly about information collection, object perception, and object control. In the perception layer within the IoD, tasks related to security of RFID (radio-frequency identification), WSN, RSN (RFID Sensor Network), GPS technology, and so on will be performed.

Transportation Layer. Also referred to as network layer, the transportation layer's main function is transmitting information obtained from the perception layer. This layer encompasses the Wi-Fi, establishing and maintaining MANET/FANET and 3G/4G/5G networks, leading to a heterogeneity problem for the exchange of information among different networks, which is even more challenging when it comes to the IoD and its inherent integration among different networks (IoT, FANETs)..

Application Layer. This layer supports all sorts of business services and realizes intelligent computation and resources allocation in screening, selecting, producing, and processing data. The security issues it faces cannot be solved in other layers of the IoT model, such as privacy protection issue, which can become a real demand in certain special contexts. The application layer can be organized in different ways according to different services, and usually includes middleware, M2M, cloud computing platform, and service support platform [13]. Thus, the attacker may still use it as a gateway to obtain information from the network, since the flying thing is authorized and will be able to access private and confidential information. This is a consequence of the high connectivity of things and the increased contact surface that generates more possible threats to be explored by malicious entities.

43.4.2 Safety of Internet of Drone based systems

The European Aviation Safety Agency (EASA) will require a documented safety risk assessment performed by the operator and a manual of operations, which lists the risk mitigation measures for all unmanned drones with 'specific' operation purposes (as per EASA A-NPA 2015-10).

The Federal Aviation Authority (FAA) requires a preflight assessment including risk mitigation actions so that small unmanned aircraft will pose no undue hazard to other aircraft, people, or property

in the event of a loss of control or other safety hazards (as per FAA NPRM RIN 2120–AJ60).

The drone flight safety is the desired optimum state in which drone operations executed in certain circumstances can be controlled with an acceptable operational risk. By performing a safety risk assessment, commercial industry could help in advance to identify drone operation safety hazards. The UAS safety risk assessment, based on a systematic approach from safety hazard identification to risk management, ensures the maintenance of the required safety standards for drone operations. Drone Industry Insights presents a four-phase model of a UAS safety risk assessment. This approach is an appropriate solution, which fits according to the effort and usability, in everybody's organization. This model, which should be used for drone flight permission and insurance applications, is the fundamental frame for a safe and reliable organization set up. Not only the results but also the whole UAS safety risk assessment process should be documented to ensure a continuous safety assurance

The UAS safety risk assessment is an instrument used to identify and assess active and latent safety hazards for drone operation. This safety risk assessment includes actions for mitigating the predicted probability and severity of the consequences or outcomes of each operational risk. An UAS safety risk assessment makes safety risks measurable so that risks can be better controlled. We recommends to separate the UAS safety risk assessment into the following four phases.

1) Safety Hazard Identification: Occurrences such as near misses or latent conditions, which led or could have led to drone operational flight safety harm, will be identified.

2) Safety Risk Assessment: All identified hazards will be assessed, according to the operational risks severity and operational risk probability.

3) Safety Risk Mitigation: According to the operational risk acceptance level, risk mitigation action will be defined.

4) Safety Documentation: Not only the results but also the whole UAS safety risk assessment process should be documented to ensure a continuous safety assurance.

Safety Hazard Identification. With the first phase of the UAS safety risk assessment, we shall collect and identify operational drone

safety hazards separated into “active failures” and “latent conditions”, both of which occur or might occur during the flight operations. Active failures are actions – including errors and violations – that have an immediate effect. Generally, they are viewed as unsafe acts. Active failures are generally associated with front-line personnel (pilots, air traffic controllers, engineers, and so on). Latent conditions are those that exist in the UAV system well before a damaging outcome is experienced. Initially, these latent conditions are not perceived as harmful, but could become evident once the system defenses are breached. People removed in time and space from the event generally create these conditions.

Safety hazards identification methodologies.

1) Reactive: This methodology involves analysis of past outcomes or events. Hazards are identified through investigation of safety occurrences. Incidents and accidents are clear indicators of system deficiencies; therefore, they can be used to determine the hazards that contributed either to the event or to the latent.

2) Proactive: This methodology involves an analysis of existing or real-time situations during drone operation.

3) Predictive: This methodology involving data gathering is used to identify possible negative future outcomes or events during drone operation, analyzing system processes and the environment, to identify potential future hazards, and to initiate mitigating actions.

The following methods can be used to identify safety hazards:

- 1) Flight Operations Data Analysis (FODA).
- 2) Flight Reports.
- 3) Maintenance Reports.
- 4) Safety (& Quality) Audits / Assessments.
- 5) Voluntary reporting of Incident/accidents/near misses.
- 6) Mandatory accident reporting to the competent authority.
- 7) Brainstorm acc. to Failure Mode Effects Analysis (FMEA).
- 8) Surveys.

The identified safety hazards must be run through a root-cause analysis to identify the safety hazards causes and their potential consequences. The potential outcome shall be assessed according to their risks in the next phase, the UAS safety risk assessment.

Safety Risk Assessment. The second phase, the UAS risk

assessment, measures the projected probability and severity of the consequences of the identified safety hazards of drone operation. This phase presents the fundamentals of safety risk management.

Safety risk probability. The safety risk probability is defined as the likelihood or frequency that the consequence of safety hazard might occur. All scenarios should be taken into consideration. The probability must be categorized into criteria such as numbers. These numbers should be assigned to each probability level. Table 43.2 displays a common used five level probability table. It is possible to extend the safety risk probability to 6, 10, or 15 values.

Table 43.2 – Common used five level probability table

Lekelihood	Detail (“customized example”)	Value
Frequently	Likely to occur many times or has occurred frequently (“five times during operation”)	5
Occasional	Likely to occur sometimes or has occurred infrequently (“every second operation”)	4
Remote	Unlikely to occur, but possible or has occurred rarely (“I know it from some events”)	3
Improbable	Very unlikely to occur or not known to have occurred (“It happened once and I heard about it from other operator”)	2
Extremely improbable	Almost inconceivable that the event will occur (“never happened”)	1

UAV safety risk severity. The safety risk severity is defined as the extent of harm that might reasonably occur as an outcome of the identified safety hazard. The severity assessment can be based on injuries (persons) and/or damages (Drones and buildings, power lines, or the cost dimension). The levels of severity are shown in Table 43.3.

Additionally risk assessors often use the “probability of detection” as a third dimension of the risk assessment (comparing to risk severity and probability). This dimension is commonly required in the product development, and it involves natural or technical safety barriers.

Table 43.3 –Typical five levels of severity

Severity	Customized Detail	Value
Catastrophic	Death to people; Drone, equipment or buildings destroyed	E
Hazardous	Serious injury to persons; major equipment or buildings damage	D
Major	Injury to persons; Further operation not possible without major adjustments	C
Minor	Minor incident to persons; Minor effect on system performance	B
Negligible	No injury to persons; Minor consequences on system	A

UAV safety risk acceptance. The third step in the UAV safety risk assessment process is to determine the safety risks that require actions. The safety risk acceptance indicates the combined results of the safety risk probability and safety risk severity assessments. The respective assessment combination is presented in the safety risk assessment matrix shown in Table 43.4.

Table 43.4 – Safety risk assessment matrix

Safety risk probability	5	5A	5B	5C	5D	5E
	4	4A	4B	4C	4D	4E
	3	3A	3B	3C	3D	3E
	2	2A	2B	2C	2D	2E
	1	1A	1B	1C	1D	1E
		A	B	C	D	E
Safety risk severity						

Safety risk probability	5	5A	5B	5C	5D	5E
	4	4A	4B	4C	4D	4E
	3	3A	3B	3C	3D	3E
	2	2A	2B	2C	2D	2E
	1	1A	1B	1C	1D	1E
		A	B	C	D	E
Safety risk severity						

This UAS safety risk matrix can be customized according to the UAS Company's business or safety policy.

The combination of risk probability and severity indicates following:

1) The safety risk acceptance level: 1. Red is not acceptable 2. Yellow is tolerable but requires risk mitigation 3. Green is an acceptable level

2) The UAS safety risk index (SRI) can be used as an Indicator for statistical data acquisition and for a "before/after comparison" to measure the efficiency of a UAV safety risk management. Then, the UAS safety risk matrix must be exported to a safety risk acceptance matrix to determine the required actions that will mitigate the unacceptable and tolerable safety risks to an acceptable status.

Safety Risk Mitigation. The UAV safety risk mitigation explains the approach to react to unacceptable or tolerable UAV safety risks. It is a systematic reduction of the risk severity and the probability of its occurrence.

The UAV safety risk acceptance matrix (Table 43.4) provides information about the required actions for the strategies of risk mitigation:

1) Unacceptable - the probability and/or severity of the consequence is intolerable. Major mitigation or redesign of the system is necessary to reduce the probability or the severity of the consequences of the safety hazard to an acceptable level.

2) Tolerable level - the consequence and/or likelihood is of concern; measures to mitigate the risk to a reasonably low level should be sought for. This risk can be tolerated if the risk is understood and if it has an endorsement within the organization.

3) Acceptable level - the consequence is very unlikely or not severe enough to be of concern. The risk is tolerable and the safety objective has been met. However, consideration should be given to reduce the risk further to a reasonably practical level.

Table 43.5 – UAV safety risk acceptance matrix

Acceptance level	Assessed UAS safety risk index	Recommended actions
Unacceptable	3D, 4D, 5D, 1E, 2E, 3E, 4E, 5E	Immediate mitigation action and escalation is required; An operation stop should be considered
Tolerable	4A, 5A, 3B, 4B, 5B, 1C, 2C, 3C, 4C, 5C, 1D, 2D	The safety risk shall be mitigated as low as reasonable practicable and should be approved
Acceptable	3D, 4D, 5D, 1E, 2E, 3E, 4E, 5E	No action required

UAV safety risk mitigation actions can be separated into two dimensions:

1) Corrective actions - Actions with an immediate effect for the safety hazard.

2) Preventive actions - Actions that have a long-term effect on the safety hazard to mitigate the risk to an acceptable level.

The UAV safety risk mitigation describes the last step of a UAV safety risk assessment. The question, if a continuous review of UAS safety risks and a safety performance increase is necessary, is obsolete. UAV safety risk documentation and documented risk management procedures are required and are described in the following paragraphs.

Safety Documentation. Not only UAV risk mitigation exercises need to be documented, but also the ambition of continuous improvement and a transparent organization need a documented risk management process. Additionally a safety risk database – which shall be used as an evidence for required pre-flight checks or as a basis for UAS operation manuals – should be established. Recommendations:

1) Set up an UAS safety risk database including safety hazards and mitigation actions.

2) Establish a risk monitoring procedure.

3) Establish voluntary and mandatory reporting systems.

4) Establish a safety culture.

A risk management process example is displayed in Fig 43.20:

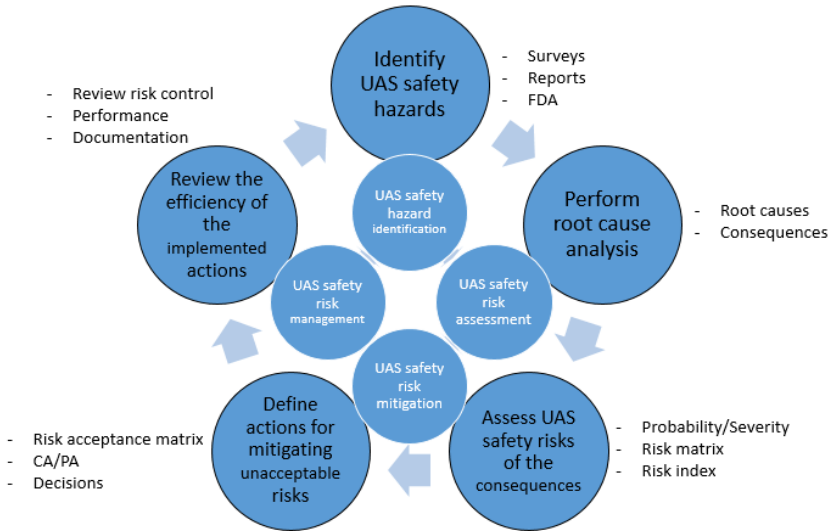


Fig. 43.20 – Risk management process example

43.4.3 Reliability of Internet of Drone based systems

Consider the IoD-based system presented in [14-17] and shown in Fig. 43.21. The constantly active wired network of the measurement and control modules and its wireless extension includes sensors and actuators from 1 to n which are connected to m traditional measurement and control modules. Each of them includes the multichannel analog to digital converter (ADC) or digital-to-analog converter (DAC), microcontroller of the traditional data processing and an adapter of the wired interface. Through this interface the measurement and control modules interact with the control and decision making center receiving commands and sending measurement results. To provide the work of those modules within the system of post-emergency monitoring each module is equipped with an additional wireless microcontroller which receives data from the wireless network, or prepares data for the transmission through wireless network. This microcontroller operates only in pre-emergency and post-emergency modes. It receives measurement results (from the measuring module microcontroller or

adapter of wired interface), then compresses, encodes and transmits it through the wireless interface. Measurement and control modules, with the absence of network power, are charged from the independent accumulator unit (it is not presented in Fig. 43.21).

In the normal exploitation mode the data and commands exchange is running through the wired network. If it is damaged during an accident, another wireless network is created on the basis of drones. Due to “Master’s” commands drones are situated in the air in a way to run following functions: to cover all measuring modules which are equipped with the wireless connection; to distribute data streams through drones as evenly as possible; to secure the highest possible trustworthiness of the transmission for sensor data and control instructions; to avoid obstacles and do not create obstacles to each other.

In the independent power supply of the measurement and control modules (from the backup accumulators only) it is very important to minimize their power consumption. For this purpose all possibilities have to be explored including a limitation of the wireless interface power. Drones must be placed in the appropriate zones close enough to the signal sources. Error level during the message exchange can be considered as one of the important criteria for the effective energy-saving. If the error level is acceptable for the selected coding method then it is enabled to try decreasing the transmitter’s power of the wireless interface both as a part of measurement modules and a part of drones.

Note that sensor data collection and actuators control (exchange in the network of measurement and control modules), and retransmitting of these data (message exchange with the center of decision making and control), and drones control (following the “Master’s” commands) are different tasks which have very little in common. Except while running the exchange task in the network of the measurement and control modules, the errors level may be defined and this information should be included when selecting the place for drone’s dislocation. That’s why to increase the reliability of the post-emergency monitoring system’s functioning it is reasonable to distribute solutions to these tasks at the hardware level. Those tasks must be performed by different microcontrollers equipped with their own peripheral devices. During

this it is expedient to form the three independent wireless networks of data exchange (measurement and control modules, retransmitted data and drones control networks) which will not conflict with each other, create queues, etc.

According to the proposed concept the three systems of post-emergency monitoring systems (S1, S2, S3) and reliability block diagrams (correspondingly: RBD1 (Fig. 43.22), RBD2 (Fig. 43.23) and RBD3 (Fig. 43.24)) have been developed.

Each system has a general way for increasing the system reliability, which includes sliding redundancy in SS, DR and DM – any failed element of the main chain ((S1- S2-...-Sk) for SS, (R1- R2-...-Rq) for DR and (M1- M2-...-Mg) for DM) can be replaced by means of any element of the redundancy chain ((Sr1- Sr2-...-Srm) for SS, (Rr1- Rr2-...-Rrp) for DR and (Mr1- Mr2-...-Mrh) for DM). Moreover, each system has a possibility to replace the failed main chain by means of the redundancy chain: (CD-DR-DM) by means of (CW-WS) for S1, (DR-DM) by means of WS for S2, (WS₁-WS₂- ...-WS_n) by means of ((DR-DM)₁-(DR-DM)₂ -...-(DR-DM)_n) for S3.

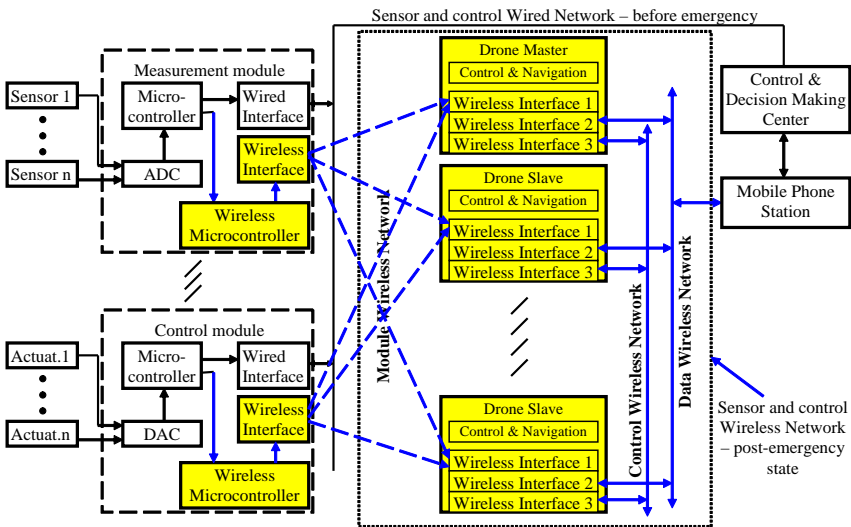


Fig. 43.21 – IoD-based system

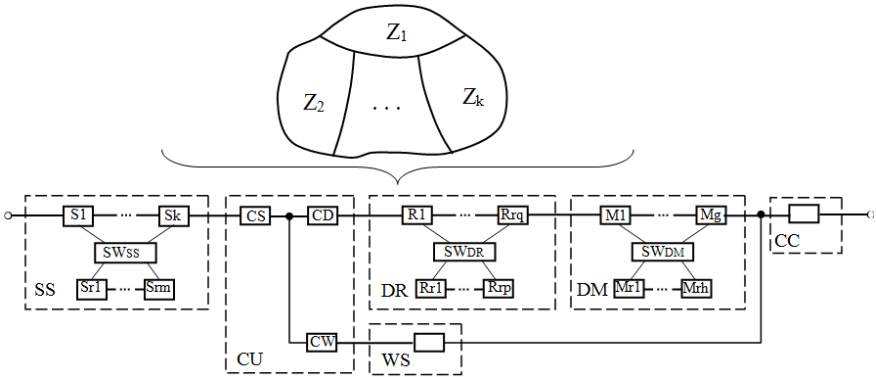


Fig. 43.22 – Reliability block diagram of the system with general sensors (S1), where Si (Srv) – sensors (redundant sensors), SS – sensor system, SW – switching units, CS – sensor controller, CD – drone system interface controller, CW – wired system interface controller, CU – controller unit, DR – drone transmission system, DM – drone monitoring system, Rj - transmission drones, Mb – monitoring drones, WS - wired system, CC – crisis centre

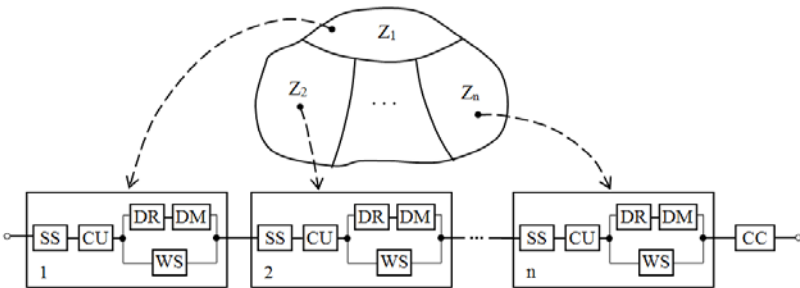


Fig. 43.23 – Reliability block diagram of the system with separated zones of sensors and drones (S2)

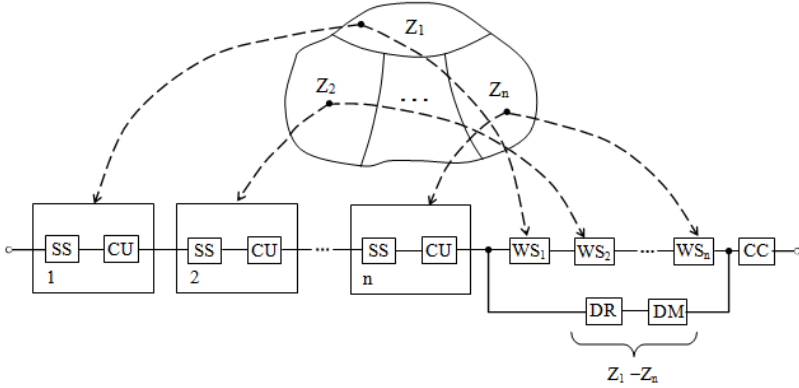


Fig. 43.24 – Reliability block diagram of the system with separated zones of sensors and general drone fleet (S3)

Based on the proposed reliability block diagrams we can obtain the following formulas for calculating the reliability function (RF) for each of these systems:

$$P_{S1}(t) = p_{SS}(t) \cdot p_{CS}(t) \cdot [1 - (1 - p_{CD}(t) \cdot p_{DR}(t) \cdot p_{DM}(t)) \times (1 - p_{CW}(t) \cdot p_{WS}(t))] \cdot p_{CC}(t) \quad (43.1)$$

where $p_{SS}(t) = e^{-k \cdot \lambda_S \cdot t} \cdot \sum_{i=0}^m \frac{k \cdot \lambda_S \cdot t}{i!}$; $p_{CS}(t) = e^{-\lambda_{CS} \cdot t}$;

$$p_{CD}(t) = e^{-\lambda_{CD} \cdot t}; p_{DR}(t) = e^{-q \cdot \lambda_R \cdot t} \cdot \sum_{j=0}^p \frac{q \cdot \lambda_R \cdot t}{j!};$$

$$p_{DM}(t) = e^{-g \cdot \lambda_M \cdot t} \cdot \sum_{l=0}^h \frac{g \cdot \lambda_M \cdot t}{l!}; p_{CW}(t) = e^{-\lambda_{CW} \cdot t};$$

$$p_{WS}(t) = e^{-\lambda_{WS} \cdot t}; p_{CC}(t) = e^{-\lambda_{CC} \cdot t}.$$

$$P_{S2}(t) = \{ p_{SS}(t) \cdot p_{CU}(t) \cdot [1 - (1 - p_{DR}(t) \cdot p_{DM}(t)) \cdot (1 - p_{WS}(t))] \}^n \cdot p_{CC}(t) \quad (43.2)$$

where $p_{CU}(t) = e^{-\lambda_{CU} \cdot t}$.

$$P_{S3}(t) = (p_{SS}(t) \cdot p_{CU}(t))^n \cdot [1 - (1 - \prod_{i=1}^n p_{WS_i}(t)) \cdot (1 - (p_{DR}(t) \cdot p_{DM}(t))^n)] \cdot p_{CC}(t) \quad (43.3)$$

43.5 Work related analysis

The advantages of using a drone fleet when comparing to a single powerful drone, a conceptual architecture for a drone swarm divided into three layers (Drone Abstraction, Fleet Abstraction, Swarm Abstraction), three types (static drone fleet, dynamic drone fleet, and hybrid drone fleet) depending upon the target environment and situation are presented in [1].

The study [2] presents different networking architectures for UAV-to-UAV (U2U) and UAV-to-infrastructure (U2I) communication that can be applied at the various layers of open system interconnection networking model. Since in-flight UAVs are highly mobile, mobile ad-hoc network (MANET) protocols are used for U2U communication where each UAV is considered as a mobile node in MANET.

Hiromoto et al. [14] describe the mobile Ad-Hoc (wireless) network for emergency scenarios in nuclear power plant. Authors proposed the system with such properties as flexibility and a self-forming and self-healing network topology that dynamically adjusts to the moving configuration per each intermediate routing node. It is also proposed to integrate MANET and Bluetooth-like technologies to create an unmanned formation of autonomous quadcopters that provides both indoor and outdoor communications coverage inside and outside of the nuclear power plant.

The main tasks of our research are:

- 1) to consider communication technologies used for unmanned aerial vehicles:
- 2) to highlight the main features for Internet of technology and the main security issues related to IoD-based applications.
- 3) to discuss phases for the aircraft system safety risk assessment .

4) to present a concept of IoD-based post-emergency monitoring system and to develop the reliability models according to the concept.

The following European MSc and PhD programs have been analysed to develop lecture material for this module:

- MSc Drone Technology and Applications (Liverpool John Moores University, United Kingdom) [18];

- PhD UAS Safety and Security System (Cranfield University, United Kingdom) [19];

- PhD Artificial Intelligence in Unmanned Aerial Vehicle Networks (Queen Mary University of London, United Kingdom) [20];

- PhD UAV-based Remote Sensing (University of Neuchâtel (UniNE), Switzerland) [21];

- PhD Unmanned Aerial Vehicles (UAVs) for Cadastral Mapping (Twente University, the Netherlands) [22].

In the USA, the universities that have the best accredited drone programs are Oklahoma State University, Embry-Riddle Aeronautical University, North Dakota University, Kansas State Polytechnic University [23], Unmanned Vehicle University (Phoenix, AZ) [24].

Oklahoma State University has a very serious program that includes every approach to drones: from engineering to design. The university has many of its own flying facilities and students have built over 200 UAVs, some of which have set world records at the time they've been made. Also, the students have an access to various laboratories and acoustic anechoic and reverberation chambers. Thus, research is possible in a wide spectrum of fields – propulsion, aeroacoustics, sensors, etc [23].

Embry-Riddle Aeronautical University offers studies at every level of education – from undergraduate to masters. If you're interested in the aspects of operating, regulations and surveillance studies of UAVs, you can just study for a Bachelor of Science degree in Unmanned Aircraft Systems Science. But if you want to be an engineer, this university is one of the rare ones (and it was the very first one!) that offers a Master of Science degree in Unmanned and Autonomous Systems Engineering [23].

At North Dakota University drone engineering and development of UAVs is in the center of attention – their students are expected to

impress with their math and engineering skills, serious opinions and the creative ability to produce great ideas. For the students that meet these requirements, there's an equally impressive reward – a Bachelor of Science degree in Aeronautics with a Major in Unmanned Aircraft Systems Operations. Their endeavors and goals are also valued by the U.S. Army, which is working closely with the university research groups [23].

Unmanned Vehicle University proposes courses which focus on unmanned systems engineering and program/project management. The curriculum includes architecture, development, modeling & simulation, analysis, integration, as well as test and management of complex systems and processes [24].

Conclusions and questions

The advantages of using a drone fleet when comparing to a single powerful drone can be categorized as follows: multiple simultaneous interventions, greater efficiency, complementarities of fleet members, reliability, technology evolution, cost.

A conceptual architecture for a drone swarm is divided into three layers: Drone Abstraction, Fleet Abstraction, and 3) Swarm Abstraction

There are three types of a drone fleet that can be potentially deployed depending upon the target environment and situation: Static DF, Dynamic DF, and 3) Hybrid DF, which combines both the static and dynamic DFs together into a single collaborative unit.

There are two types of communication for drone fleets (Internet of Drone based systems): centralized and decentralized.

The basic task of UAS is collecting data using onboard IoT devices and utilities. Data collection and reporting methods can be classified as follows: 1) Time Driven, 2) Space Driven, 3) Space-Time Driven, 4) Event Driven, 5) Query Driven, and 6) Space-Query Driven.

The following communication technologies are used for UAVs: 1) Cellular Systems, 2) WiMAX (802.16), 3) Satellite Communications, 4) Wi-Fi (IEEE 802.11), 5) Bluetooth (IEEE 802.15), and 6) Zigbee (IEEE 802.15.4).

The Internet of Drones is an architecture designed for providing coordinated access to controlled airspace for drones. The architecture,

usually, comprises two groups of components: Zone Service Providers and drones.

There are several security issues that could exist in Internet of Drone based applications, which are mostly inherited from the underlying networks and technologies (e.g., UAS, IoT). The main security issues can be imposed by the different network layers; Physical Layer, Data Link Layer, Network Layer, Transport Layer, 5) Perception Layer, 6) Transportation Layer.

The UAS safety risk assessment is an instrument used to identify and assess active and latent safety hazards for drone operation. This safety risk assessment includes actions for mitigating the predicted probability and severity of the consequences or outcomes of each operational risk.

A concept of IoD-based post-emergency monitoring system was presented, and the reliability models according to the concept were developed for the following IoD-based systems: the system with general sensors, the system with separated zones of sensors and drones, the system with separated zones of sensors and general drone fleet.

In order to better understand and assimilate the educational material that is presented in this section, we invite you to answer the following questions:

1. Name the advantages of using a drone fleet when comparing to a single powerful drone.
2. What is a multi-level drone fleet and what missions can it be used for?
3. What is a standalone drone swarm and what missions can this swarm be used for?
4. What does Layer “Drone Abstraction” focus on?
5. What operation does Layer “Drone Abstraction” comprise?
6. What does Layer “Fleet Abstraction” focus on?
7. What operation does Layer “Fleet Abstraction” comprise?
8. What does Layer “Swarm Abstraction” focus on?
9. What operation does Layer “Swarm Abstraction” comprise?
10. What is a dynamic drone fleet and what missions can it be used for?
11. What is a hybrid drone fleet and what missions can it be used for?

12. What is a centralized communication?
13. What is a UAV Ad-Hoc Network?
14. What is a Multigroup UAV Network?
15. What is a Multilayer UAV Ad-Hoc Network?
16. What is mesh networking?
17. Name the advantages of mesh networking?
18. What is the Delay Tolerant Network?
19. What is FANET?
20. What major categories are the FANET protocols classified into?
21. What is a Wide FANET?
22. What sensors are used in drones for data collecting?
23. What communication technologies are used for UAVs?
24. That is an Internet of Drones?
25. That layers does Internet of Drones consist of?
26. Explain how an Internet of Drones can be used for surveillance tasks in smart farms.
27. Explain how an Internet of Drones can be used in smart cities.
28. Explain how an Internet of Drones can be used in big events.
29. What phases does the UAS safety risk assessment comprise?
30. What is Safety Hazard Identification?
31. What is Safety Risk Assessment?
32. What is Safety Risk Mitigation?
33. What is Safety Documentation?
34. Give examples of reliability models for an Internet of Drones?

References

1. R. Akram, K. Markantonakis, K. Mayes, O. Habachi, and D. Sauveron, "Security, privacy and safety evaluation of dynamic and static fleets of drones," in *Proc. 36th IEEE/AIAA Digital Avionics Syst. Conf. (DASC)*, St. Petersburg, FL, USA, 2017.
2. N. Motlagh, T. Taleb, and O. Arouk, "Low-Altitude Unmanned Aerial Vehicles-Based Internet of Things Services: Comprehensive Survey and Future Perspectives," *IEEE Internet of Things J.*, vol. 3, no. 6, pp. 899–992, Dec. 2016.
3. J. Li, Y. Zhou, and L. Lamont, "Communication architectures and protocols for networking unmanned aerial vehicles," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Atlanta, GA, USA, 2013, pp. 1415–1420.

4. E. W. Frew and T. X. Brown, "Airborne communication networks for small unmanned aircraft systems," *Proc. IEEE*, vol. 96, no. 12, pp. 2008–2027, Dec. 2008.
5. J. Kwon and S. Hailes, "Scheduling UAVs to bridge communications in delay-tolerant networks using real-time scheduling analysis techniques," in *Proc. IEEE/SICE Int. Symp. Syst. Integr. (SII)*, Tokyo, Japan, 2014, pp. 363–369.
6. D. Pigatto, M. Rodrigues, J. V. Fontes, A. Pinto, J. Smith, and K. Branco, "The internet of flying things," in *Internet of Things A to Z: Technologies and Applications*, Q. F. Hassan, Ed., 1st ed. Wiley-IEEE Press, 2018, pp. 529–561.
7. Bekmezci, O. K. Sahingoz, and S. Temel, "Flying ad-hoc networks (FANETs): A survey," *Ad Hoc Networks*, vol. 11, no. 3, pp. 1254–1270, Jan. 2013.
8. M. A. Khan, A. Safi, I. M. Qureshi, and I. U. Khan, "Flying ad-hoc networks (FANETs): A review of communication architectures, and routing protocols," in *Proc 1st Int. Conf. Latest Trends in Electrical Engineering and Computing Technologies (INTELLECT)*, At Karachi, Pakistan, 2017.
9. M. B. Yassein and N. A. Damer, "Flying ad-hoc networks: Routing protocols, mobility models, issues," *Int. J. Advanced Comp. Science and Appl.*, vol. 7, no. 6, pp. 162–168, 2016.
10. O. K. Sahingoz, "Routing protocols in flying Ad-hoc networks (FANETs): Concepts and challenges," *Journal of Intelligent & Robotic Systems*, pp. 513–527, Apr. 2014.
11. A. Mukherjee, V. Keshary, K. Pandya, N. Dey, and S.C. Satapathy, "Flying Ad hoc Networks: A Comprehensive Survey,". In: *Information and Decision Sciences. Advances in Intelligent Systems and Computing*, S. Satapathy, J. Tavares, V. Bhateja, J. Mohanty, Eds., vol. 701. Springer, Singapore, 2018, pp. 569–580.
12. A. Guillen-Perez and M.-D. Cano. (2018, Sept.). Flying ad hoc networks: A new domain for network communications. *Sensors*. 18(10). Available: <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6209929/>.
13. Q. Jing, A. V. Vasilakos, J. Wan, J. Lu, and D. Qiu, "Security of the Internet of Things: perspectives and challenges," *Wireless Networks*, vol. 20, no. 8, pp. 2481–2501, Jun. 2014.
14. R. Hiromoto, A. Sachenko, V. Kochan, V. Koval, V. Turchenko, O. Roshchupkin, and K. Kovalok, "Mobile Ad Hoc wireless network for pre- and post-emergency situations in nuclear power plant," in *Proc. 2nd IEEE Int. Symp. on Wireless Systems within the Conf. on Intelligent Data Acquisition and Advanced Computing Systems*, Offenburg, Germany, IDAACS-SWS 2014, pp. 92–96.

15. V. Kharchenko, “Diversity for safety and security of embedded and cyber physical systems: fundamentals review and industrial cases,” in *Proc. 15th Biennial Baltic Electronics Conf.*, Tallinn, Estonia, BEC 2016, pp. 17–26.

16. V. Kharchenko, A. Sachenko, V. Kochan, and H. Fesenko, “Reliability and survivability models of integrated drone based systems for post emergency monitoring of NPPs,” in *Proc. Int. Conf. on Inform. and Digital Technologies 2016*, Rzeszow, Poland, IDT 2016, pp. 127–132.

17. V. Kharchenko, H. Fesenko, A. Sachenko, R. Hiromoto, and V. Kochan, “Reliability issues for a multi-version post-severe NPP accident monitoring system,” in *Proc. 9th IEEE Int. Conf. Intell. Data Acquisition and Advanced Computing Syst.: Technology and Applicat.*, IDAACS 2017, vol. 2, pp. 942–946.

18. MSc Drone Technology and Applications. (2019, May). Available: <https://www.ljmu.ac.uk/study/courses/postgraduates/drone-technology-and-applications>.

19. PhD Studentship in UAS Safety and Security System. (2019, May). Available: <https://www.adventuseducation.lk/university/cranfield-university/phd-studentship-in-uas-safety-and-security-system/>.

20. Artificial Intelligence in Unmanned Aerial Vehicle Networks. (2019, May). Available: <https://www.findaphd.com/phds/project/artificial-intelligence-in-unmanned-aerial-vehicle-networks/?p104547>.

21. University of Neuchâtel (UniNE) Switzerland – PhD Position in UAV-based remote sensing. (2019, May). Available: <https://www.suasnews.com/2018/04/university-neuchatel-unine-switzerland-phd-position-uav-based-remote-sensing/>.

22. PhD Candidate (Promovendus) Unmanned aerial vehicles (UAVs) for cadastral mapping, ITC, Twente University. (2019, May). Available: <http://www.sense.nl/search/item/10865702/PhD-Candidate-Promovendus-Unmanned-aerial-vehicles-UAVs-for-cadastral-mapping-ITC-Twente-University>.

23. Drone Programs at Universities and Colleges. (2019, May). Available: <https://www.dronesinspector.com/drone-programs-at-universities-and-colleges/>.

24. Drone Programs at Universities and Colleges. (2019, May). Available: <https://www.uvxuniversity.com/uav-education/>.

PART XII. IOT FOR HEALTHCARE SYSTEMS

44. INFRASTRUCTURE OF THE IOT FOR HEALTHCARE SYSTEMS

Prof., DrS V. S. Kharchenko, Assoc. Prof., Dr. D.D. Uzun,
PhD student A.A. Strielkina, Dr. O. O. Illiashenko (KhAI)

Contents

Abbreviations	485
44.1. Standards requirements to IoT for healthcare systems	486
44.2 Techniques of IoT for healthcare systems realization	489
44.2.1 Existed techniques	490
44.2.2 Prospective techniques	491
44.3 Developing and modeling infrastructure of the IoT for healthcare systems	495
44.3.1 Development of infrastructure of the IoT for healthcare systems	495
44.3.2 Modeling of infrastructure of the IoT for healthcare systems	498
44.3.3 Cases.....	500
44.4 Work related analysis	504
Conclusions and questions.....	505
References	506

Abbreviations

AI – Artificial Intelligence
AMQP – Advanced Message Queuing Protocol
BAN – Body Area Network
CDMA – Code Division Multiple Access
CoAP – Constrained Application Protocol
ECG – Electrocardiogram
FDA – Food and Drug Administration
FMEA – Failure Mode and Effects Analysis
HIPAA – Health Insurance Portability and Accountability Act
HL7 – Health Level Seven
ICT – Information and Communications Technology
IoHT – Internet of Healthcare Things
IoMT – Internet of Medical Things
JMS – Java Message Service
MHRA – Medicines and Healthcare Products Regulatory Agency
MQTT – Message Queuing Telemetry Transport
OSI – Open System Interconnection
QoS – Quality of Service
RA – Reference Architecture
REST – Representational State Transfer
RFID – Radio Frequency Identification
SoC – System-on-a-Chip
SSL – Secure Sockets Layer
TCP – Transmission Control Protocol
TLS – Transport Layer Security
XMPP – eXtensible Messaging and Presence Protocol

44.1. Standards requirements to IoT for healthcare systems

The Internet of Things (IoT) is the network concept, combining physical devices from a variety of industries in a single network with the possibility of telemetry and perform various functions.

The development IoT in healthcare technology will bring the new direction - Internet of Medical Things (IoMT) or Internet of Healthcare Things (IoHT). This fast distribute collection of the networked devices, including wearables, implants, skin sensors, home monitoring tools, and mHealth applications has the potential to connect patients and their providers, harnessing the power of AI with innovative techniques.

Up-to-date advances in healthcare providing, microelectronics and sensor manufacturing, and data processing and storage have made it possible to change the approach for developing complexes for healthcare to a new level [1]. the sensors have become much more affordable, smaller in size and more accurate in measurements, their maintenance does not require personnel, and a beginner electronics developer can understand their work. Such devices allow monitoring the state of human health without a patient stay in the hospital [2]. Taking into account the portable medical devices market as a whole, according to the ABI Research company, in 2016 the delivery of wearable devices used to monitor and monitor patients both remotely and directly in hospitals reached about 8 million pieces in the global scale and by 2021 the volume of shipments of such equipment will increase to 33 million units. Experts expect that in 2021 the release of devices for remote medical monitoring will grow by 35% and amount to 60% of the total number of products used to monitor patients [3].

There are three categories of IoT healthcare approaches: person-to-person (e.g., one person receives information about health condition of another person), person-to-computer (e.g., device helps to manage a patient's health), person-as-a-computer (e.g., with a human body motions or heat exchange processes etc. communicate to digital technologies). This section deals with the person-to-computer approach.

Medical devices are equipment projected generally for a medical use. Such devices are different from other consumer goods or products. It is clear that they are an integral part of healthcare system. The regulation and standardization of such systems must meet worldwide, national and

regional plans, laws and practices. Unfortunately, regulatory requirements to such kind of devices vary all round the world. The most developed regulation process has the US. The Food and Drug Administration's (FDA) regulatory guidances cover almost all processes involved in medical devices intended for human use. The FDA registers and lists such devices and verifies compliance with Premarket Submission requirements, conducts field examinations and analyzes samples to ensure they fulfil with appropriate standards and/or label requirements. The requirements to medical devices of many countries are based on the FDA's. In the European Union there is a slate of regulations. It includes Medical Devices Directive (93/42/EEC) and Active Implantable Medical Device Directive (90/385/EEC) and comes into force on May 2020. Considering the United Kingdom regulations, their Medicines and Healthcare Products Regulatory Agency (MHRA) ensures that medicines and medical devices work and are acceptably safe. The MHRA also too assess and authorize medical devise to be sold and supplied in the UK, regulates clinical trials of medical devices, monitors and ensure compliance with statutory obligations relating to medical devices, and promotes safe use of such kind of devices.

If we consider the whole healthcare infrastructure it is needed to analyze regulatory documents separately on healthcare, IoT and cybersecurity (because any information about health status, provision of healthcare, or payment for healthcare should be private and protected; it will be considered in the Section 45). Correlation of these components is presented in Fig. 44.1.

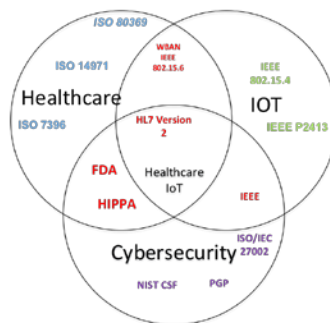


Fig. 44.1 – The simplified correlation of regulatory documents in the healthcare system

There are a number of international standards for the medical devices certification. IEC 62304:2006 [4] establishes the medical device software lifecycle requirements. This standard is currently under revision and harmonization with ISO 82304 [5] that concerns to the safety and security of health software products designed to function on general IT platforms and proposed to be placed on the market exclusive of dedicated hardware.

IEC 62366 is the process-based standard that specifies usability requirements for the development of medical equipment. This standard harmonized in the EU and the USA.

ISO 14971 is aimed to risk management of medical devices. This standard determines the requirements for risk management to regulate the safety of the medical device by the manufacturer during the product life cycle. ISO 14971 includes such features as inherent safety by design (e.g., automate device functions, use specific connectors etc.), protective measures in the medical device itself or in the manufacturing process (e.g., warning screens, alerts for hazardous conditions, physical safety guards, shielded elements, etc.) and information for safety (e.g., warning or caution statements in the user manual, trainings etc.). This standard serves in the interconnection with other standard for more advanced level regulation and comprehensive quality management system – ISO 13485. Compliance with ISO 13485 is frequently seen as the first step in reaching compliance with European regulatory requirements.

ISO 10993 series set requirements to biocompatibility evaluation of medical devices. It works in connection with FDA regulatory documents.

The IEC 60601 series is a set of technical standards for the safety and essential performance of medical electrical equipment. The requirements of this standard differ depending on the region of the globe. One of the main components is the risk management procedure (in the form of FMEA), which should be included as part of the document submitted to the certification authority, which will take responsibility for the medical product certification.

There is an enormous number of emerging IoT standards. The latest Gartner Hype Cycle for IoT Standards and Protocols profiles 30 standards. Considering IoT driven devices and applications the

standards set includes standards for information technologies (e.g., ISO and IEEE, etc.).

IEEE standards for LANs specifies Wi-Fi (IEEE 802.11) and ZigBee (802.15.4). Standards for PANs contain Bluetooth and BLE, as well as IEEE 802.15.4j and IEEE 802.15.6, which are the IEEE standards associated with the body area network (BAN). IEEE 802.15.4 is a standard which identifies the physical layer and media access control for low-rate wireless personal area networks. IEEE 21451-7 establishes smart transducer interface for sensors and actuators-transducers to RFID systems communication protocols and transducer electronic data sheet formats. For cellular networks GSM/UMTS and CDMA standards are used.

ISO/IEC 30141 offers an internationally standardized IoT Reference Architecture (RA), which the organization said will help ensure that connected systems are "seamless, safer and far more resilient." It describes the options, characteristics and aspects of IoT systems, IoT domains, and interoperability of IoT entities. In addition ISO/IEC 30141 provides a technology-neutral reference point for stating standards for IoT and encourages openness and transparency in the benefits and risks identification. This RA includes defining of:

- Characteristics of IoT systems;
- Characteristics, principles and requirements of the IoT RA;
- IoT RA framework;
- Conceptual reference model;
- IoT References Architectures.

ISO/TC 215 (technical committee on health informatics) provides data exchange standards HL7 (Health Level Seven). These standards focus on the application layer in the OSI model. HL7 identifies a number of flexible standards, guidelines and methodologies by which various healthcare systems can communicate with each other.

44.2 Techniques of IoT for healthcare systems realization

At the moment, according to the statistics, deaths due to the cardiovascular diseases are very widespread. For this reason, the electrocardiograph was chosen as a one of main parts of the overall healthcare monitoring system. According to the World Health

Organization, the most common causes of death in 2015 are ischemic heart disease and stroke [6]. To reduce the risk of catastrophic consequences from such diseases, taking into account the development of technologies, two options for prophylaxis are suggested: medical examination in inpatient departments of hospitals with a healthcare authority supervision (standard situation), and disease prevention using modern medical equipment, which can have compact dimensions and the possibility of autonomous use.

Taking into account the analysis of the modern publications [7]-[8] it is possible to present the general architecture of the system (see Fig. 44.2).

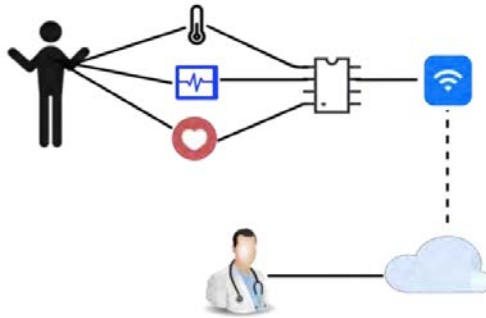


Fig. 44.2 – The general architecture of the healthcare IoT system

The onboard sensors on the patient's body are connected to the main microcontroller, which processes the data and sends them to the cloud storage using a wireless network. Then the healthcare authority (decision-maker), access to data and recommendations, which are formed by a cloud service.

44.2.1 Existed techniques

Nowadays there are prototypes and designs of wearable healthcare devices for recording and processing of electrical activity of the heart. They use various options for both hardware and software solutions. The papers [9]-[10] contain the description of the creation of devices of such kind using costly equipment or equipment, inferior to the technical specifications of the case proposed below.

At the moment, there are several solutions for remote monitoring of a person's condition. One of them is MySignals - development platform for medical devices and eHealth applications [10]. This product includes hardware and software solutions. The advantages of this solution are flexibility (the ability to connect up to 15 different sensors), project implementation and access to the market, the availability of its own API and cloud services. The main disadvantages are pricing (project annual tariff plans costing about EUR 200 for a software solution, as well as high hardware costs - EUR 1,900 per set), lack of information on security and device certification.

Another example is the project, which is called "ECG dongle". This solution consists of a cardiograph device in the form of a USB-dongle, application for Android devices and cloud storage. The advantages of this solution are the compactness of the device, its low cost (about USD 60 per device). The disadvantages are dependence on the external device, incompleteness of the research - it is not possible to determine the preliminary diagnosis (should consult a doctor) and a high probability of a technical error [11].

In paper [12] the outdated and expensive equipment were used. Also in this project is using paid software MatLab, which is difficult to use beginners or organization without a lot of funding.

The expensive software but without advanced wireless technology is used in [13]. Cloud technologies are not used and the system is designed for the one device only.

After analyzing advantages and disadvantages of the devices described above, it can be concluded that these projects are incomplete in terms of the incompleteness of the project infrastructure, not paying attention to security and privacy issues, excessive simplicity or high cost of the device in case of the full functionality. This paper describes the solution, which take into account all abovementioned factors.

44.2.2 Prospective techniques

Modern data transmission protocols for IoT have their own advantages and disadvantages. Among the shortcomings the redundant data, unreliability, poor security can be identified.

According to Open System Interconnection (OSI) protocols layers, many application-level protocols are used to transfer data to IoT, the most common of which are: MQTT, XMPP, AMQP, JMS, CoAP, REST/HTTP [14].

Such protocols like MQTT, XMPP, AMQP, JMS are based on a broker: publish/subscribe. The broker (server) can be deployed on a cloud platform or on a local server. Client programs should be installed as an application on smart devices. The CoAP (Constrained Application Protocol) protocol is a limited data transfer protocol similar to HTTP but adapted to work with "smart" lowperformance devices. Also, REST / HTTP consists of two technologies - REST and HTTP, so REST is a style of software architecture for distributed systems, which describes the principles for the interaction of smart device applications with the REST API (Web service) programming interfaces [15].

At the moment, the Message Queuing Telemetry Transport (MQTT) protocol is very popular due to such advantages [16]:

- Asynchronous protocol;
- Compact messages;
- Work in unstable communication on the data line;
- Support for multiple levels of Quality of Service (QoS);
- Easy integration of new devices.

The MQTT protocol runs on the application layer over TCP/IP. MQTT messages are exchanged between a client (client), which can be a publisher or subscriber (publisher/subscriber) of messages, and a broker of messages (for example, Mosquitto MQTT). The publisher sends data to the MQTT broker, specifying a topic in the message, topic. Subscribers can receive different data from a variety of publishers, depending on the subscription to the relevant topics.

The reliability issue for data transmission to the MQTT is solved due to the availability of Quality of Service levels. MQTT supports three levels of QoS in the transmission of messages. Through the use of the second and third level, it is possible to receive confirmation from the recipient.

To ensure security in the MQTT protocol, a security method is implemented, such as connecting to a broker through TLS / SSL. In the context of IoT technologies, security can be implemented by using hardware crypto protection modules.

The modern market provides solutions for monitoring the patient's conditions. The device was assembled from the following components:

1) Cardiograph based on AD8232 module [17] is set to monitor the heart rate by forming heart bioelectric signals. This kit includes a printed circuit board with an AD8232 microcircuit installed on it, a 3.5 mm connector for connecting the cable to the electrodes, indication LEDs, an analog output for connection (for example to Arduino). The microcircuit is 50% smaller and uses 20 percent less energy than similar devices, which allows it to be used in a wide range of products for health monitoring, both in personal observation and in remote medical control.

2) Gyro-accelerometer MPU-6050-MOD is a module that combines sensors: a 3-axis gyroscope and a threeaxis accelerometer. In the case of a medical device, this module can be used to determine the position of the patient's body during measurements; the position of the body significantly affects the result of certain measurements. Communication with the head unit is due to a two-pin interface I2C.

3) Cryptochip Atmel ATECC508A - allows providing security between the device with sensors and a cloud. It is actually a co-processor that allows you to generate persistent encryption keys using cryptographic algorithms on elliptical curves. The key length is 256-bit, the chip guarantees a unique 72-bit serial number, and for storing keys, certificates and data, the built-in 10Kb EEPROM memory is available (up to 16 keys can be stored in the built-in memory) and a device that collects information.

There are various solutions for connecting the modules described above, including the popular board Raspberry Pi, ESP and very popular Arduino platform, which was excluded from the comparison due to lack of built-in wireless communication modules. The results of the comparison of several existed hardware solutions for implementation of the main controller selection is presented in Table 44.1.

Table 44.1 – Comparison of controllers

Criteria	Device		
Manufacturer	ESP8266	ESP32	Raspberry Pi Zero W
	Espressif	Espressif	Raspberry Pi Foundation
Type	Microcontroller	Microcontroller	Single board computer
Microcontroller (CPU)	Xtensa singlecore 32-bit L106	Xtensa dualcore 32-bit LX6 600	ARMv6Z ARM1176JZF-S
Frequency	80 MHz	160 MHz	1 GHz
RAM	160 Kb SRAM	512 Kb SRAM	512 Mb SDRAM
GPIO	17	36	40
Software PWM	8-channel	16- channel	6- channel
SPI	2	4	2
ADC	10-bit	12- bit	None
Wi-Fi	802.11	b/g/n	802.11 n
Bluetooth	None	4.2 Classic and BLE	4.1 Classic and BLE
Power usage	Up to 215 mA in transmit mode, 100 mA in receive mode, 70 mA in standby mode	160-260mA. Without WiFi and Bluetooth enabled - 20mA	100 mA (0.5 W) on average (standby), 350 mA (1.75 W) maximum
Power	2,2 - 3,6 V	2,2 - 3,6 V	5 V
Price	\$2.20	\$3.50	\$10.00

In connection with the development of cloud technologies, new products are actively appearing on the market. Among them there are three leaders in the cloud technology market for IoT: Azure IoT Core from Microsoft, Cloud IoT Core from Google and Amazon Web Services IoT. The comparison of above-mentioned cloud services is presented in Table 44.2.

Table 44.2 – Comparison of the Cloud service solutions

Criteria	Platform		
	Azure IoT Core	Cloud IoT Core	AWS IoT
Type	IaaS, PaaS		
Communication protocols	HTTP, MQTT, AMQP	HTTP, MQTT	
Security	None	None	TLS
Data visualization	Yes		
Free tariffs	Yes		No
Price	Free - up to 8,000 messages per day. \$50 - \$50,000 per month (depending on the number of messages)	Free - up to 250MB of traffic per month. Further prices range from \$0.0045 to \$0.00045 per Mb (depending on traffic)	\$0.7 - \$1 for a million messages (depending on the total number of messages)
Trial period	1 month	No	12 months

44.3 Developing and modeling infrastructure of the IoT for healthcare systems

There is a need to analyze the existing hardware and software components for the construction of the healthcare solutions using IoT platform and cloud service and provide the rationality for their choice. with attention to security and privacy issues. The designed prototype with its implemented functionality can compete with professional instruments for measurement of the ECG, albeit at a much cheaper price. Moreover, it is needed to model a healthcare IoT infrastructure using the queuing theory.

44.3.1 Development of infrastructure of the IoT for healthcare systems

Taking into account the goal of the cost-effective solution development and based on the comparison results, the Amazon Web

Services IoT has been selected to build the project, as this service has proved as the safest solution. Another benefit of AWS is its compliance with the US Data Transmission and Protection Act (HIPAA), which allows the use of a secure AWS environment for the processing, maintenance and storage of private healthcare and medical data.

Based on the analysis, the ESP32 system was chosen for hardware development, since it contains wireless WiFi and Bluetooth modules, and there is a 12-bit analog-to-digital converter. For the convenience of prototyping and debugging, ESP-WROOM32 was chosen with a convenient design for debugging and quick start using a micro-USB cable and a computer (without programmers and prototyping boards). The assembled prototype of the device is shown in Fig. 44.3.

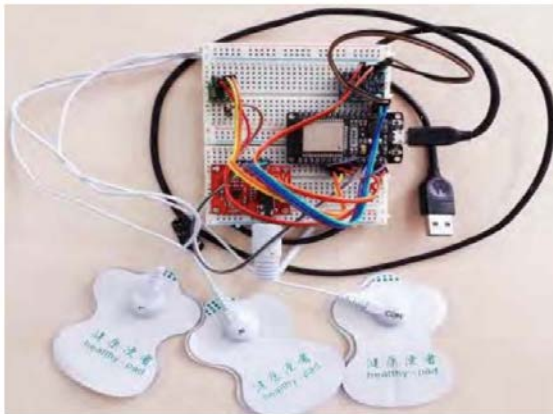


Fig. 44.3 – The assembled device prototype

The following requirements were considered for choosing software platform:

- Support of all modules described earlier;
- Support of popular programming language;
- Support of Cloud services;
- Easy-to-flash and debugging support;
- Availability.

Mongoose OS is an open source operating system for IoT microcontrollers and Systems on Chip (SoC) was chosen for meeting these requirements. Additional features of this OS are development and

debugging directly in the browser window, supporting of two programming languages - JavaScript and C, supporting on-the-air update and integration with Cloud services.

The developed prototype has tended to be an effective and functional healthcare device that allows to monitor the state of the electrical activity of the human heart, collect data and send them to the Cloud storage using a protected TLS connection and MQTT protocol with 1 level of Quality of Service. The measurement results are transferred to the cloud in JSON format - a lightweight text-based data exchange format.

At the current stage of development, using AWS IoT, it is possible to see a simple analysis of the data being processed and provide brief statistics on the number of device connections to the Cloud broker and the time when these connections took place, as well as the number of incoming and outgoing messages using the MQTT protocol.

Figure 44.4 contains the graphic representation of the ECG. This chart shows the processed ECG shot using 3-channel Cardiosensor. This graph is a representation of the patient's ECG measurement for 15 seconds (the optimum time for a diagnostic measurement) using the prototype developed. Filtering of noise and interference in the measurements occur automatically with the hardware module AD8232. The abscissa represents the maximum value of the oscillation amplitude of the ADC within the measurement scale that is determined by the possible values of 212 (4096). The axis of ordinate represents the number of discrete values of time within which the fixation cardiac electrical activity values.

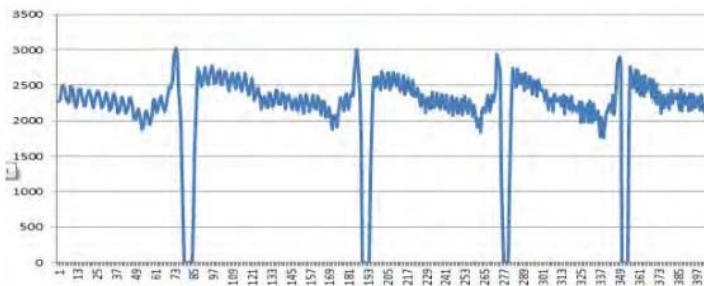


Fig. 44.4 – Graphical representation of the ECG

As soon as one of the most critical factors of the mobile devices is power consumption, for the autonomy of the designed device, it is possible to use a lithium battery with a capacity of about 2500 mAh.

44.3.2 Modeling of infrastructure of the IoT for healthcare systems

For this case, the queueing systems are those systems at which random service requests from IoT device (customer) are received at random times, while incoming requests are serviced by means of the available service channels [18, 19]. Under the flow of service is understood the flow of requests, serviced one after another by one continuously occupied channel (for example, Cloud). Fig. 44.5 shows the queueing theory model for the considered case of the healthcare IoT system.

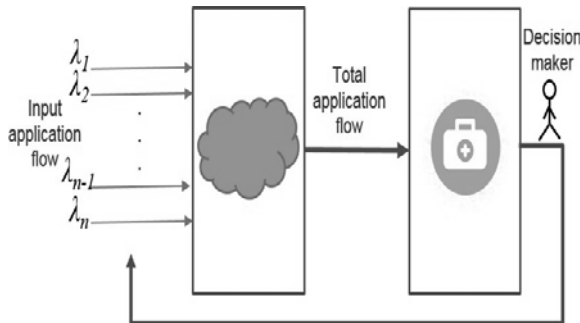


Fig. 44.5 – The queueing system for the healthcare IoT system

When considering a single serviced device, the proceeding processes can be represented by a Markov stochastic process (chain) with discrete states and discrete time. However, when considering the IoT infrastructure (due to the huge number of devices and the difference in their characteristics), it should be noted that in this case, all flows are simplest, and the process occurring in the IoT system is a Markov stochastic process (chain) with discrete states and continuous time. The assumptions of the Markov stochastic process (chain) using are that the intensity of failures λ and repairs μ is assumed to be constant, events are independent of each other, and the probability of occurrence of two or more events during a short time interval is much

less than the probability of occurrence of one event during the same time period. Visibly, there is a stationary state in this process. It is not necessary to formulate the Kolmogorov equation since the structure is regular.

There is a hypothetical situation. The hospital, which is part of the IoT infrastructure, receives three service requests from users of the networked electrocardiograph (for example, results of ECG planned measurement, request an appointment, and statistics). The flow of all requests is the simplest. The average time of receiving a new request from an electrocardiograph user is 30 min (determined by subjective characteristics), t . When the request is received, the healthcare staff begins to process it. The processing time for one request is distributed according to the exponential law and on average is 10 min, t_{pr} . At the initial time, there are no requests in the system. It is required to determine the reliability characteristics of this system.

In this way, there are four possible states in this system:

- S_0 – There are no service requests in the system.
- S_1 – There is one service request in the system.
- S_2 – There are two service requests in the system.
- S_3 – There are three service requests in the system.

We will assume that the processes of receipt and processing of requests are homogeneous Markov; simultaneous receipt of several service requests and simultaneous processing are practically impossible. Since all applications are equivalent, from the point of view of the reliability, it does not matter which service request is in the state S_3 , it is important that only one.

With this in mind, the situation is modeled by the "birth–death" process (Fig. 44.6).

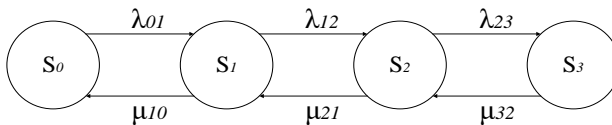


Fig. 44.6 – A scheme of “birth–death” process for the considered case

According to Fig. 44.6, λ_{01} , λ_{12} , and λ_{23} are the intensities of service requests flow, and μ_{10} , μ_{21} , and μ_{32} are the intensities of processing flow.

The intensity of receipt of one service request is equal to $\lambda = 1/t$, and the intensity of processing of one request is equal to $\mu_{10} = 1/t_{pr}$.

There are no requests in the state S_0 ; consequently $\lambda_{01}=3 \lambda$; in the state S_1 , one request was received – $\lambda_{12}=2 \lambda$, and in the state S_2 , two requests were received – $\lambda_{23}=\lambda$. In the state S_3 , two requests are processing, so $\mu_{10}=3 \mu$, for the state $S_2 \mu_{21}=2 \mu$, and for $S_1 \mu_{32} = \mu$.

According to [20], the probability of a state when there are no requests in the system:

$$P_0 = \frac{1}{1 + \frac{\lambda_{01}}{\mu_{10}} + \frac{\lambda_{01}\lambda_{12}}{\mu_{10}\mu_{21}} + \frac{\lambda_{01}\lambda_{12}\lambda_{23}}{\mu_{10}\mu_{21}\mu_{32}}} \approx 0.4219.$$

Similarly, the remaining probabilities are calculated, which are equal to $P_1=0.4219$, $P_2=0.14$, and $P_3=0.016$.

44.3.3 Cases

The model considering attacks on vulnerabilities. In case of a successful cyberattack on a single vulnerability in the healthcare IoT system, the developed “birth–death” model is modified as follows, as shown in Fig. 44.7.

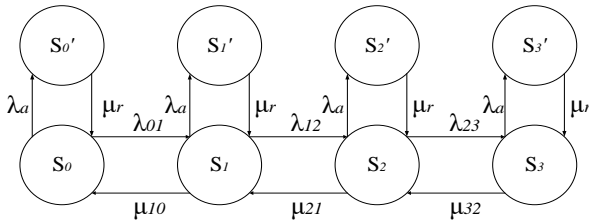


Fig. 44.7 – A Markov model for the considered case of a successful attack at one stage of the service request processing (with a halt) case

Let us suppose that the successful attack on the healthcare IoT system occurs with a probability of 20% (every fifth attack is successful), and $\mu_r = 0.9$. Let us suppose that at the initial instant of time with a probability 100% is in state S_0 .

If the healthcare IoT system continues to perform its functions without halts during the attacks, in this case, an appropriate Markov model is shown in Fig. 44.8.

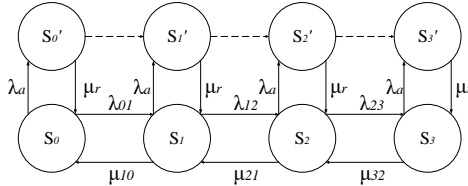


Fig. 44.8 – A Markov model for the considered case of a successful attack at one stage of the service request processing (without halts)

The model considering elimination of vulnerabilities. In the cases discussed above, the vulnerabilities are not eliminated, and the system just restarts and continues to function in the same way. Fig. 44.9 illustrates a case that when the healthcare IoT system has one vulnerability is eliminated (with $\mu_r' = K_\mu \mu_r$, $K_\mu < 1$, $t_r' > t_r$).

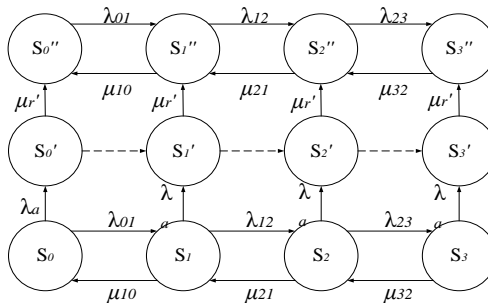


Fig. 44.9 – A Markov model for the considered case of a successful attack at one stage of the service request processing (with halts and eliminating of one vulnerability)

In the previous cases, a system with one vulnerability was considered. Further models with two vulnerabilities are proposed (Fig. 44.10 and 44.11). In the first case (Fig. 44.10), as in the cases depicted in Fig. 44.7 and 44.8, the second vulnerability is not eliminated and the

system just restarts and continues to function in the same way (with $\lambda_a' = K_\lambda \cdot \lambda_a, K_\mu < 1$).

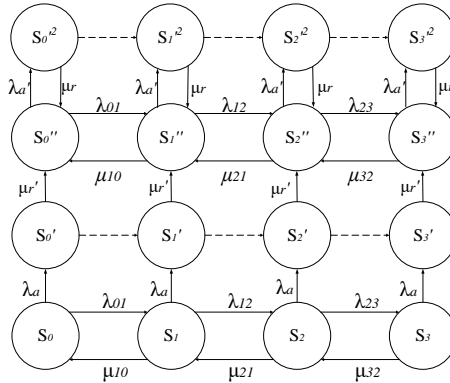


Fig. 44.10 – A Markov model for the considered case of a successful attack at one stage of the service request processing (with halts and system has two vulnerabilities and one vulnerability is eliminated)

In the second case (Fig. 44.11) as in the case depicted in Fig. 44.9, the second vulnerability is eliminated.

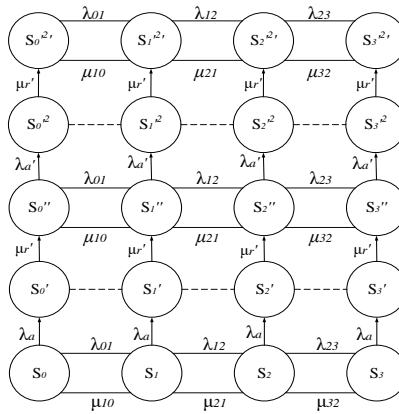


Fig. 44.11 – A Markov model for the considered case of a successful attack at one stage of the service request processing (with halts and with halts and system has two vulnerabilities and two vulnerabilities are eliminated)

For the cases depicted in Fig. 44.7 and 44.8, the availability functions are calculated as:

$$F_a(t) = P_{s_0}(t) + P_{s_1}(t) + P_{s_2}(t) + P_{s_3}(t) \quad (44.1)$$

and for Fig. 44.9 and 44.10 as:

$$F_a(t) = P_{s_0}(t) + P_{s_1}(t) + P_{s_2}(t) + P_{s_3}(t) + P_{s_0}''(t) + P_{s_1}''(t) + P_{s_2}''(t) + P_{s_3}''(t) \quad (44.2)$$

and for Fig. 44.11 as:

$$F_a(t) = P_{s_0}(t) + P_{s_1}(t) + P_{s_2}(t) + P_{s_3}(t) + P_{s_0}''(t) + P_{s_1}''(t) + P_{s_2}''(t) + P_{s_3}''(t) + P_{s_0}^{i_2}(t) + P_{s_1}^{i_2}(t) + P_{s_2}^{i_2}(t) + P_{s_3}^{i_2}(t) + P_{s_0}^{i_2}(t) + P_{s_1}^{i_2}(t) + P_{s_2}^{i_2}(t) + P_{s_3}^{i_2}(t) \quad (44.3)$$

The analysis of the obtained results shows that when one vulnerability and for other case two vulnerabilities are eliminated, the healthcare IoT system has a higher probability to be operational than just restarting; however, the t_r' value affects the duration of the availability function transition period to a stationary mode. Fig. 44.12 shows the combined plot of availability functions for all considered cases discussed above.

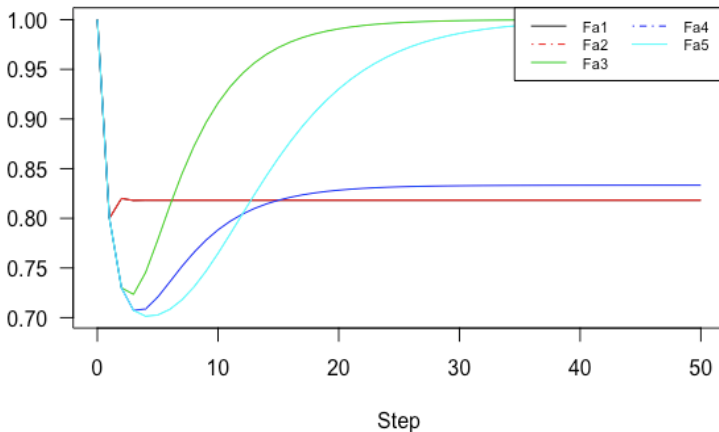


Fig. 44.12 – Availability functions plot for all considered cases

For the cases depicted as Fa3, Fa4, and Fa5, the availability functions fall below due to the loss of availability for removing vulnerabilities ($t_r' > t_r$) and then increase to a steady value (after

removing vulnerabilities, the healthcare IoT system becomes more secure and correspondingly more reliable) and it takes more time to get to a steady value for a case depicted as Fa5 due to the fact that the resources spent on the removal of the second vulnerability. System availability enhancing can be achieved by increasing the parameters μ_r and μ_r' that is speeding up the recovery uptime.

44.4 Work related analysis

Healthcare IoT systems are widely used all around the world many of these systems have been deployed throughout the European Union and USA. The University of North Dakota provides a four-year educational program for medical doctors and turned to IoT technology using solution provider AVI Systems. The initiative leads to four-pronged plan, the “Healthcare Workforce Initiative,” which addresses the state’s healthcare staff needs, including reducing the burden on disease, retaining more graduates in North Dakota and improving the healthcare delivery system.

There are some doctoral thesis on the healthcare IoT technology. One among them is [21]. The paper the focuses from technology point of view on advances in connectivity for IoT in healthcare. On the business side, the author identified and presented how the conditions of the health and social care structure in Sweden affect the establishment of IoT solution.

Atlantic Council in partnership with Intel Security [22] provide a series of reports to examine the rewards and risks of the healthcare IoT infrastructures.

One of the most famous and almost all covering paper is [8]. The authors tried to show all the healthcare IoT trends, solutions, platforms, services and applications. They outlined main problems during development and using of such devices related mostly to standardization and regulatory issues. In addition, that paper analyzed healthcare IoT security and privacy features, including requirements, threat models, and attack taxonomies and proposed an intelligent collaborative security model to minimize security risk.

The authors of [23] presented three use cases for quality requirements for IoT in healthcare applications. One of them is for

safety and violence. They gave a simple construct for a patient or caregiver safety use case. Also, they refer to the US Under-writers Laboratories [24] and as well recommended using “traditional techniques for defining misuse and abuse cases”.

In [25] authors provide an integrated healthcare system principles and services for empowering patients. The system is based on advanced cloud-based ICT systems and uses continuous user and technical requirements analysis.

The paper [26] describes a design methodology approach for IoT-based information system for healthcare. The methodology approaches the design target from the perspective of the stakeholders, contracting authorities and potential users; the home care problem not only from the designer’s perspective, but also considering the contracting authority’s and potential users’ requirements, which means that separately from the technical requirements, the design procedure considers the multifarious constraints, including the lifetime, energy issue, usage comfort and even the price.

Conclusions and questions

In this section the materials for Industrial training module “IoT for healthcare systems” are presented. It can be used for preparation to lectures and self-learning. Practical part, recommendations for learning and program of the course are described in [N].

The IoT represents new, exciting opportunities for almost every area of our life. Moreover, of course, a healthcare is not an exception. The IoT can significantly improve the existing healthcare system. Modern healthcare has risen to an unattainable level earlier over the past decade. Today, the healthcare sector is a high-tech industry, where all areas of healthcare are successfully developing that can save lives of previously hopeless patients. The technical equipment of healthcare institutions has significantly been improved; it has become possible to diagnose the disease at the earliest stage and to quickly restore the working capacity of patients. This section presented a brief analysis of international standards and regulations on healthcare IoT requirements. The techniques of healthcare IoT realization are described. The case for IoT infrastructure development with the networked ECG monitor is

presented. The Markov models and simulation results of healthcare IoT infrastructure are shown and discussed.

Nevertheless, with all the benefits of using such networked devices, the security, safety and reliability risks are increasing. Next steps should be dedicated to security and safety assessment of the healthcare IoT infrastructure.

In order to better understand and assimilate the educational material that is presented in this section, we invite you to answer the following questions.

1. What is IoMT and IoHT?
2. What problems do IoMT and IoHT solve in humans' lives?
3. What is difference between medical and healthcare IoT systems?
4. What are the responsibilities of the FDA?
5. What regulation documents for medical equipment certification are used in the EU?
6. How can regulation documents and standards can be divided for the healthcare IoT infrastructure?
7. Which standard is used for medical devices usability certification? What requirements does it describe?
8. What standards are used for medical devices risk management? What requirements do they describe?
9. What standards are used in IoT domain?
10. Which standard describes for IoT Reference Architecture? What requirements does it describe?
11. Describe general IoT infrastructure. What components does it include?
12. What existing solutions do you know for remote persons' health condition monitoring?
13. What protocols are used in the healthcare IoT infrastructure?
14. What is difference of MQTT with other protocols?
15. Is it possible to use the queueing theory to model healthcare IoT systems? What are the assumptions to such systems modelling?

References

1. S. Patel, H. Park, P. Bonato, L. Chan and M. Rodgers, "A review of wearable sensors and systems with application in rehabilitation", *Journal of*

NeuroEngineering and Rehabilitation, vol. 9, no. 1, p. 21, 2012. Available: 10.1186/1743-0003-9-21.

2. "24-Hour Holter Monitoring: Purpose, Procedure, and Results", *Healthline*, 2019. Available: <https://www.healthline.com/health/holter-monitor-24h>. [Accessed: 20- Oct-2018].

3. O. Bay, "mHealth Wearables Boost Patient Healthcare Both Inside and Outside the Hospital", *Abiresearch.com*, 2019. Available: <https://www.abiresearch.com/press/mhealth-wearables-boost-patient-healthcare-both-in/>. [Accessed: 20- Oct- 2018].

4. ISO/IEC 62304:2006, *Medical device software. Software lifecycle*. UK, The international organization of standardization. 2006.

5. ISO 82304, *Software in medical devices*. UK, The international organization of standardization. 2006.

6. "The top 10 causes of death", *Who.int*, 2019. Available: <https://www.who.int/news-room/fact-sheets/detail/the-top-10-causes-of-death>. [Accessed: 10- Mar- 2019].

7. A. Strielkina, D. Uzun and V. Kharchenko, "Modelling of healthcare IoT using the queueing theory", *2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, 2017. Available: 10.1109/idaacs.2017.8095207.

8. S. Islam, D. Kwak, M. Humaun Kabir, M. Hossain and K. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey", *IEEE Access*, vol. 3, pp. 678-708, 2015. Available: 10.1109/access.2015.2437951.

9. D. Krishnan, S. Gupta and T. Choudhury, "An IoT based Patient Health Monitoring System", *2018 International Conference on Advances in Computing and Communication Engineering (ICACCE)*, 2018. Available: 10.1109/icacce.2018.8441708.

10. "MySignals - eHealth and Medical IoT Development Platform", *My-signals.com*, 2018. Available: <http://www.my-signals.com/>. [Accessed: 20- Dec- 2018].

11. A. Pivovarova and A. Pivovarova, "OVERVIEW: ECG Dongle - inexpensive and very accurate pocket cardiograph", *Lifehacker*, 2018. Available: <https://lifehacker.ru/2016/05/03/ecg-dongle/>. [Accessed: 20- Dec- 2019].

12. U. Satija, B. Ramkumar and M. Sabarimalai Manikandan, "Real-Time Signal Quality-Aware ECG Telemetry System for IoT-Based Health Care Monitoring", *IEEE Internet of Things Journal*, vol. 4, no. 3, pp. 815-823, 2017. Available: 10.1109/jiot.2017.2670022.

13. Real time wireless ECG monitoring systemK, 2015. Available: http://www.ksct.iisc.ernet.in/spp/40_series/39S_bestprojreports/39S_BE_0847.pdf. [Accessed: 11- Dec- 2018].
14. "The OSI Model: An Overview", Sans.org, 2018. Available: <https://www.sans.org/reading-room>. [Accessed: 10- Oct- 2018].
15. "IoT - Internet of Things | IoT Network Protocols", Lessons-tva.info, 2018. [Online] (in Russian). Available: www.lessonstva.info/articles/net/013.html. [Accessed: 23- Mar- 2018].
16. "What is MQTT and what does it need in IIoT? Description of the MQTT protocol", Ipc2u.ru, 2018. [Online] (in Russian). Available: <https://ipc2u.ru/articles/prostye-resheniya/chto-takoe-mqtt/>. [Accessed: 23-Mar- 2018].
17. "AD8232 Heart Rate Monitor Hookup Guide - learn.sparkfun.com", Learn.sparkfun.com, 2018. Available: <https://learn.sparkfun.com/tutorials/ad8232-heart-rate-monitorhookup-guide>. [Accessed: 23- Oct- 2018].
18. Lakatos, L., Szeidl, L. and Telek. M. (2012). *Markovian Queueing Systems. Introduction to Queueing Systems with Telecommunication Applications*. New York, NY: Springer, 199–224.
19. Sztrik, J. (2012). *Basic Queueing Theory*. Available at: irh.inf.unideb.hu/~jsztrik/education/16/SOR_Main_Angol.pdf [Accessed: 10-Sept- 2018].
20. U.S. Food and Drug Administration. *Classify your device*. Available at: www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm2005371.htm [Accessed: 18- Dec- 2018].
21. A. Laya, "The Internet of Things in Health, Social Care, and Wellbeing", Doctoral Thesis, KTH Royal Institute of Technology, 2017.
22. J. Healey, N. Pollard and B. Woods, "The Healthcare Internet of Things: Rewards and Risks", Atlantic Council, Washington, 2015.
23. P.A. Laplante, M. Kassab, N.L. Laplante, J.M. Voas, J. "Building Caring Healthcare Systems in the Internet of Things," *IEEE Systems Journal*, pp. 1-8, 2017. Available: 10.1109/JSYST.2017.2662602.
24. "Applied Safety Science and Engineering Techniques. Taking Hazard Based Safety Engineering (HBSE) to the Next Level," *IEEE*, p. 11, 2010.
25. A. Kor, C. Pattinson, R. Pope and A. Schulte, "An Integrated Healthcare System and Services for Empowering Patients", pp. 171-177, 2015.
26. D. Dziak, B. Jachimczyk and W. Kulesza, "IoT-Based Information System for Healthcare Application: Design Methodology Approach", *Applied Sciences*, vol. 7, no. 6, p. 596, 2017. Available: 10.3390/app7060596.

45. SECURITY AND PRIVACY IN IOT FOR HEALTHCARE SYSTEMS

Prof., DrS V. S. Kharchenko, Assoc. Prof., Dr. D.D. Uzun,
PhD student A.A. Strielkina, Dr. O. O. Illiashenko (KhAI)

Contents

Abbreviations	510
45.1 Standards and requirements to security and privacy of healthcare IoT systems.....	511
45.1.1 Standards analysis for IT healthcare systems security and privacy	512
45.1.2 Requirements to security and privacy of healthcare IoT systems	515
45.2 Techniques and tools of healthcare IoT security and privacy assessment	515
45.2.1 Security and privacy gaps analysis.....	515
45.2.2 Attacks tree analysis	518
45.2.3 Theory of games	521
45.3 Markov' s chains and queue theory analysis of healthcare IoT security and availability.....	522
45.3.1 Security and availability models development	522
45.3.2 Cases.....	523
45.4 Work related analysis	529
Conclusions and questions.....	530
References	532

Abbreviations

6LoWPAN – IPv6 over Low power Wireless Personal Area Networks

BNEP – Bluetooth Network Encapsulation Protocol

DoS – Denial of Service

FDA – Food and Drug Administration

FIPS – Federal Information Processing Standards

FTA – Fault Tree Analysis

IEC – International Electrotechnical Commission

IEEE – Institute of Electrical and Electronics Engineers

ISO – International Organization for Standardization

HIMSS – Healthcare Information and Management Systems Society

HIPAA – Health Insurance Portability and Accountability Act

HITECH – Health Information Technology for Economic and Clinical Health

HL7 – Health Level Seven

L2CAP – Logical Link Control and Adaptation Protocol

NIST – National Institute of Standards and Technology

PHI – Protected Health Information

WBAN – Wireless Body Area Network

WLAN – Wireless Local Area Network

45.1. Standards and requirements to security and privacy of healthcare IoT systems

IoT systems can be met in any field of humans' life: sport, education, retail, infrastructure, transport and healthcare. The last one can cause a new scientific revolution within IT and medical fields. Modern joined hardware and software solutions have grown in complexity; decisions regarding patient care have often become entangled in a multitude of goals and means of controls [1]. To stay in the market and thrive, healthcare-related companies and organizations are focusing more on individual objectives – the products companies on product sales, the healthcare delivery organizations on providing services at the right price point, the payers on actuarial modelling. And somewhere in the mix, the traditional goal of obtaining the best results for the patient and overall benefit for the healthcare system was reduced [2]. Dealing with patients' medical data, confidentiality and security and privacy are prevalent for a good health-related product. During transferring and syncing information between networked and connected healthcare devices, data should be encrypted from endpoint to endpoint.

The healthcare field is extremely sensitive due to the dealing with a personal data and private information (Protected Health Information, PHI) which shall be highly secured. That is why data confidentiality and data security have to be considered on the designing stage of the healthcare IoT architecture. Such issues as reliability, authenticity also should be given a high priority.

According to the latest publications [3] – [5] there a lot of issues related to cybersecurity assessment of healthcare IoT-based systems due to their complexity. Among them are different objectives, legal and regulatory contexts, governance arrangements, diversity of implementation technologies, etc. That is why it is needed to develop an approach that takes into account all aspects of development processes, regulatory and standardization, different methodologies for security, risk, hazard assessment, etc.

When any changes are made to a medical device, including the embedded software, means additional cost and time to market are under the requirement for renewed Food and Drug Administration (FDA) approval.

Aforementioned leaves known vulnerabilities open longer than would otherwise occur and forces extra cost to the manufacturer in the regulatory compliance process. The FDA Safety and Innovation Act report distinguished that with the increase in data exchange between devices and electronic medical record systems, and the use of the wireless spectrum, that the FDA needed to be clearer in its aspects of regulation that will implement to cybersecurity vulnerabilities [6].

PHI includes sensitive data from medical records. It can be any patient's private information which needs to be highly protected. HIPAA (Health Insurance Portability and Accountability Act of 1996) is the US legislation that gives data privacy and security provisions for safeguarding medical information and data. The law has emerged into greater distinction in recent years with the increase of health data breaches caused by cyber and ransomware attacks on the health insurers and providers [7].

45.1.1 Standards analysis for IT healthcare systems security and privacy

The cloud-based healthcare services grant new assuring course for the healthcare industry to advance and achieve by introducing new advancement and practices in existing one. It encompasses the patients' data safety, decreasing the operational cost, increasing the popularity of healthcare services among the users, high computation and easy to access facility, best resources utilization, sharing of records, research support etc. [7]. On the other hand, based on the cloud computing cannot guarantee securing for PHI data and safety of medical and healthcare devices even if the system is built in compliance just to international regulations. In this case cloud computing and its cybersecurity issues are needed to be reviewed.

Each layer of healthcare IoT system have been taken into account and the cybersecurity regulation model for a trust healthcare IoT system was built. Fig. 45.1 represents a hierarchical model for secure healthcare IoT system.

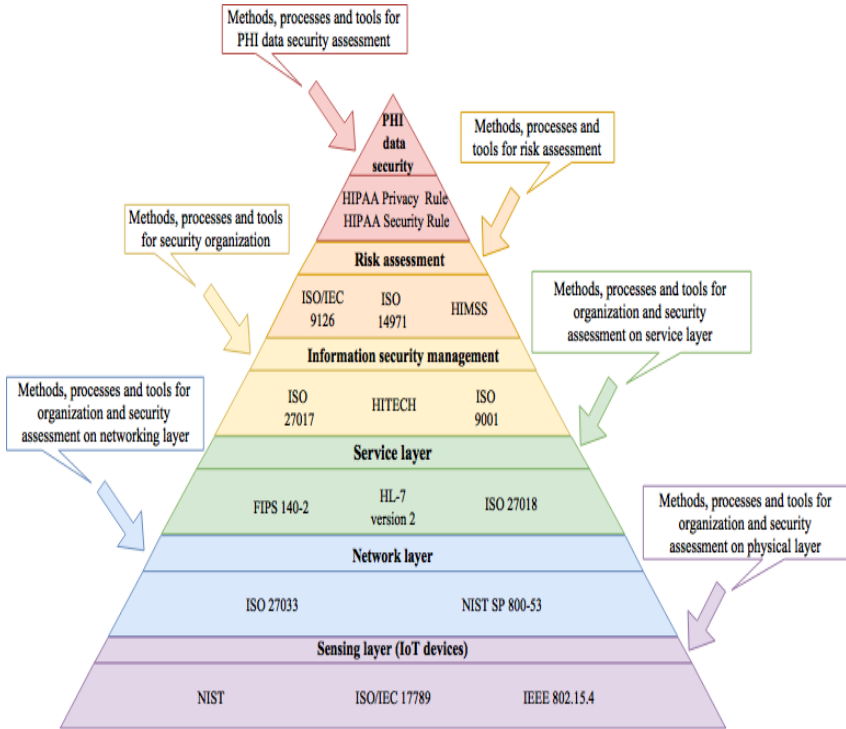


Fig. 45.1 – Hierarchical cybersecurity model for healthcare IoT system

Sensing layer includes standards dedicated for IoT in general, not only for medical devices:

1. NIST's Cybersecurity for the IoT program promotes the development and employment of different types of regulation techniques to enhance the cybersecurity of the IoT devices and the environments in which they are deployed. By co-operating with stakeholders across government, industry, international bodies and academia, the program directs to cultivate trust and foster an environment that empowers innovation [8].

2. ISO/IEC 17789:2014 defines the cloud computing reference architecture. This involves the cloud computing roles, activities, functional elements and bonds between them [9].

3. IEEE 802.15.4 defines the physical layer and access control for low-rate wireless personal area networks. It is maintained by the IEEE 802.15 working group. The most popular wireless specifications are based on it. Also, it can be used with 6LoWPAN and common protocols to form a wireless embedded Internet [10].

Network layer standards are dedicated to provide network security that includes devices, security of management activities associated with the devices, applications/services, and end-users, in addition to the information being transferred security – ISO 27033 [11] and represents the security controls and associated assessment procedures – NIST 800-53 [12].

Service layer has to be protected by standards for clouds and service configurations such as FIPS 140-2 [13] for static data, ISO 27018 [14] for protecting data in a cloud and Health Level 7 [15] for transfer medical data between software applications used by various providers. Compliance with ISO 27018 guarantees a systematic approach for data protection and proves that the provider is a "conscious citizen" in the cloud ecosystem. On this layer there are data storage and processing.

On the top there are three layers related to information security management, risk assessment and PHI data protection as a high rank component. Normative documents which are presented there explains how to work with sensitive medical data (HIPAA [16], [17]), how to organize security in healthcare and medical systems (Health Information Technology for Economic and Clinical Health (HITECH) [18], ISO 27017 [19]) and how to reduce risks associated with humans' life.

Information security management layer gives guidance and recommendations guidance on the cloud security aspects (ISO 27017), improving healthcare quality, safety and efficiency, testing (HITECH) and a system of quality management (ISO 9001 [20]).

Risk assessment layer has standards for the evaluation of quality (ISO/IEC 9126 [21]), risk management for medical devices (ISO 14971 [22]) and a compliance with Healthcare Information and Management Systems Society (HIMSS [23]).

PHI data security layer consists of the rules that institute policies and procedures for maintaining the privacy and the security of

individually identifiable health information, outlines numerous attacks relating to healthcare, and establishes civil and criminal penalties.

45.1.2 Requirements to security and privacy of healthcare IoT systems

Based on the analysis results the following requirements for medical and healthcare IoT systems could be highlighted:

Requirement 1: Ensure that organization follows cybersecurity rules. Variety of the international standards provide us with a trust solutions for building cybersecurity systems, protecting data and managing trouble-free work of the devices. It is highly recommended to build the systems in compliance to the official regulations.

Requirement 2: Apply trust network architecture. As IoT systems are network based and all data is transmitted through the network it's important to avoid malware attacks while information is being sent from one device to another.

Requirement 3: Provide PHI data protection. Protected Healthcare Information include itself private patients' information. The information might be related to an individual's present, past or future health condition, either in physical or mental terms, as well as the current condition of a person. Data modification can cause irreversible consequences.

The presented profile-forming database of standards was used to develop a comprehensive methodology for the cybersecurity assessment of the healthcare IoT system.

45.2 Techniques and tools of healthcare IoT security and privacy assessment

45.2.1 Security and privacy gaps analysis

Networked healthcare devices raise four main issues:

- *random failures* (the complication of connecting IT to the creates opportunities to fall work, operational etc.);
- *privacy* (this issue is extremely important due to patient personal data collected);
- *deliberate disruption* (as any other networked technology medical network systems could have a lot of vulnerabilities. The US

Department of Homeland Security is studying about twenty trials of presumed cybersecurity flaws in the connected medical devices that criminals could exploit, such as forcing an infusion pump to overdose a patient, or instructing a heart implant to “deliver a deadly jolt of electricity”);

– *malware disruption* (malware attacks could damage the whole system by attacking just single device).

Failures also may occur in the IoT based systems. Fig. 45.2 depicts in outline the main causes of healthcare IoT based system failures.

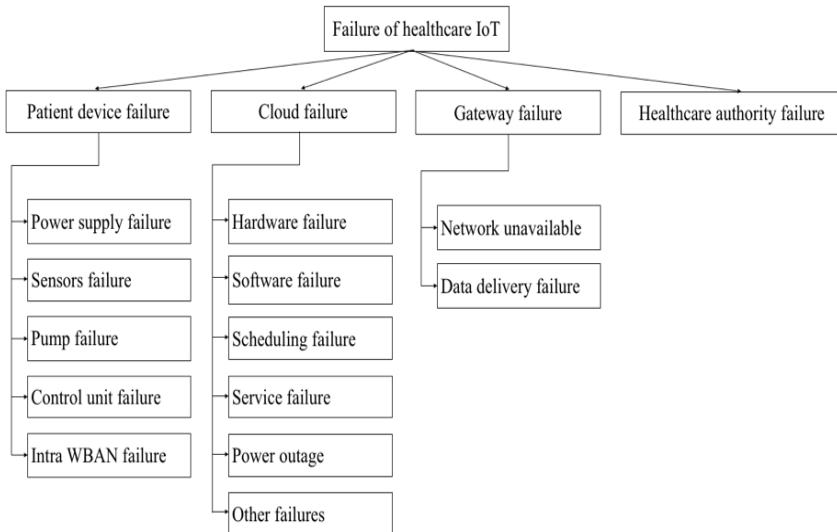


Fig. 45.2 – Classification of the healthcare IoT failures

Since cyberattacks are the possible consequences of the threat implementation the existing vulnerabilities. Therefore, it is necessary to consider the attack as a malicious action affecting the healthcare IoT system's performance.

About 250 cyberattacks were targeted on health sector (only publicly disclosed incidents) in 2016-2017. There are several types of attacks on IoT that were discussed in many papers. The authors of these papers presented attacks' targets, weaknesses, and technique of the security attacks. The main categories of IoT attacks are aimed for control, data, controllers (end-nodes) and networks. Attacks on data are

very devastating in the healthcare field due to the physician–patient privilege and a patient privacy and confidentiality. Attacks on control involve imply an intruder's intention to gain access to the management of both the entire healthcare IoT system and individual components. Attacks on controllers are aimed at end-nodes (patients' devices) to gain access to control them and make a physical damage. Attacks on networks are aimed to sniffing out, copying the confidential information or any other data flowing in the networks.

After analyzing classification of attacks according the main aims and focus is presented in Fig. 45.3.

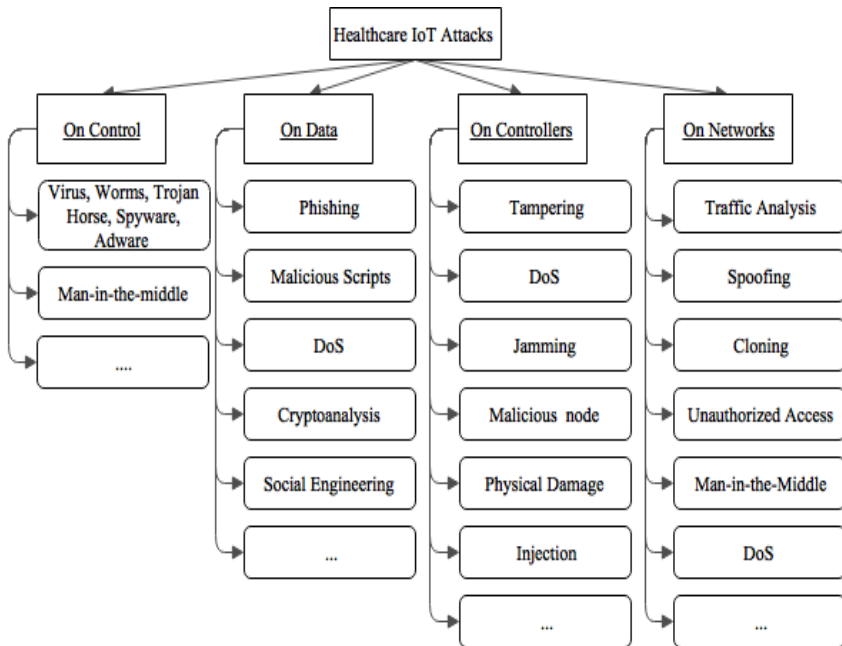


Fig. 45.3 – Classification of the healthcare IoT attacks

Such attacks on vulnerabilities can prevent the devices and infrastructure to communicate correctly and without failures.

45.2.2 Attacks tree analysis

To analyze the security and/or safety problems of the IoT system, a fault or attack tree analysis method can be applied. Guidance for Industry and FDA Staff mentions the use of this method when creating healthcare devices to identify and classify hazards. The scope of failure trees is not limited to information technology; this method is also used in such areas as the aviation industry, the military industry, the nuclear industry, etc. The fault tree aggregates the possible ways of achieving the main event (component failure, subsystem failure, and successful attack). To build the fault tree, it is necessary to analyze possible attacks on the IoT infrastructure or its individual components.

In the analysis of security, the cyber assets of the system should be identified – this is something that has value and importance for the system owner or for the intruder who can attack the system. Since the IoT infrastructure consists of several components and communication channels, it may be advisable to consider the security problems of each component and communication channels separately. In this case, several trees will be built as a decomposition of one large tree.

Consider an abstract example of a fault tree for the IoT system. As mentioned above, first we need to identify the main event. Examples of such an event may be the fault of a certain sensor, violation of the integrity, or confidentiality of the transmitted information. For healthcare systems, the issues of violation of the information privacy can be especially relevant. For critical decision-making systems, the main event can be the damage to the patient's health.

After determining the main event, it is necessary to determine the most frequent options for achieving this event. Assume that the failure of at least one of the components – cloud storage, information gathering device, communication channel, or healthcare provider – can lead to the occurrence of the main event “IoT infrastructure failure.” The failure of the cloud storage can occur if all previous events A_1, \dots, A_k occur. The failure of the information-gathering device may arise under the condition that all previous events B_1, \dots, B_l occur. The failure of the communication channel can occur if all previous events C_1, \dots, C_m occur. The failure of a healthcare provider can arise under the condition that all previous events D_1, \dots, D_n occur. In this case, $k, l, m,$ and n are

the numbers of events preceding the corresponding event. The described tree structure is shown in Fig. 45.4.

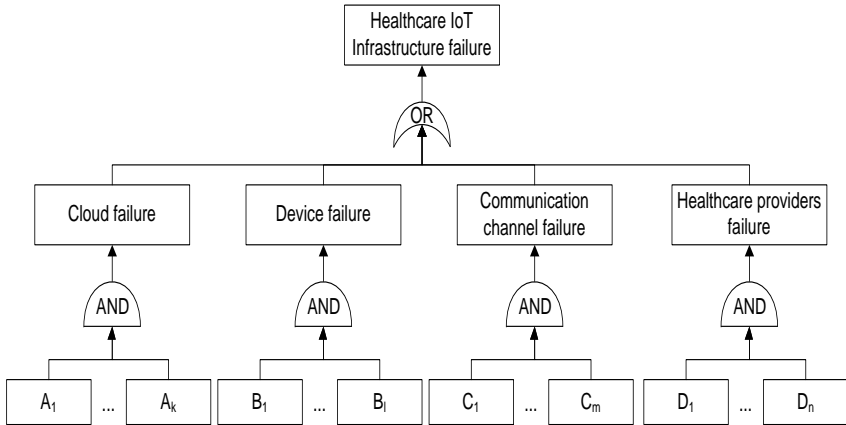


Fig. 45.4 – The structure of FTA

Let us consider the fragment of the fault tree in the subsystem of the device worn by the patient. Calculation of the amount of insulin administered occurs on the local device, and the current blood sugar level is transferred to the Cloud for monitoring by a healthcare professional. The critical values of the blood sugar level can be obtained if the measurement is incorrect or when incorrect insulin doses are administered. Information about such an event should be noted in the controlling healthcare organization. The fault tree fragment shown in Figure 45.4 shows possible scenarios in which critical values of the indicators may not be transmitted to the Cloud.

Using this model probability of system failure (prevent the sending of critical indicators), P_{sf} can be calculated using the following formula (45.1)

$$P_{sf} = P_1P_2P_3 + P_1P_4P_5 \quad (45.1)$$

where $P_1 - P_5$ are probabilities of the following events correspondingly: access to WLAN is gained; unencrypted channel is used; integrity check is missed; real device is disconnected; and device identification is broken.

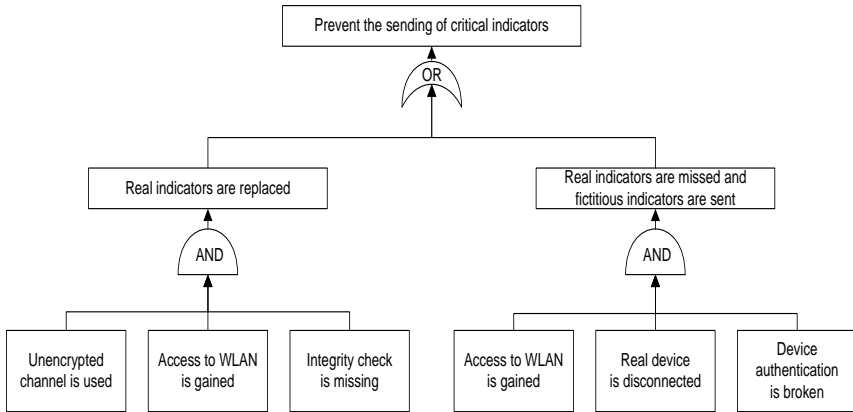


Fig. 45.5 – The tree fragment of possible scenarios in which critical values of the indicators may not be transmitted to the Cloud

It is assumed that sending prevention of the critical values of the indicators in the cloud can be achieved in two ways. The first method is shown on the left side of the tree; in this case, the sensor data have been replaced due to transmission over the unencrypted channel and lack of integrity check. The second method is shown on the right side of the tree; it replaces the actual device with a dummy device, which sends to the cloud indicators that are certainly not critical.

In practice, attack or fault trees have a more complex structure, combining various options for using the elements AND/OR. The structure depends on the most likely scenarios of attacks considered in the process of analyzing the security problems of the healthcare IoT system. In this case, different scenarios can be complex and have intersections in the form of identical events.

To calculate the probability of the main event occurrence, it is necessary to parameterize the constructed tree. By parameterization we mean the definition of the probability of occurrence of events at the lower level. Data for parameterization can be obtained by collecting statistics of attacks and component failures. In the absence of statistics and, as a result, the impossibility of determining quantitative indicators, it is possible to use the method of expert assessments and the use of

variables of fuzzy logic (for example, low, medium, and high probability).

In our case, failures in the system can arise due to external actions (attacks), or without them (failures caused by processes occurring within the components of the system). The purpose of the tree is to determine the probability of the main event. The tree in Fig. 45.5 can be viewed as part of the tree in Fig. 45.4, which is used to evaluate the reliability of the system.

The disadvantage of fault trees is the impossibility of determining all possible scenarios for the occurrence of the main event. There is also the problem of detailing each scenario, since excessive detail can reduce the visibility of the overall security state of the infrastructure in question. Besides, in case of implementing maintenance procedures, the development of trees becomes very complex and their parameters such as recovery rates or middle time of repair cannot be taken into account as a whole.

Using the considered trees allows to graphically represent possible scenarios for reaching the main event, assess the probability of the main event, and identify the weaknesses in the security or safety of the infrastructure. In addition, the fault tree is convenient to use when choosing countermeasures to counter possible failures and attacks.

45.2.3 Theory of games

Analysing security issues against various threats it is advisable to consider the actions of the two sides: the parties to the protect (of the healthcare IoT system) and the parties to the offender (an attacker). The relationship between these players is determined as a payoff matrix. The condition for the effective protection is a rule: the cost of the protection tools should be less than the cost of the losses incurred in the successful implementation of attack.

An approach how to calculate an effective protection factor was presented in [24]:

$$\lambda_{ij} = \frac{S_j}{(1 - p_{ij}^{(p)}) \square p_{ij}^{(a)} \square D}, \quad i = \overline{1, n}, j = \overline{1, m}, \quad (45.2)$$

where S_j - is a cost of protection tool; $p_{ij}^{(p)}$ - is an attack reflection probability; $p_{ij}^{(a)}$ - is an attack probability; D - the value of the average damage of the healthcare IoT system.

45.3 Markov' s chains and queue theory analysis of healthcare IoT security and availability

Nevertheless, with all the benefits of using such networked devices, the security, safety and reliability risks are increasing. Thus, the security, safety and reliability assessment of such systems is a complex process. Such systems are characterized by a large number of failures due to the dynamism, multicomponence and multilevelness. For reducing these issues, the fragmentedness of the models being developed should be used in some cases to describe repeated parts of models which have similar structure and differ only values of some parameters. It concerns fragmentedness caused by changing of design faults and attacked vulnerabilities number and the corresponding failure rates.

45.3.1 Security and availability models development

It is necessary to develop mathematical models for an availability function definition. In this paper, the assumptions considered to the development of the availability models are the following:

- the rates of failures and attacks are constant, the flows of failures and attacks' rates obey the Poisson distribution law;
- the models do not consider eliminating of any reasons because of what failures caused, the system provides just standard protection tools;
- the tools of control and diagnostics are triggered ideally; it means that they detect correctly and in time all appearing failures and faults;
- the occurring process in the healthcare IoT system is a process without after-affects, the probability of each event in the future depends just on the state of the IoT system in the present time and does not depend how the system arrived at this state previously. Thus, it satisfies the Markov property.

In general, in the healthcare IoT system, the failures of single (or attacks on) subcomponents are possible. These failures may lead to the failures of the main components of infrastructure (i.e. insulin pump, cloud, etc.). In its turn, the failures of main components may lead to

failure of the whole healthcare IoT system. Fig. 45.6 shows the dependence of the healthcare IoT system failures, where state 0 corresponds to condition when there is no any failure in the system, state 1 – there is one failure (of subcomponent), state 2 – there are two failures (subcomponent and main element), state 3 – there are three failures (the failure of the whole healthcare IoT system).

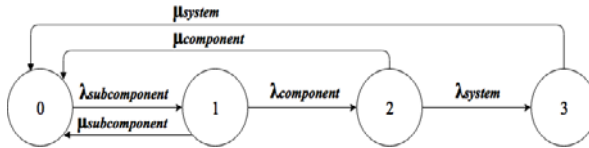


Fig. 45.6 – Dependence of the healthcare IoT failures

45.3.2 Cases

A Markov Model of Healthcare IoT Considering Component Failures. In more details Fig. 45.7 shows a Markov graph of the functioning of the main components of healthcare IoT system if failures occur, where λ - the failure rate, μ - the recovery rate. Thereby, the basic states of the healthcare IoT system are: 1 - normal condition (upstate) system; 2 - failure due to the power supply (battery) pump causes discharge, recharging and/or causing damage; 3 - failure of any one and/or more sensors of the insulin pump due to the out-of-order, does not deliver any output to inputs, delivers null output values and/or no meaningful values and/or impurity etc.; 4 - pump failure (inaccurate size/rate of insulin dose) due to the components defects, improper position of pump, ambient temperature, air pressure and/or design errors etc.; 5 - software of insulin pump control module failure due to buffer overflow or underflow, incorrect libraries, wrong algorithms or programming, threshold setting error etc.; 6 - hardware of insulin pump control module failure due to overheating, short or open circuit, high leakage current, high or low impedance, missed alarm, false alarm, fail to read/write data and/or design error etc.; 7 - intra wireless body area network (WBAN) communication failure due to the packet loss, isolation, a communication module failure (e.g., L2CAP, BNEP etc.), header corruption and/or length mismatch and/or payload corruption etc.; 8 - insulin pump (as the patient's complex) failure due to the

failure of any one or more main components; 9 - extra gateway communication partial failure due to data delivery failures; 10 - extra gateway communication partial failure due to Bluetooth/cellular/WiFi network unavailable; 11 - partial failure due to the refusal of the mobile application of the reader (control unit); 12 - cloud software failure due to a planned or unplanned reboot, software updates and/or complex design; 13 - cloud hardware failure due to hard disk failures, RAID controller, memory and/or other devices; 14 - cloud scheduling failure due to overflow and/or timeout; 15 - cloud service failure due to request stage and/or execution stage; 16 - cloud failure due to power outage; 17 - cloud failure due to the failure of any one and/or more cloud components; 18 - failure due to incorrect assignment or programming of the device by a healthcare authority related to device functions or lack of functions; 19 - failure of the IoT healthcare system.

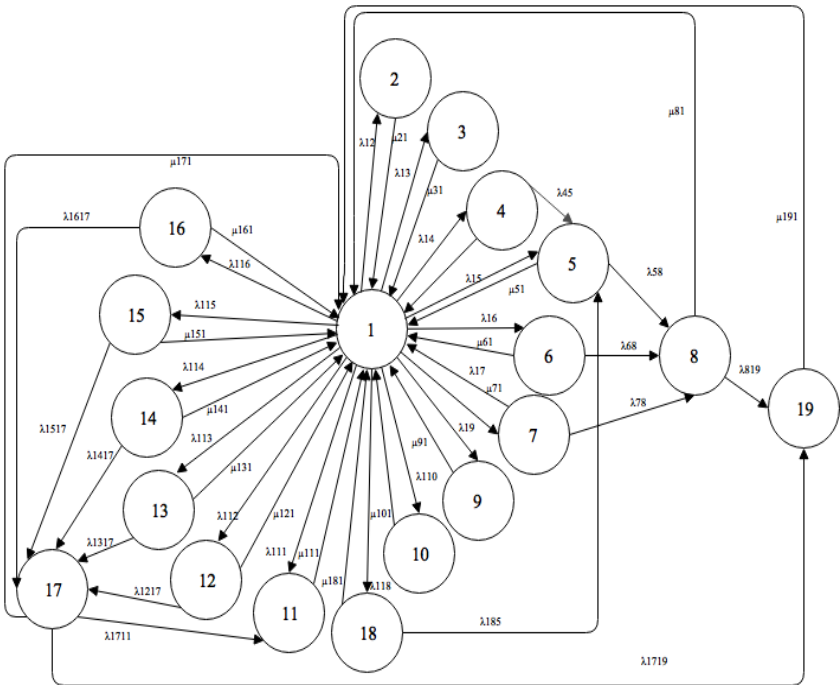


Fig. 45.7 – A Markov's graph of the healthcare IoT failures

A system of the Kolmogorov differential equations for presented Markov model is:

$$dP_1 / dt = -(\lambda_{12} + \lambda_{13} + \lambda_{14} + \lambda_{15} + \lambda_{16} + \lambda_{17} + \lambda_{19} + \lambda_{110} + \lambda_{111} + \lambda_{112} + \lambda_{113} + \lambda_{114} + \lambda_{115} + \lambda_{116} + \lambda_{118})P_1(t) + \mu_{21}P_2(t) + \mu_{31}P_3(t) + \mu_{41}P_4(t) + \mu_{51}P_5(t) + \mu_{61}P_6(t) + \mu_{71}P_7(t) + \mu_{81}P_8(t) + \mu_{91}P_9(t) + \mu_{101}P_{10}(t) + \mu_{111}P_{11}(t) + \mu_{121}P_{12}(t) + \mu_{131}P_{13}(t) + \mu_{141}P_{14}(t) + \mu_{151}P_{15}(t) + \mu_{161}P_{16}(t) + \mu_{171}P_{17}(t) + \mu_{181}P_{18}(t) + \mu_{191}P_{19}(t);$$

$$dP_2 / dt = -\mu_{21}P_2(t) + \lambda_{12}P_1(t);$$

$$dP_3 / dt = -\mu_{13}P_3(t) + \lambda_{13}P_1(t);$$

$$dP_4 / dt = -(\mu_{41} + \lambda_{45})P_4(t) + \lambda_{14}P_1(t);$$

$$dP_5 / dt = -(\mu_{51} + \lambda_{58})P_5(t) + \lambda_{16}P_1(t) + \lambda_{45}P_4(t) + \lambda_{185}P_{18}(t);$$

$$dP_6 / dt = -(\mu_{61} + \lambda_{68})P_6(t) + \lambda_{16}P_1(t);$$

$$dP_7 / dt = -(\mu_{71} + \lambda_{78})P_7(t) + \lambda_{17}P_1(t);$$

$$dP_8 / dt = -(\mu_{81} + \lambda_{819})P_8(t) + \lambda_{58}P_5(t) + \lambda_{68}P_6(t) + \lambda_{78}P_7(t);$$

$$dP_9 / dt = -\mu_{91}P_9(t) + \lambda_{19}P_1(t);$$

$$dP_{10} / dt = -\mu_{101}P_{10}(t) + \lambda_{110}P_1(t);$$

$$dP_{11} / dt = -\mu_{111}P_{11}(t) + \lambda_{111}P_1(t) + \lambda_{1711}P_{17}(t);$$

$$dP_{12} / dt = -(\mu_{121} + \lambda_{1217})P_{12}(t) + \lambda_{112}P_1(t);$$

$$dP_{13} / dt = -(\mu_{131} + \lambda_{1317})P_{13}(t) + \lambda_{113}P_1(t);$$

$$dP_{14} / dt = -(\mu_{141} + \lambda_{1417})P_{14}(t) + \lambda_{114}P_1(t);$$

$$dP_{15} / dt = -(\mu_{151} + \lambda_{1517})P_{15}(t) + \lambda_{115}P_1(t);$$

$$dP_{16} / dt = -(\mu_{161} + \lambda_{1617})P_{16}(t) + \lambda_{116}P_1(t);$$

$$dP_{17} / dt = -(\lambda_{1711} + \lambda_{1719} + \mu_{171})P_{17}(t) + \lambda_{1217}P_{12}(t) + \lambda_{1317}P_{13}(t) + \lambda_{1417}P_{14}(t) + \lambda_{1517}P_{15}(t) + \lambda_{1617}P_{16}(t);$$

$$dP_{18} / dt = -(\mu_{181} + \lambda_{185})P_{18}(t) + \lambda_{118}P_1(t);$$

$$dP_{19} / dt = -\mu_{191}P_{19}(t) + \lambda_{919}P_8(t) + \lambda_{1719}P_{17}(t).$$

Initial values are:

$$P_1(0) = 1, P_i(0) = 0, i = 2,3, \dots, 19.$$

To solve a system of the linear Kolmogorov differential equations it is necessary to carry out the collection and analysis of statistics on failures of healthcare IoT systems.

Simulation of the Model. Hence the initial data for Markov model simulating were taken from the statistics of the insulin pump manufacturers, the Cloud providers and experts' assessments. Due to the heterogeneous nature and complexity of statistical data, and not to overflow with excess information, the sequence of rates' calculations and the rates are not given.

The up-state is state 1, and eighteen others are states with failures of different components and parts of the healthcare IoT system. The obtained probabilities of finding the healthcare IoT system in each state of Markov model are shown below (stationary values):

Pf1 = 0.9853745;	Pf2 = 0.000103622;	Pf3 = 0.003330566;
Pf4 = 0.000251795;	Pf5 = 0.001162896;	Pf6 = 0.0003859747;
Pf7 = 0.006145591;	Pf8 = 0.0009757008;	Pf9 = 0.001486934;
Pf10 = 0.0006328081;	Pf11 = 3.207395e-05;	Pf12 = 3.070724e-05;
Pf13 = 1.056492e-05;	Pf14 = 2.90451e-05;	Pf15 = 2.596815e-05;
Pf16 = 5.734457e-06;	Pf17 = 3.038937e-08;	Pf18 = 1.545724e-05;
Pf19 = 2.957985e-08.		

Hence $A(t) = P_1(t)$, Fig. 45.8 shows the availability function value changing before a transition to the stationary value ($A_{stationary} = 0.9853745$). According to the simulation results the function gets a qua approximately at step 2300 h, i.e. 3 months later after beginning of work.

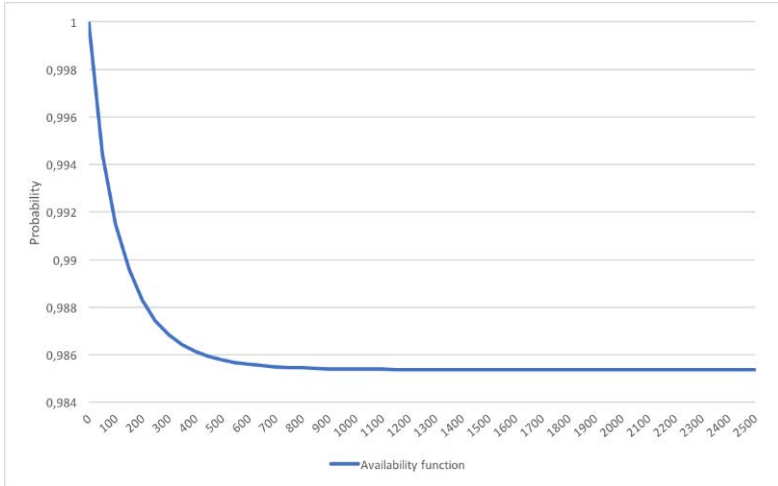


Fig. 45.8 – Availability function changing before a transition to the stationary value

The analysis of obtained results shows that the complete failure of the healthcare IoT system does not happen too often (one case on the analysed time interval due to the complete failure of the Cloud). Nevertheless, failures of constituent elements of the system arise quite often that may affect the performance of mission-critical functions of the healthcare IoT system and in the worst case, lead to the death of the patient. The most often failures are due to the failure of the insulin pump and its particular elements and components and some components of the Cloud.

Availability of the system can be improved by more fast recovery (repair) of the equipment and system resources and application of more reliable devices.

A Markov Model of the Healthcare IoT Considering the Attacks on Vulnerabilities. The model does not take into account eliminating of vulnerabilities and design faults. The failure and/or attack, recovery and/or repulse rates are constant.

Fig. 45.9 shows a Markov's graph of the main components functioning of the healthcare IoT system during attacks, λ - the failure and/or attack rate, μ - the recovery and/or reflection rate. Thereby, the basic states of the healthcare IoT system are: 1 - normal condition

(upstate) system; 2 – traffic analysis attack; 3 – spoofing attack; 4 – cloning attack; 5 – unauthorized access to the network or database; 6 – failure of the network; 7 – failure due the data leakage; 8 – man-in-the-middle attack; 9 – DoS/DDoS attack; 10 – failure due the loss of control; 11 – attacks on software (i.e., viruses, worms, Trojan horses, spyware, adware, etc.); 12 – phishing attack; 13 – malicious scripts injection attacks; 14 – social engineering; 15 – failure or controllers (hardware, end-nodes); 16 – tampering of the end-nodes attack; 17 – jamming attack; 18 – malicious node injection attack; 19 – physical damage; 20 – complete failure of healthcare IoT system.

Such Markov model for the healthcare IoT system can be divided into four levels: the first level is the upstate (state 1), the second level are the states state the transition to which occurred due to attacks (states 2-5, 8, 9, 11-14, 16-19), the third level implies states with different failures (states 6, 7, 10, 15); the fourth level is a failure of a whole system (state 20). So, there is only one up-state in the considering system.

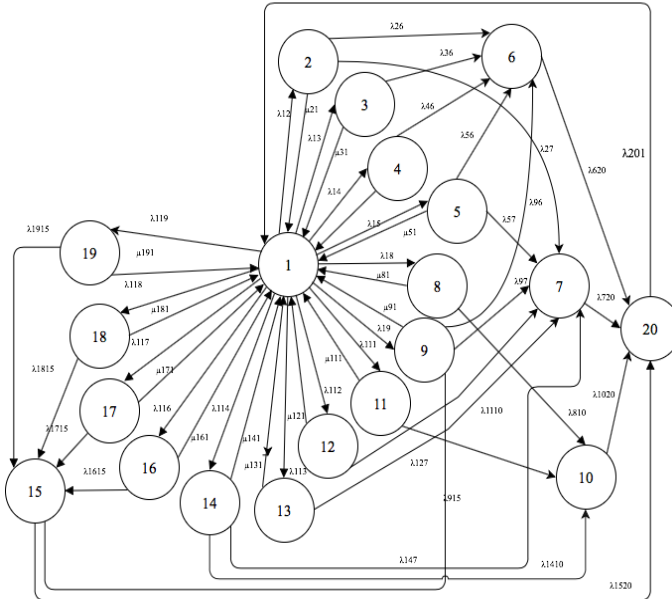


Fig. 45.9 – Markov’s graph of attacks on the healthcare IoT infrastructure

After solving the system of Kolmogorov-Chapmen equations, it is possible to obtain the availability function value of the healthcare IoT system, the number of system failures due to cyberattacks.

To solve a system of linear Kolmogorov differential equations it is necessary to collect and analyse statistics on failures and attacks on the healthcare IoT infrastructure. The data for model simulation was taken from the statistics and experts' assessments.

The obtained stationary value probabilities for the considered Markov model are:

Pa1 = 0.9200121;	Pa2 = 5.73576e-05;	Pa3 = 4.294692e-05;
Pa4 = 0.0001696415;	Pa5 = 0.0002171216;	Pa6 = 0.01081887;
Pa7 = 0.04191969;	Pa8 = 4.88764e-05;	Pa9 = 0.0001009014;
Pa10 = 0.01365914;	Pa11 = 5.696207e-05;	Pa12 = 0.0001208568;
Pa13 = 1.517664e-05;	Pa14 = 0.001280493;	Pa15 = 0.00138444;
Pa16 = 0.000618885;	Pa17 = 0.002611121;	Pa18 = 0.0005009447;
Pa19 = 0.005841538;	Pa20 = 0.0005229814.	

The analysis of the obtained results shows that the biggest influence on the change in the availability function has the λ_{19} rate – DoS/DDoS attack (one of the most frequent and destructive attacks), next is the λ_{14} rate – social engineering (i.e., human factor), next the rates λ_{15} – unauthorized access to the network or database and λ_{11} – attacks on software (i.e., viruses, worms, Trojan horses, spyware, adware, etc.), that are confirmed by statistical data.

45.4 Work related analysis

While the field of information technologies is growing it absorbs any aspect of humans lives and attracts a lot of attention for further researches. The healthcare field is not an exception. There are numerous of scientific papers dedicated to the IT healthcare revolution and potential problems.

The authors of [25] presented all healthcare IoT trends, solutions, platforms, services and applications. They outlined main problems during development and using of such devices related mostly to standardization and regulatory issues. In addition, that paper analyzed healthcare IoT security and privacy features, including requirements,

threat models, and attack taxonomies and proposed an intelligent collaborative security model to minimize security risk.

Attacks on vulnerabilities of IoT based systems can be simulated using Markov's modelling. In [26] was presented and explained how Markov modelling can be used to evaluate the reliability of the complex systems parallel redundant system. In [27] was shown that dependability consists of many measures (as reliability, availability, safety, performability and security and its attributes). Authors presented a good state-of-the-art how Markov models can be applied to the dependability and security analysis.

The authors of [28] presented three use cases for quality requirements for IoT in healthcare applications. One of them is for safety and violence. They gave a simple construct for a patient or caregiver safety use case. Also, they refer to the US Under-writers Laboratories [29] and as well recommended using "traditional techniques for defining misuse and abuse cases".

The faults/attacks trees are a flexible tool that is used to model various undesirable events in different spheres of human activities. For example, in [30], trees were used to analyze hacked email victimization scenarios. In [31], FTA was used to calculate the medication error.

Conclusions and questions

In this section the materials for Industrial training module "IoT for healthcare systems" are presented. It can be used for preparation to lectures and self-learning. Practical part, recommendations for learning and program of the course are described in [N].

IoT-based healthcare systems are making a revolution in any industry of people' life. More and more hospitals are starting to implement network of physical devices. Such approach raised some risks because devices that contain a treasure trove of patient data are attractive targets for cybercriminals. While building a trust IoT architecture it is highly recommended to follow official international regulations and norms.

The hierarchical cybersecurity model for healthcare IoT system is developed. It shows how to protect information, devices and humans' life by securing each layer of IoT system. Moreover, the conceptual

model of cybersecurity assessment for the healthcare IoT system is proposed.

The overview of the healthcare IoT system failures and attacks is presented. To determine the security and/or safety problems of the healthcare IoT infrastructure, a method for analyzing fault/attack trees was examined, which makes it possible to estimate the probability of failure/attack on the healthcare IoT system. A Markov models set for the healthcare IoT infrastructure that allows taking into account the specificity of end user devices, communication channels, technologies of data flows and safety and security issues of these components has been developed. Based on the conducted analysis and classification of the main possible failures and attacks on healthcare IoT infrastructure the Markov models considering failures and attacks on components are constructed. For the developed models the probabilities of finding IoT system in each state of the Markov model are shown. The obtained results show possible most frequent failures and attacks on the healthcare IoT system.

Future steps will be devoted to the enhancement of hierarchical cybersecurity model taking into account evolving regulations and technologies, specifically concentrating on the privacy aspect.

In order to better understand and assimilate the educational material that is presented in this section, we invite you to answer the following questions.

1. What are the most prelevant issues dealing with patients' medical data?
2. Why do the medical data should be protected from endpoint to endpoint?
3. What is the PHI?
4. What are the responsibilities of the FDA?
5. What is the HIPAA?
6. What levels does the cybersecurity regulation model have?
7. What does NIST's Cybersecurity for the IoT program include?
8. What standards are used for medical devices risk management? What requirements do they describe?
9. What standards are used in cloud computing reference architecture?

10. What standards are used on network level of the cybersecurity regulation model?
11. What standards are used in service level of the cybersecurity regulation model?
12. What are requirements to security and privacy of healthcare IoT systems?
13. What is the classification of the healthcare IoT infrastructure failures?
14. What is the classification of the healthcare IoT infrastructure attacks?
15. For what reason is attack tree analysis used?
16. For what reason is game theory approach used?
17. Give assumptions for Markov model using in the healthcare IoT security and availability modeling.

References

1. K. Taylor, H. Ronte and S. Hammett, *Healthcare and Life Sciences Predictions 2020 A bold future?*. London: The Deloitte Centre for Health Solutions, 2014.
2. Elton and A. O'Riordan, *Healthcare Disrupted: Next Generation Business Models and Strategies*, 1st ed. Wiley, 2016, p. 288.
3. *Internet of Things realising the potential of a trusted smart world*. London: Royal Academy of Engineering, 2018, p. 54.
4. "Improving cybersecurity requires major coordinated effort, say top engineers - Royal Academy of Engineering", *Raeng.org.uk*, 2018. [Online]. Available: <https://www.raeng.org.uk/news/news-releases/2018/march/improving-cybersecurity-requires-major-coordinated>. [Accessed: 14- Mar- 2018].
5. J. Nurse, S. Creese and D. De Roure, "Security Risk Assessment in Internet of Things Systems", *IT Professional*, vol. 19, no. 5, pp. 20-26, 2017.
6. Rouse, M., *HIPAA (Health Insurance Portability and Accountability Act)*. [Online]. Available: <http://searchhealthit.techtarget.com/definition/HIPAA>. [Accessed: 05- Oct- 2018].
7. "Cloud Computing Systems and Applications in Healthcare", *Advances in Healthcare Information Systems and Administration*, 2017.
8. *NIST Cybersecurity for IoT programs*. [Online]. Available: <https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program>. [Accessed: 11 - Oct- 2018].
9. ISO 50545: 2014 *Cloud Computing. Software references*. UK, The international organization of standardization, 2014.

10. IEEE802.15.4 *Low-Rate Wireless Personal Area Networks*. US, IEEE standards association, 2011.

11. ISO/IEC 27033-1:2015 *Preview Information technology -- Security techniques -- Network security*. Geneva, The international organization of standardization, 2015.

12. J T Force, T Initiative, "Security and privacy controls for federal information systems and organizations" in NIST Special Publication, pp. 53, 2013.

13. N. F. PUB, "140-2: Security requirements for cryptographic modules," Information Technology Laboratory, *National Institute of Standards and Technology*, 2001.

14. ISO/ IEC 27018:2014(E) *Protection for personally identifiable information*, Switzerland, 2014.

15. Health Level Seven. [Online]. Available: <http://www.hl7.org>. [Accessed: 05- Oct- 2018].

16. *Standards for privacy of individually identifiable health information [45 CFR parts 160 and 164]*. Department of Health and Human Services, 2002.

17. *Security Standards for the Protection of Electronic Protected Health Information [45 CFR parts 160 and 164]*. Department of Health and Human Services, 2003.

18. *The Health Information Technology for Economic and Clinical Health Act (HITECH) Act*, 2009. [Online]. Available: <http://www.hipaasurvivalguide.com/hitech-act-text.php>. [Accessed: 1 - Mar- 2018].

19. ISO/IEC 27017:2015 *Code of practice for information security controls based on ISO/IEC 27002 for cloud services*. The international organization of standardization, 2015.

20. ISO 9001:2015. *Quality management systems — Requirements*. The international organization of standardization, 2015.

21. ISO/IEC 9126:2001. *Software engineering -- Product quality*. The international organization of standardization, 2015.

22. ISO 14971. *Application of risk management to medical devices*. The international organization of standardization, 2009.

23. *The Healthcare Information and Management Systems Society*. [Online]. Available: <http://www.himss.org>. [Accessed: 1 - Mar- 2018].

24. A. Strielkina, A. Tetskyi, B. Selin, O. Solovyov, D. Uzun. "Service for Vulnerabilities Analysis and Security Assessment of Open Source Systems," *CERes Journal*, vol. 1, iss. 2, pp. 53-64, 2015.

25. S. Islam, D. Kwak, M. Humaun Kabir, M. Hossain and K. Kwak, "The Internet of Things for Health Care: A Comprehensive Survey", *IEEE Access*, vol. 3, pp. 678-708, 2015. Available: 10.1109/access.2015.2437951.

26. K. S. Trivedi and D. Selvamuthu, "Markov modeling in reliability," in *Encyclopedia of Quantitative Risk Analysis and Assessment*. John Wiley & Sons, Ltd, 2008. DOI: 10.1002/9781118445112.stat03635.

27. D.M. Nicol, W.H. Sanders, and K.S. Trivedi, "Model-based evaluation: From dependability to security", *IEEE Transactions on Dependable and Secure Computing*, vol. 01, no. 1, pp. 48-65, 2004. DOI: 10.1109/TDSC.2004.11.

28. P.A. Laplante, M. Kassab, N.L. Laplante, J.M. Voas. "Building Caring Healthcare Systems in the Internet of Things," *IEEE Systems Journal*, pp. 1-8, 2017. Access: 10.1109/JSYST.2017.2662602.

29. Applied Safety Science and Engineering Techniques. Taking Hazard Based Safety Engineering (HBSE) to the Next Level. IEEE, p. 11, 2010.

30. V. Nagaraju, L. Fiondella, T Wandji, T. "A survey of fault and attack tree modeling and analysis for cyber risk management," *Proceedings of the IEEE International Symposium on Technologies for Homeland Security (HST)*, pp.1-6, 2017.

31. M. Lyons, S. Adams, M. Woloshynowych, C. Vincent. "Human reliability analysis in healthcare: a review of techniques," *International Journal of Risk and Safety in Medicine*, v. 16, pp. 223-237, 2004.

46 .WEARABLE AND EMBEDDED IOT-BASED SOLUTIONS FOR BIOMEDICAL APPLICATIONS

DrS., Prof. I. S. Skarga-Bandurova,

Assoc. Prof., Dr. T.O. Biloborodova (V. Dahl EUNU)

Contents

Abbreviations	536
46.1 Biomedical sensors and data acquisition techniques.....	537
46.1.1 Analyzing IoT sensor data in medicine.....	540
46.1.2 Study of health data acquisition techniques in IoT environments.....	541
46.2 Biomedical signal processing models for real time health data analytics	543
46.2.1 Real time tagging, aggregation, and temporal correlation ...	544
46.3 Developing and testing smart wearable devices	547
46.3.1 Embedded and wearable IoT-based systems for biomedical applications	547
46.3.2 Wearable IoT device configuration.....	550
46.3.3 Data analysis and prediction techniques	554
46.3.4 Cases	562
46.4 Work related analysis.....	570
Conclusions and questions.....	572
References.....	572

Abbreviations

AI – Artificial Intelligence
ARIMA – Autoregressive Integrated Moving Average
BD – Big Data
BIC – Bayesian Information Criterion
CI/CD – Continuous Integration and Continuous Delivery
CPLD – Complex Programmable Logic Device
DNA – Deoxyribonucleic Acid
ECG – Electrocardiogram
EEG – Electroencephalogram
EGG – Electrogastrogram
EHR – Electronic Health Record
EMG – Electromyogram
ENG – Electroneurogram
IIR – Infinite Impulse Response
IoT – Internet of Things
ML – Machine learning
PCG – Phonocardiogram
RNA – Ribonucleic Acid
SNR – Signal-to-Noise Ratio
WBAN – Wearable Body Area Network

46. Wearable and embedded IoT-based systems for biomedical applications

Health IoT Systems are becoming more common every day. Healthcare IoT is an important part of the digital transformation of healthcare. Internet of Things (IoT) includes sensors, devices, software and hardware, a network connection, and data exchange. Application IoT in healthcare provides creating new business models and performing changes in workflows, improving the quality of care, prevention and diagnosis of diseases. Another great advantage of Healthcare IoT is that it is still in its infancy stage that gives us a wide range of opportunities [1].

Healthcare IoT allows us to perform monitoring of health indicators, automatic treatment management, tracking of human condition data in real time. Wearable applications today track physical condition, physical activity, track pathological abnormalities and coordinate user actions. Improving the relevance of data interpretation reduces the time spent by end users on data collection. Possession of skills and abilities to interpret data on the health and condition of the patient will help to avoid chronic diseases, improve cognitive functions, improve physical condition, etc.

In this Chapter we will discuss some aspects related to developing Wearable and Embedded IoT-based solutions for biomedical applications. Execute a quick tour on biomedical sensors and data acquisition techniques; discuss the configuration of wearable devices on the example of an ECG device and deep into data analysis and prediction technique on the example EEG data gathered from the wearable device.

46.1 Biomedical sensors and data acquisition techniques

Sensors are the key components in all devices and measurement systems. They are widely used to monitor a person's physical parameters in medicine, health care, and other related fields. In accordance with the basic principles of work, biomedical sensors can be divided into physical, chemical and biological [2]. Classification of sensors on this principle is presented in Fig.46.1.

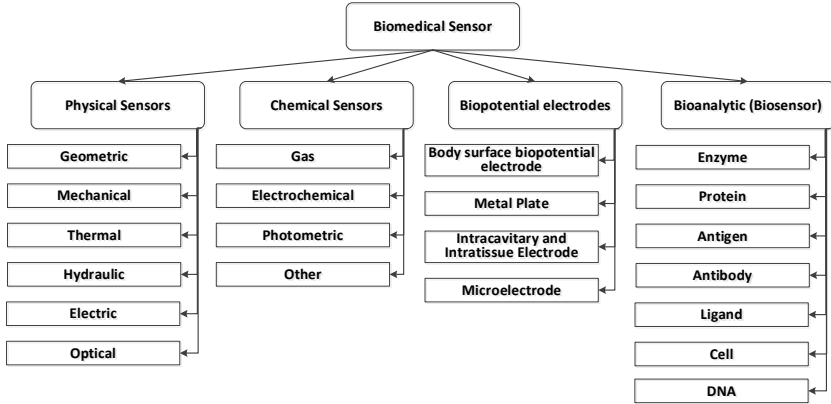


Fig. 46.1 – Classification of Biomedical Sensors

Physical sensors are used to measure blood pressure, body temperature, current and blood viscosity, biological magnetic field, etc. [3]. Chemical sensors are used to determine the constituent elements and the concentration of body fluids, for example, to determine the pH, blood glucose concentration. Biological sensors are used to determine enzymes, antigen, antibodies, hormones, DNA, RNA, microorganisms. Physical sensors measure geometric, mechanical, thermal, and hydraulic variables. In biomedicine, the use of this type of sensor allows you to measure parameters such as muscle movement, blood pressure, body temperature, blood flow, etc. A special role in the use of sensors for diagnostic purposes is occupied by sensors recording electrical phenomena in the body, commonly called electrodes. The most common of these are EEG, ECG, EMG sensors. Another example of a physical sensor is an optical sensor that uses light to collect information.

Chemical sensors operate on chemical quantities, such as identifying the chemical composition, determining the concentration of various chemicals, and monitoring chemical activity in the human body. An example of a chemical sensor is electrochemical sensors, which are used to measure the concentration of chemicals. Also, these include photometric sensors, which are optical devices for detecting chemical concentrations of substances based on changes in light transmission, reflection, or color.

Bioanalytical sensors are essentially chemical sensors, but they are often classified as a separate category of sensors. In bioanalytical sensors, physic-chemical changes in the biologically active material resulting from the interaction with the analyte are converted to an electrical output signal by an appropriate transducer. The sensitive components of a bioanalytical sensor may contain enzymes, cells, antibodies, DNA, RNA, and other biologically active substances. In accordance with the biological sensitive component, bioanalytical sensors can be divided into five classes: enzyme, microbial, cellular, tissue and immune. The main application of bioanalytical sensors in biomedicine is in the detection of clinical and chemical research data and the monitoring, monitoring, and correction of the state of certain physiological parameters of a person.

There is another interesting taxonomy of biomedical sensors proposed in [4] where authors distinguish 4 types of sensors they are physiological sensors, wearable activity sensors, human sensors and contextual sensors.

Physiological sensors measure patient physiological statistics or vital signs. (e.g., iPhone applications for heart rate monitoring).

Wearable activity sensors measure attributes of gross user activity, different from narrowly focused vital sign sensors. (e.g., accelerometers used for gait monitoring. Sports shoe manufacturers enabled their running shoes with sensors capable of tracking walking or jogging activities).

Human sensors: means that we can use humans as the integrators of sensing results. (e.g. people use Web searches and Twitter to generate reports on important events related to their health).

Contextual sensors are embedded in the environment around the user to measure different contextual properties. Examples include motion detection sensors, temperature sensors, audio and video sensors, weather sensors, etc.

In addition, one more existing classification of sensors is their separation into active and passive.

Active sensors are those sensors that require an external power source to convert the input signal to an output signal, while *passive sensors* are those that inherently provide their own energy or receive energy from the measured phenomenon into useful electrical potential or current.

Depending on the intended use, biomedical sensors can be evaluated by the following key parameters.

Measurement range: The sensor range corresponds to the minimum and maximum operating limits, which are expected to be accurately measured by the sensor.

Sensitivity: Sensitivity refers to the ratio of change in output for a given change in input signal. Another way to determine the sensitivity is to find the slope of the calibration line connecting the input signal with the output. High sensitivity means that a small change in input causes a significant change in output.

Accuracy (correct measurement): Accuracy refers to the difference between the true value and the actual value measured by the sensor. Classically, accuracy is expressed as the ratio between the previous difference and the true value; it is defined as the percentage for all indications. Note here that the true value can be traced to the main reference standard.

Precision (measurement accuracy): Precision refers to the reproducibility of measurements under the same conditions. Highly reproducible readings indicate high accuracy. Precision should not be confused with Accuracy. For example, the measurement can be very accurate, but not necessarily correct.

Resolution: The resolution is characterized by a minimum change in the measured value that the sensor can sense.

Reproducibility: Reproducibility is the ability of a sensor to produce identical results when the same conditions are met. It is determined by the maximum difference in the output values of the sensor, obtained by two measurements of parameters. Usually, it is expressed as a percentage of the maximum value of the input signal. With a small measurement range, reproducibility is very high. Reproducibility may vary by measurement range.

46.1.1 Analyzing IoT sensor data in medicine

Biomedical sensors generate massive data sets, structured and unstructured, obtained at high speed, requiring real-time analysis. Biomedical data, in addition to the usual data of simple signals, include such complex data as images (mammograms, x-rays, magnetic resonance imaging, etc.), wave analysis (EEG, ECG, audio files) [5].

The challenges arising from the analysis of such data can be determined as follows.

Increase measurement accuracy: The improvement of biomedical wearable devices leads to an increase in the accuracy of the units of measurement and, consequently, to an increase in the volume of data.

Duration of biomedical sensor data: As a rule, biomedical wearable devices continuously receive data on the state of the human body, which must be processed to quickly respond to critical situations.

Variety of data: The analysis of biomedical sensor data for medical problems will not be complete without taking into account the patient's historical data. There are various medical data stored in a medical electronic card, various medical records, and the results of examinations. This heterogeneous data may include text, images, audio, and video. Also, it is important to bear in mind that the same data category obtained with the help of various devices may have different measurement standards, etc.

Extracting deep knowledge: The significance of data from a single data source is limited. Thus, the current direction of research is the development of an approach based on the use of pooled data. This will allow extracting more high-quality useful knowledge from various data-sources and personalizing the recommendations.

The integration of data from various sources, platforms, systems is provided through various software interfaces. Their use allows you to easily extract the necessary data, knowledge, information. If necessary, the extracted information and information can be converted into feedback information and / or actions.

46.1.2 Study of health data acquisition techniques in IoT environments

According to the World Health Organization (WHO), heart disease is one of the leading causes of death worldwide. The development of information technology and IoT allow monitoring of the state of human heart activity using inexpensive, wearable devices [6]. ECG monitoring and diagnostic systems are the most common among IoT systems developed in the field of health. They are designed to receive, collect, monitor and analyze heart rate data and an electrocardiogram of a

person. Information is obtained using a wearable device that helps to track and identify changes in the state of the heart.

Next, we consider the stages of designing a person's ECG signal monitoring system in real time.

A block diagram of the monitoring system of the human ECG signal is shown in Figure 46.2 [7].



Fig. 46.2 – Simplified health monitoring system structure

ECG monitoring device

A wearable ECG device is responsible for collecting ECG data from human skin, and then transmitting this data to an access point through a wireless channel.

ECG monitoring data storage

Server, IoT cloud storage provides a fast and convenient way to store ECG signal data. The IoT cloud architecture for ECG monitoring includes server selection and basic data transfer procedures. IoT cloud storage uses three types of servers of different functionalities, that is, a storage server, an HTTP server, and an MQTT server. Basic data transfer processes using the IoT cloud storage of a specific patient's ECG signal can be easily accessed using a web browser. In addition to the patient himself, a person who has the appropriate access rights can receive information to this patient's personal data.

Graphic interface for monitoring ECG data

Regardless of additional mobile applications, users can log into the IoT cloud storage and access the ECG data just by visiting a specific website using the web browser of any OS platform. In addition to displaying ECG signals in real time, you can also get data on the

history of life, history of the disease, select the start and end times for transmitting ECG signal data.

46.2 Biomedical signal processing models for real time health data analytics

Biomedical signal analysis and processing consists of measuring signals from biological sources, related to various physiological processes. Examples of such signals include the electrocardiogram (ECG), electroencephalogram (EEG), electroneurogram (ENG), phonocardiogram (PCG), electromyogram (EMG), the vibromyogram (vibration signals that accompanies EMG), electrogastrogram (EGG), carotid pulse (CP), signals recorded using catheter-tip sensors (signals such as left ventricular pressure, right atrial pressure, aortic pressure), the speech signals, and many others.

These signals can be either discrete or continuous depending on the kind of care or severity of a particular pathological condition. The processing and interpretation of physiological signals is challenging due to the low signal-to-noise ratio (SNR) and the interdependency of the physiological systems. The signal data obtained from the corresponding medical instruments can be copiously noisy, and may sometimes require a significant amount of preprocessing.

Some tools and common techniques for data preprocessing are represented in Volume 1 (Part II).

Abnormal values of any variable do not always uniquely indicate a certain state of the organism. Thus, a separate classification of the states of each variable studied, obtained as a result of monitoring the human biophysical state, is not able to predict the human condition. Also, it is necessary to take into account the conflict of values of variables when the forecast is carried out in conditions of a normal state of one variable and an anomalous state of another. Modeling real data is usually associated with the processing of uncertain information. Traditionally, uncertainties are handled by probabilistic methods, such as Bayesian methods and Dempster-Shafer theory. The main limitation of the Bayesian inference is that it cannot simulate the inaccuracy of measuring errors. The theory of evidence or Dempster-Shafer (D-S) allows conclusions to be drawn from the incomplete and uncertain knowledge provided by various independent data sources. The first

advantage of its use is the ability to cope with ignorance and lack of information. In particular, the Dempster-Shafer theory gives a clear assessment of the inaccuracies and contradictions between information from various sources and can deal with any combination of hypotheses. The second advantage is the possibility of obtaining a quantitative assessment of inaccuracies and conflicts that may exist between different sources of information. In addition, the use of the Dempster-Shafer approach is characterized by low computational power and the possibility of using incomplete information. The main disadvantage of the method is the struggle with a high degree of conflict. Despite this shortcoming, the D-S theory is a convenient alternative for data fusion.

Using the basics of D-S theory in data classification has a certain advantage. In the conditions of imperfect, incomplete, uncertain, irrelevant or redundant data, the use of elements of the Dempster-Shafer theory allows us to improve the efficiency of data classification.

For classification the D-S approach can be viewed as an extension of classical probabilistic reasoning, which draws conclusions from incomplete and uncertain knowledge provided by various independent sources of knowledge. The Dempster-Shafer theory quantifies inaccuracies and conflicts that may exist between different sources of information. Also, the advantage of using the D-S theory is low computational power [8].

46.2.1 Real time tagging, aggregation, and temporal correlation

Different arrays of biomedical data (streaming, structured, unstructured, categorical, obtained in real time) can be combined and used to search for hidden patterns in them. The integration of medical, biomedical, clinical data and their analysis using a single model make it possible to develop a high-quality system for supporting the adoption of medical decisions presented in Fig. 46.3, which uses EHR.

Biomedical real-time status monitoring allows for an analogy between physiological changes and indicators.

The requirements for analytics of integrated biomedical data include the following technologies.

Real-time data labeling: classifying data as it arrives.

Real-time aggregation: using a sliding window to aggregate data allows you to extract patterns from data and detect deviations in them.

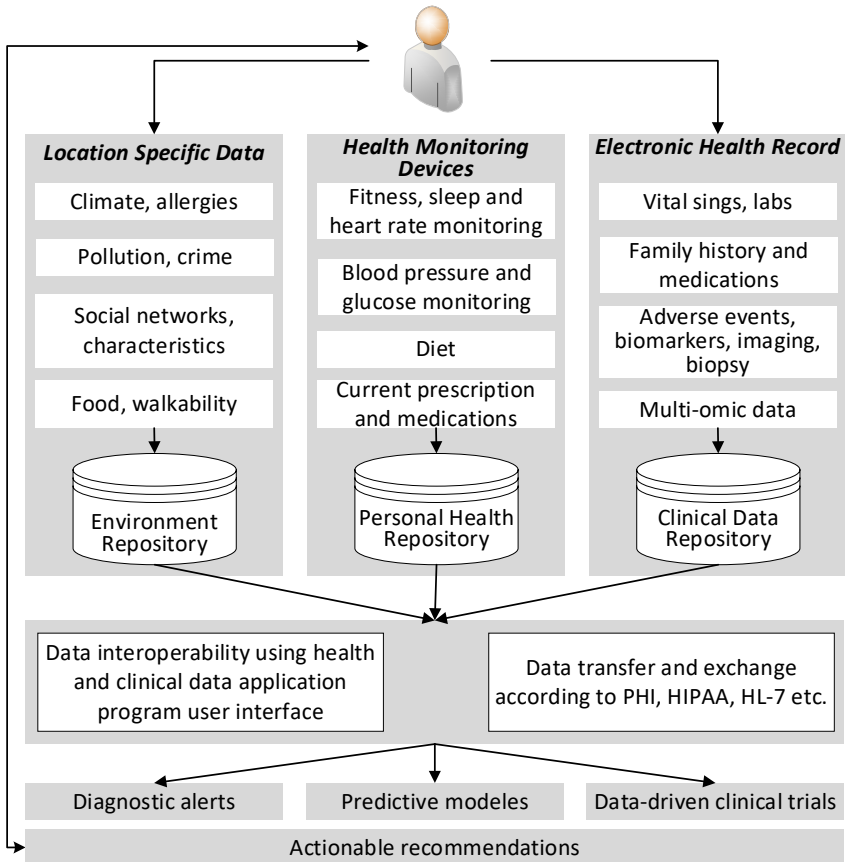


Fig. 46.3 – Health care and well care data for incorporating biomedical, health care and wellness monitoring information with EHR

Formally, the aggregated time series can be defined as follows [9]. A one-dimensional discrete time series $X = \{x_k\}$ is a set of values of the cumulative variable x at discrete time k , where $0 \leq k < T$, and T is the length of the series. X denotes the number of runs in the data. The purpose of real-time aggregation is to determine X , which satisfies the set value of the quality parameter, denoted as $R = \{r_k\}$.

The quality parameter is obtained by measuring the quality of the R series using the average relative error E between R and the original X series:

$$E = \frac{1}{T} \sum_k \frac{|r_k - x_k|}{\max\{x_k, \delta\}}, \quad (46.1)$$

where δ is a user-defined constant (also called a threshold) to mitigate the effect of excessively small query results. We define $\delta = 1$ for the total number of data series. The usefulness of R increases as each r_k approaches x_k , the extreme case of which would have $r_k = x_k$ for each k .

Real-Time Time Correlation: Identify future events based on association with past events in real time.

Temporal correlation is also called trend analysis [10]. Under conditions of temporal correlation, the data demonstrate regular cyclical regular fluctuations. These fluctuations have a constant interval between successive peaks, which is the cycle period. Different models can be used to model historical patterns of behavior and change: regression, moving average, etc.

Along time, all measurements can be formulated as time series. In trend analysis, an observed time series can be decomposed into three components: the trend (long term direction), the seasonal factor (systematic, calendar related movements) and the irregular factor (unsystematic, short term fluctuations). As a result, a general trend analysis method can be expressed as:

$$y_t = \text{local_mean} + \text{seasonal_factor} + \text{error} \quad (46.2)$$

where the local mean is assumed to have an additive trend term and the error is assumed to have zero mean and constant variance. At each time t , the smoothing model estimates these time-varying components with level, trend, and seasonal smoothing states denoted by L_t , T_t , and S_{t-i} ($i=0, 1, \dots, M-1$), respectively. The set of updating equations are given by

$$\begin{aligned} L_{t+1} &= \alpha(y_{t+1} - S_{t+1-M}) + (1-\alpha)(L_t + T_t) \\ T_{t+1} &= \beta(L_{t+1} - L_t) + (1-\beta)T_t \\ S_{t+1} &= \gamma(y_{t+1} - L_{t+1}) + (1-\gamma)S_{t+1-M} \end{aligned} \quad (46.3)$$

where α , β and γ are three convergent matrices of smoothing constants, and M is the time interval for a season. The m -step-ahead forecast at time t is

$$\hat{y}_{t+m} = L_t + mT_t + S_{t+m-M} \quad (46.4)$$

Note that, the parameters α , β and γ of regression models are learned from the past time series by minimizing the errors between the estimated values from models and their actual observations.

46.3 Developing and testing smart wearable devices

46.3.1 *Embedded and wearable IoT-based systems for biomedical applications*

The development of information technology in healthcare is leading to an increasing use of wearable devices for monitoring biomedical information.

The use of Embedded and wearable IoT-based systems for biomedical applications can be divided as follows, as it shown in Figure 46.4.

Health monitoring systems provide monitoring of the patient's physical condition for the prevention of pathological conditions before any symptoms appear (posture correctors [12], fitness trackers [13-15]) and systems that attempt to detect health at an early stage.

Systems attempting to detect health at an early stage are aimed at detecting medical conditions at an early stage by monitoring and analyzing various biomedical signals, such as heart rate, blood glucose, blood sugar, EEG and ECG for a long period of time.

Medical care automation systems, unlike health monitoring systems, medical automation systems improve the patient's quality of life with the presence of the disease, providing the necessary therapy.

In terms of their functionality, they can be divided into medication administration systems (insulin administration systems) and systems used during the rehabilitation of the patient.

The human computer interface [16] systems are used to extract the context from the implicit information received, collected, processed by wearable devices, which characterizes the situation of a person or place

related to a conversation, helps us transfer ideas to each other and respond accordingly [17,18].

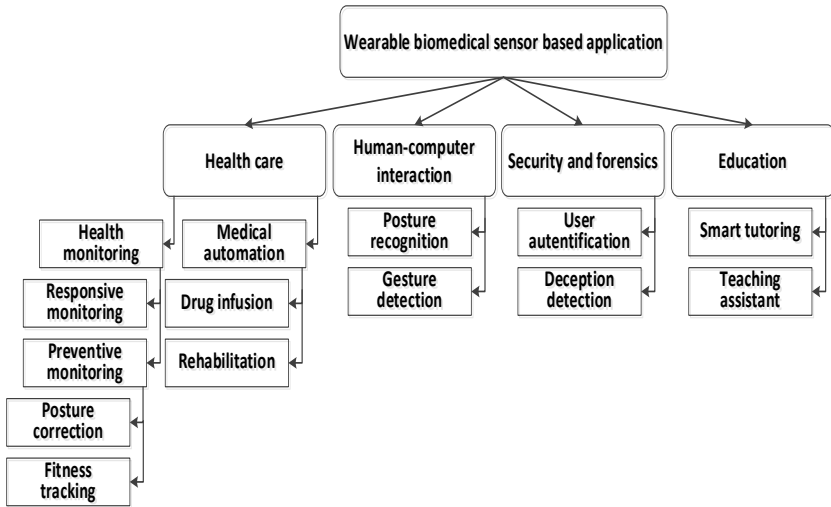


Fig. 46.4 – The scope of an applications based on wearable biomedical sensor [11]

Also, systems developed in the field of information security for detecting lies [19] and authentication of an individual can be referred to Embedded and wearable IoT-based systems for biomedical applications.

Lie detection systems process collected data from various signals (usually heart rate, blood pressure, and accelerometers) to detect suspicious changes in a person's physical condition.

Authentication systems refer to the verification process of identifying a person's identity based on certain credentials [20].

Another area of application for embedded and wearable IoT-based systems is smart learning: learning systems that choose the best learning plan according to student responses.

The architecture of a wearable biomedical information monitoring system is represented by three main components, presented in Fig.46.5.

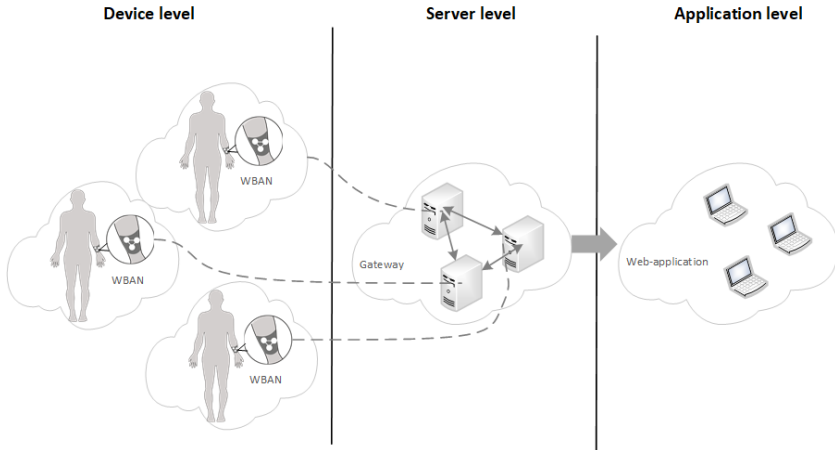


Fig. 46.5 – Health monitoring system architecture
(Adapted from [21, 22])

The first necessary component is various types of wearable devices and sensors that perceive the physical signals of the human body, which are directly wearable devices.

Biomedical sensors can also be directly integrated into garments and accessories, thus forming a wearable body area network (WBAN) [23].

WBAN is a subset of wearable biomedical sensors and systems that can be used to control, stimulate, treat, replace the biological and physical functions of the human body [24].

Such integration requires consideration of two general limitations when developing a biomedical information monitoring system: limited memory capacity of the device and limited power capacity. These restrictions affect the storage, processing and transmission of data:

1. Data received by the device cannot be stored on it for a long period of time and must be transferred to another device / server.
2. When developing a wearable system for monitoring biomedical information, energy-saving data processing algorithms have an advantage.

These factors determine the need for a second component of the system — external storage, processing, and data transfer devices. Data can be transmitted directly from sensors or using external devices with more computational power (eg, a smartphone). Continuous processing

of data in conjunction with the operation of the wireless network adapter consumes a lot of energy resources, which can quickly be exhausted and as a result, disrupt the execution of its direct purpose. External devices usually perform primary signal processing and transfer data to the next level (cloud storage, servers) for further analysis and long-term storage.

As an external device, WBAN can control the physiological parameters of the human body and be used for their collection and transmission.

The third component is represented by cloud storages, servers. Since wearable biomedical information monitoring devices and base stations have limited resources, the resulting data is usually sent to servers, cloud storage for processing and long-term storage.

46.3.2 Wearable IoT device configuration

Consider the configuration of wearable devices on the example of an ECG device.

A wearable ECG device is responsible for collecting ECG data from human skin, and then transmitting this data to an access point through a wireless channel. As shown in fig. 46.6, the ECG monitoring node in our system mainly includes: 1) a sensor module; 2) controller module with wireless adapter; and 3) power module.

1. Sensor module is the basis of the monitoring device, which is responsible for obtaining human ECG data.

Recorded physiological signals usually consist of a source signal and noise. Noise occurs at each stage of data collection, before they are digitized. Noise of the power supply module, muscular noise, noise of the analog-digital converter suppresses ECG signals.

Power line interference is an electromagnetic field from a power line, causing sinusoidal interference at 50 or 60 Hz.

This noise causes problems when interpreting low frequency signals such as an ECG. Consequently, many methods have been used to eliminate power line noise in ECG signals [25]. In [26], a nonlinear function of wavelet coefficient shrinking was used to remove the power line frequency, an adaptive noise removal method was used in [27], and in [28] the procedure was used to subtract the power line interference

from the ECG, which applies to almost all possible cases sampling frequency and interference frequency.

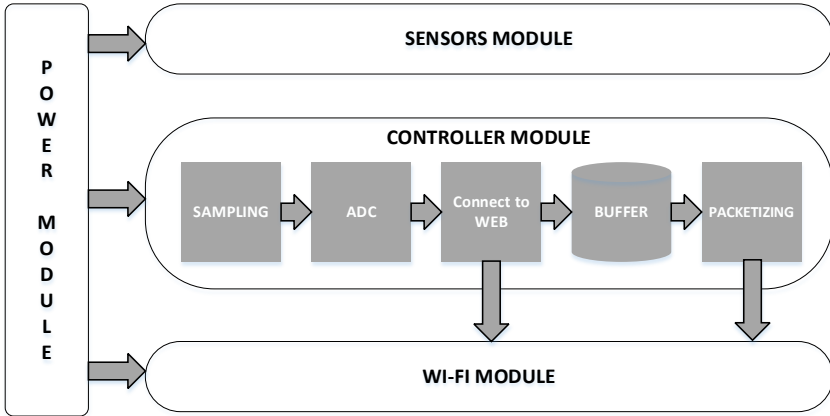


Fig. 46.6 – Wearable device configuration

This module filters and amplifies the received ECG signal. The frequency of the ECG signal lies between 0.5 Hz and 100 Hz [29] and this must be taken into account when choosing the method of filtering the ECG signal. To eliminate this kind of noise, an Infinite impulse response (IIR) filter can be used. The equation for this filter can be represented as follows

$$y[n] = \sum_{k=0}^M b_k x[n-k] + \sum_{k=1}^N a_k y[n-k], \quad (46.2)$$

where M is the feedforward filter order; N is the feedback filter order; b_k are the feedforward filter coefficients; a_k are the feedback filter coefficients; $x[n]$ is the input signal; $y[n]$ is the output signal.

To eliminate the baseline wander in the ECG, which can be caused by breathing, electrode impedance, body movement, various methods are used. Often used is a base level interference suppression method based on a Butterworth bandpass filter. The transfer function of the analog Butterworth filter can be represented as follows as a fractional rational function.

$$H(s) = \frac{\sum_{n=0}^N b_n s^n}{\sum_{m=0}^M a_m s^m}, \quad (46.5)$$

where b_n and a_m - real filter coefficients, a $s = j\omega$ complex variable.

After filtering, the signal is amplified using an operational amplifier.

2. A *controller module* with a wireless adapter is used to process and transmit the received ECG signal. In the controller module, it is possible to set the necessary parameters for additional signal processing, its buffering, packaging for further transmission via a wireless channel. This provides fast and convenient access to the Internet for transmitting ECG data in real time to a server or IoT cloud storage.

3. *Power module* provides reliable power supply of each module in the ECG monitoring device.

Detection of a QRS complex and measurement of heart rate.

Usually, the following elements can be distinguished on an ECG, as shown in Fig. 46.7, among them are the P, Q, R, S, T wave.

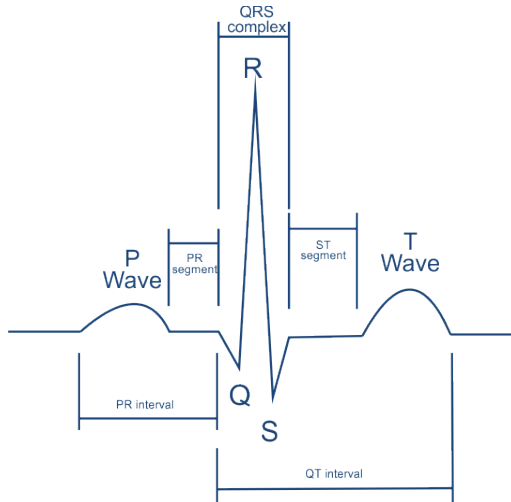


Fig. 46.7 – Elements of ECG complex

Sometimes we can see the inconspicuous U wave. The P wave reflects the process of depolarization of the atrial myocardium, the QRS complex - depolarization of the ventricles, the ST segment and the T wave reflect the processes of repolarization of the ventricular myocardium.

The QRS complex can be identified using a common method for determining ECG parameters. R-peak is easier to distinguish from noisy components, as it has large amplitude (Fig. 46.8).

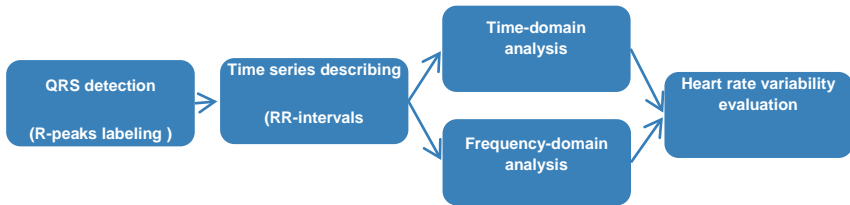


Fig. 46.8 – The general stages of heart rate variability evaluation process

After the pre-processing, variable threshold method can be used to further detect the R-peak. The formula for variable threshold value is defined as follows.

$$V_{TN} = [x(n) - x(n-1)] \cdot 70\% \quad (46.6)$$

The threshold makes it possible to differentiate R peak from the baseline, which is corresponding to 70% of ECG peak data detection. We were able to find QRS complex based on the detected R-peak. Detection of QRS complex is particularly important in ECG signal processing. In our system, we used a robust real-time QRS detection algorithm [30]. This algorithm reliably detects QRS complexes using slope, amplitude, and other information. The information obtained from QRS detection, temporal information of each beat and QRS morphology information can be further used for the other ECG parameter detection. In order to detect QRS complex, the signal is initially passed through a band-pass filter. It is composed of cascaded high-pass and low-pass filters. Subsequent processes are five-point derivative (Eq. 46.7), square (Eq. 46.8), moving window integrator (Eq.46.9), and detection.

$$y(nT) = \frac{2x(nT) + x(nT - T) - x(nT - 3T) - 2x(nT - 4T)}{8} \quad (46.7)$$

$$y(nT) = [x(nT)]^2 \quad (46.8)$$

$$y(nT) = \frac{1}{N} [x(nT - (N - 1)T) + x(nT - (N - 2)T) + \dots + x(nT)] \quad (46.9)$$

The instantaneous heart rate computed directly from R-R interval. In clinical settings, heart rate is measured in beats per minute (bpm). So the formula for determining heart rate from RR interval is given below (Eq. 46.10).

$$Heart_rate = \frac{60,000}{RRInterval(ms)} \quad (46.10)$$

46.3.3 Data analysis and prediction techniques

In the presence of multiple, incomplete, uncertain, or redundant data, the use of elements of the Dempster-Shafer (D-S) theory can improve the efficiency of data classification.

The technique to classifying real-time data from several sources involves the following eight steps: (1) Data normalization; (2) Prediction future points; (3) Analysis of residuals; (4) Probability calculation; (5) Check for conflicts; (6) Data fusion using different D-S techniques; (7) Classification; (8) Estimation of classification accuracy as follows in Fig. 46.9.

Consider a real-time classification model using a combined multi-criteria probability estimate for classifying a person's biophysical state. The methodology of the experiment consists of a sequence of six stages of processing the monitoring data of the human biophysical state obtained in real time. Since the monitoring data of the biophysical state of a person are usually characterized by different parameters, measured in unequal units at the first stage, the data are normalized using the Euclidean distance.

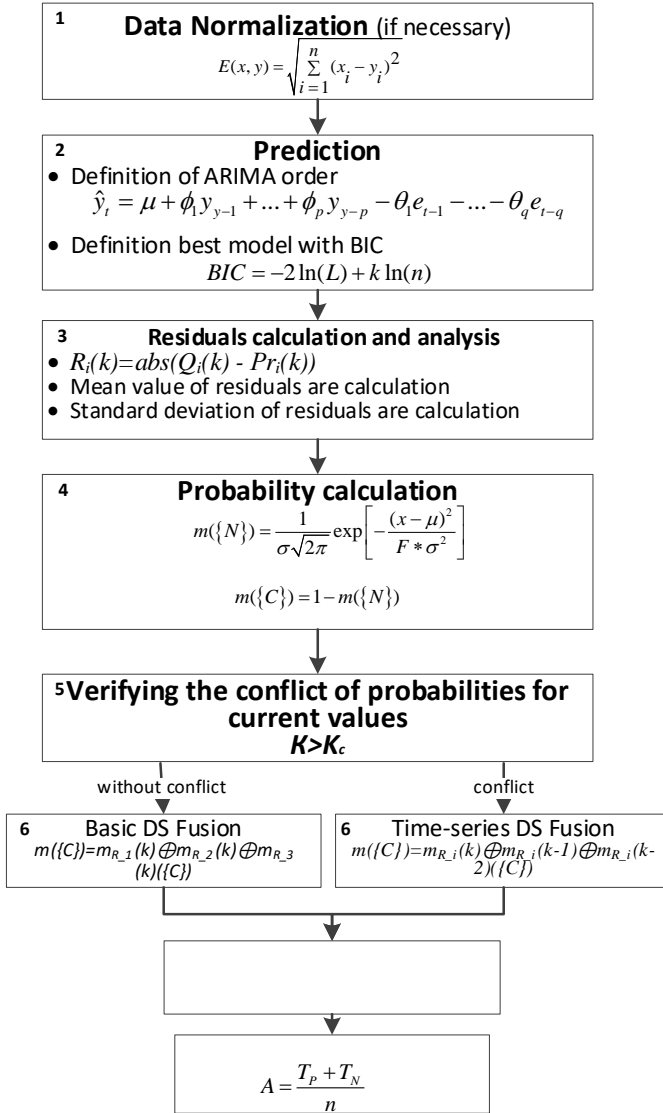


Fig. 46.9 – Technique to classifying real-time data from several sources

At the next stage, the monitoring data of the human biophysical state are analyzed using the ARIMA model, which allows one to perform exponential smoothing, a one-dimensional autoregressive

integrated moving average for the time series and to obtain a forecast of the data. To assess the quality of the ARIMA model, the Bayesian Information Criterion (BIC) was used in the work to predict the biophysical state of a person. The model with the minimum BIC value was chosen as the optimal model. The predicted values obtained are used to calculate the residuals, which are the basis for the further merging of data. Residual variables are used as sources of evidence for using the method of D-S fusion, which results in the likelihood of a person's biophysical state.

The calculation of the base probability assignment (BPA) is carried out using residues of the variables of the human biophysical state. Next, we check conflicts of probabilities of variables. If there is no conflict to determine the probability of fusion the variables of the human biophysical state, the basic method of D-S fusion is implemented. Otherwise, the proposed use of the method of D-S fusion for time series combines successive time steps and the weighted average method. At the next stage, based on the obtained estimates of the probability of fusion variables, data is classified using expert estimate to distinguish classes of states.

Step 1: Data Normalization

Normalization of parameter values is carried out using transformations of simple Euclidean distance, since, in general case, various indicators of the human biophysical state are expressed in unequal units. The Euclidean distance E between x and y point in n -dimensional space is calculated as:

$$E(x, y) = \sqrt{\sum_{i=1}^n (x_i - y_i)^2} \quad (46.11)$$

Step 2: Prediction Future Points

This step is performed using the Autoregressive Integrated Moving Average (ARIMA) model. Stationary series delays in the prediction equation are called “autoregressive” terms, lags from predictable errors are called “moving averages”, and the time series, which must be different to be stationary, is considered an “integrated” version of the stationary series. Random walk and random trend models, autoregressive models and exponential smoothing models are all special cases of ARIMA models.

The non-seasonal ARIMA model is classified as an ARIMA model (p, d, q) , where:

p is the number of autoregressive terms,

d is the number of non-seasonal differences required for stationarity,

q is the number of lagging predicted errors in the prediction equation.

The predicted value of $Y = \text{constant}$ and / or weighted sum of one or several last Y values and / or weighted sum of one or several last error values.

The prediction equation is constructed as follows. Let d denote the difference Y , then:

If $d = 0$: $y_t = Y_t$

If $d = 1$: $y_t = Y_t - Y_{t-1}$

If $d = 2$: $y_t = (Y_t - Y_{t-1}) - (Y_{t-1} - Y_{t-2}) = Y_t - 2Y_{t-1} + Y_{t-2}$

ARIMA estimates exponential smoothing, one-dimensional autoregressive integrated moving average for the time series data prediction.

The prediction equation is as follows.

$$\hat{y}_t = \mu + \phi_1 y_{y-1} + \dots + \phi_p y_{y-p} - \theta_1 e_{t-1} - \dots - \theta_q e_{t-q} \quad (46.12)$$

were, the moving average parameters (θ 's) are determined so that their signs are negative in the equation, following the agreement entered by Box and Jenkins.

The Bayesian Information Criterion (BIC) was used to assess the quality of the ARIMA model for predicting the biophysical state of a person. Bayesian information criterion (BIC, sometimes Schwarz Criterion) is a criterion for selecting a model from a class of parameterized models depending on a different number of parameters. For model estimation, the method of finding the maximum likelihood function is usually used, the value of which can be increased by adding additional parameters.

The Bayesian criterion is obtained under the assumption that the distribution of the sample belongs to the family of exponential distributions.

Let be $X = \{x_i\}_{i=1}^n$ - the observed part of the sample, where each object is characterized by the set of parameters $x_i=(x_{i1}, \dots, x_{i2})$, and L - is the maximum value of the likelihood function of the observed sample with a known number of parameters. Then the Bayes information criterion is determined as follows:

$$BIC = 2 \ln(L) + k \ln(n). \quad (46.13)$$

Then using the Bayesian criterion for the ARIMA model with SSE (Sum of Squared Errors) - the sum of squares of residues determined as follows

$$BIC = -2 \ln(L) + k \ln(n). \quad (46.14)$$

In this case, the shifted estimate of the variance of the regression residuals is logarithmized.

The model with the minimum BIC value is selected as the optimal model. This completes the stage of training the ARIMA model.

Step 3: Analysis of Residuals

Monitoring the status of n patient's indicators occurs in real time. Their measured values at time step k are defined as $Q_i(k)$, $i = 1, 2, \dots, n$. While $Pr_i(k)$ value means their predicted values obtained using the ARIMA model and the last measured values. Residuals are computed by $R_i(k) = \text{abs}(Q_i(k) - Pr_i(k))$ and $R_1(k)$, $R_2(k)$, $R_3(k)$ are rated as three biggest residuals corresponding to the three studied indicators of the human biophysical state. The residuals of the three indicators are used as the sources of evidence for the DS fusion method, and the result of the fusion is the probability of an initial or opposite biophysical state of a person.

Step 4: Calculation of Base Probability Assignment and Conflict Resolution

The calculation of basic probability assignment (BPA) is performed using the residuals. The BPA function of a person's normal biophysical state can be determined as follows.

$$m(\{N\}) = \frac{1}{\sigma\sqrt{2\pi}} \exp\left[-\frac{(x-\mu)^2}{F * \sigma^2}\right], \tag{46.15}$$

where x denotes the remainder of the indicator at a given timestamp; F is a constant; μ is the average value of the remainder of the indicator of the biophysical state of a person; σ is the standard deviation of the remainder indicator of the human biophysical state.

In the case of a binary classification, the probability of the opposite state

$$m(\{C\}) = 1 - m(\{N\}) \tag{46.16}$$

Step 5: Check for Conflict of Probabilities

At this stage, data are checked in the presence of conflicts in probabilities. If there is no conflict the base D-S data fusion technique can be used. Otherwise, we propose to utilize the D-S fusion method for time series which combines successive time steps and the weighted average.

Step 6: Data Fusion Using D-S Approach

Basic D-S fusion

The implementation of the basic D-S fusion method for $n > 2$ involves equations (7)-(9). For m_1, m_2, \dots, m_n n independent sets of BPA, the combinatorial probability fusion rule is defined as follows:

$$m(C) = m_1 \oplus m_2 \oplus \dots \oplus m_n(C) = \begin{cases} 0, & C = \Phi \\ \frac{1}{1-K} \sum_{C_i \subseteq C} \prod_{1 \leq i \leq n} m_i(C_i), & C \neq \Phi \end{cases} \tag{46.17}$$

where $K \in (0,1)$ is a coefficient of normalization that can be considered as a measure of conflict between two sets of evidence. The higher the value of K , the greater the conflict between the two proofs regarding the event of interest (in our case, the opposite biophysical state of a person). A comparison of the probability K coefficient of evidence with K_c coefficient of consistency of evidence is used to determine whether

the evidence is in conflict or not. The K coefficient is determined as follows.

$$K = \sum_{\cap_i C_i = \Phi} \prod_{1 \leq i \leq n} m_i(C_i) \tag{46.18}$$

And K_c the coefficient of the evidence consistency is determined as

$$K_c = \sum_{\cap_i C_i \neq \Phi} \prod_{1 \leq i \leq n} m_i(C_i) \tag{46.19}$$

Time-series D-S fusion

If there is a conflict, the calculation is carried out using successive time steps k and the weighted average method. For the merging via weighted average, the base probability m_i from equations (46.17) - (46.19) is converted to m_i^*

$$m_i^* = Crd \times m_i, i=1, 2, \dots, n. \tag{46.20}$$

In this case, the multi-criteria combinatorial rule is determined as

$$m(C) = m_1 \oplus m_2 \oplus \dots \oplus m_n(C) = \begin{cases} 0, & C = \Phi \\ \frac{1}{1-K^*} \sum_{\cap_i C_i = C} \prod_{1 \leq i \leq n} m_i^*(C_i), & C \neq \Phi \end{cases} \tag{46.21}$$

where coefficient K^*

$$K^* = \sum_{\cap_i C_i = \Phi} \prod_{1 \leq i \leq n} m_i^*(C_i) \tag{46.22}$$

Suppose that a probability of an opposite state is $m_{(k)} \oplus m_{k-1}(\{C\})$, where k, k-1 are the current and previous time steps respectively. And this event occurred. In this case, the final result of a multi-criteria fusion is calculated using the basic fusion equations (46.17) - (46.19) at the nearest time steps k, k-1, k-2. If the residues from the three sensitive parameters do not conflict with each other, the basic D-S fusion method is used. Otherwise, an additional test is introduced, which can be expressed as follows:

$$\begin{aligned} & m_{Ri}(k) \oplus m_{Ri}(k-1)(\{C\}) > P \text{ and } m_{Ri}(k-1) \oplus m_{Ri}(k-2)(\{C\}) > P \\ & \text{and } m_{Ri}(k-2) \oplus m_{Ri}(k-3)(\{C\}) > P, \end{aligned} \tag{46.23}$$

where $m_{R_i}(k-j)$ denotes the probability assigned i -th residual, the biggest one from the three maximal residuals on the time step $k-j$, $j = 0, 1, 2$. P is the constant threshold used to compare the results of a fusion between two adjacent fragments of a particular human biophysical state and represents consistency of evidence.

Usually, a constant threshold value is assumed to be 0.8; 0.9. If there is a sensitive parameter i that satisfies the above inequalities (46.23), then the following equation computed using the D-S fusion method is the probability of an opposite biophysical state:

$$m_{R_i}(k) \oplus m_{R_i}(k-1) \oplus m_{R_i}(k-2) \{C\} \quad (46.24)$$

If (46.23) is not met, a weighted average approach based on equations (46.21) and (46.23) are used to D-S fusion and obtaining the probability of the final event.

Step 7: Classification

For model training, the Random Forest algorithm and 5-fold cross-validation are used. When using 5-fold cross-validation, the data set is randomly divided into five sub-sets of approximately equal size. When running data from one sub-set, it is used as a test sample, and the data from the other four sub-sets are used as a training sample.

Random Forest is a classifier consisting of a set of tree-classifiers $\{h(x, \Theta_k), k = 1, \dots\}$, $\Theta_k \in \{\Theta_k\}$ are independent equally distributed random vectors, and each tree gives its voice for the most popular class for vector of input values x .

For a set of tree-classifiers $h_1(x), h_2(x), \dots, h_k(x)$ and random vectors of input values x and output value y the margin function is defined as follows

$$mg(x, y) = av_k \mathbf{1}(h_k(x) = y) - \max_{j \neq y} av_k \mathbf{1}(h_k(x) = j), \quad (46.25)$$

where $\mathbf{1}$ – indicator function, av – the average number of votes in x, y , in the determined class, the average number of votes exceeds the average number of any other class.

The result of the merger is the probability of a finite event to obtain the general normal and abnormal values of the probability function. For this data element, if the probability value of the

anomalous hypothesis is greater than the value of the normal hypothesis, then this element is classified as an abnormal state of the patient, otherwise it is classified as the normal state of the patient.

Step 8: Estimation of Classification Accuracy

The classification quality is calculated by the formula (46.26) as follows.

$$A = (T_p + T_N) / n, \quad (46.26)$$

where T_p is the number of observations with a true positive result, T_N is the number of observations with a true negative result, n is the total number of data elements.

46.3.4 Cases

The experiment was conducted using the EEG data set available in the free access to the UCI Machine Learning Repository [31]. The probability of the state of a person's closed eyes is determined on the basis of the probabilities of the combined probabilities of these EEG electrodes based on the method of D-S data fusion. Based on the obtained value of the probability of the state of closed eyes of a person, the classification was carried out using the Random Forest algorithm. Classification quality was assessed using a classification accuracy indicator.

Data description

EEG Eye State Data Set was described by [32]. The data set consists of 14 EEG values obtained from 14 electrodes, and values indicating the state of the eyes. All data is taken from one continuous EEG measurement using the Emotiv EEG Neuroheadset. The measurement duration was 117 seconds. The eye condition was detected by the camera during the EEG measurement and added later manually to the file after analyzing the video frames. The data set contains 14980 data elements, of which 6723 are with eyes closed (anomalous data), and 8257 of them are with eyes open (normal data). The data set consists of 14977 copies with 15 attributes each (14 attributes representing the values of the electrodes and the state of the eyes). Instances are stored in the case in chronological order in order to be able to analyze temporal dependencies. 8255 (55.12%) copies of the

data set correspond to the open eye and 6722 (44.88%) copies of the closed eye. Table 46.1 shows the ranges of 14 electrodes in the data set.

Table 46.1 – Minimum, maximum and average values of 14 electrodes for the state of open and closed eyes

Eye State	Closed			Open		
	min	mean	max	min	mean	max
AF3	4198	4305	4445	1030	4297	4504
F7	3905	4005	4138	3924	4013	7804
F3	4212	4265	4367	4197	4263	5762
FC5	4058	4121	4214	2453	4123	4250
T7	4309	4341	4435	2089	4341	4463
P7	4574	4618	4708	2768	4620	4756
O1	4026	4073	4167	3581	4071	4178
O2	4567	4616	4695	4567	4615	7264
P8	4147	4202	4287	4152	4200	4586
T8	4174	4233	4323	4152	4229	6674
FC6	4130	4204	4319	4100	4200	5170
F4	4225	4281	4368	4201	4277	7002
F8	4510	4610	4811	86	4601	4833
AF4	4246	4367	4552	1366	4356	4573

There is a clear difference in the amplitude of some sensors when comparing the range of values for different eye conditions. On the one hand, for the F7, F3, O2, P8, T8, FC6 and F4 sensors, the maximum values for the open state of the eye are higher than the maximum closed eye values, while the minimum values are almost the same, on the other hand, for AF3, FC5, T7 sensors, P7, O1, F8 and AF4 the minimum values for the open state of the eyes are lower than for the closed eye, while the maximum values are about the same.

The data of all sensors have a common property, which is that the open state of the eyes has a higher range of values than the closed state of the eye, while the average value remains almost the same. Accordingly, the standard deviation also increases.

The closed state of the eyes is taken as opposite to the open one and has a class value of “1”, the open state of the eyes is taken as normal and has a class value of “0”.

All values are presented in chronological order, starting with the first measured value at the top of the data. The 14 variable signals (AF3, F7, F3, FC5, T7, P7, O1, O2, P8, T8, FC6, F4, F8, AF4) are of numeric type. There are no missing values in the set. In Figure 46.10 shows the time series of the first 250 copies of the 14 electrodes of the EEG signal, which include data with eyes closed and open.

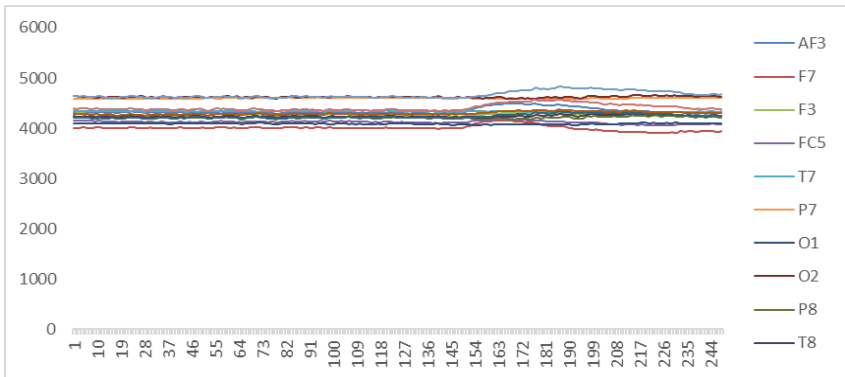


Fig. 46.10 – Time series of the first 250 copies of 14 electrodes of the EEG signal

Data Analysis

The data normalization stage is not used in this case. For the studied data there is no need to carry out normalization, since The data are presented by different sources (electrodes), but have the same scale of measurement.

At the stage of forecasting, data on the electrodes is predicted using the ARIMA model.

Table 46.2 shows the dependences between the order of the ARIMA model (p , d , q), where p is the autoregression, d is the integration of the time series, q is the moving average, and the average BIC for all variables.

The experiment on the choice of the optimal model is limited by the second order of autoregression and the moving average, and the zero order of integration of the time series.

Table 46.2 – Dependence between the order of the ARIMA model and the BIC value

(p, d, q)	mean BIC
(0, 0, 0)	4,6
(1, 0, 0)	3,77
(2, 0, 0)	3,67
(1,0,1)	3,14
(1,0,2)	3,00
(2,0,1)	3,15
(2,0,2)	3,15

Analysis of the table data showed that the optimal ARIMA model is a model order (1, 0, 2), which is selected based on the minimum average BIC values. Prediction is made. An example of graphs of real data of the AF3, F7 electrode and the obtained values predicted using the optimal ARIMA model - AF3 pr, F7 for the first 250 copies are presented in Fig.46.11, 46.12.

Some data values of one electrode do not indicate a probable state of a person, i.e. closing eyes.

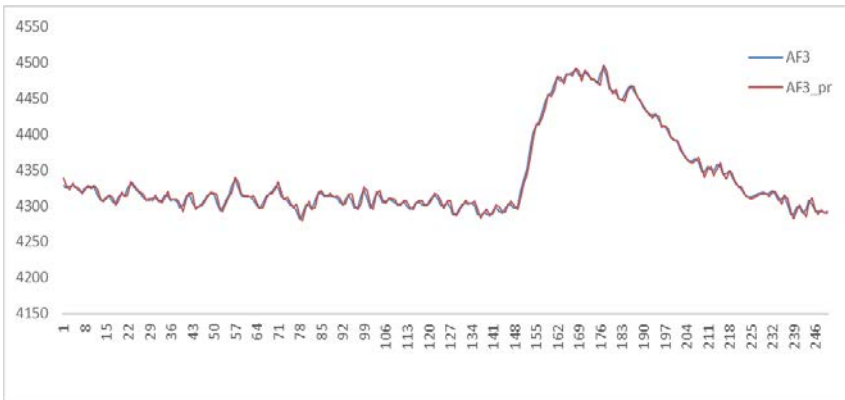


Fig. 46.11 – Graphs of real and predicted values of the signal of the electrode AF3

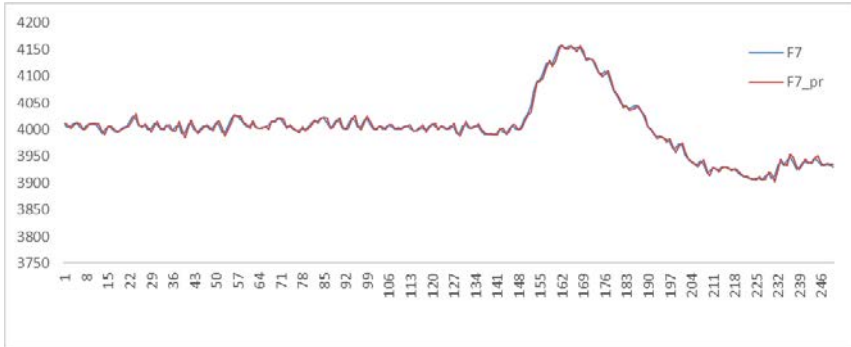


Fig. 46.12 – Graphs of real and predicted values of the signal of the electrode F7

Therefore, a separate prediction of the states of each analyzed signal of an individual EEG electrode is not able to predict the closure of the eyes. Also, it is necessary to take into account the conflict of parameter values when the forecast is carried out in conditions of the “normal” state of the signal of one electrode and the “closed” state of another electrode. Multi-criteria data fusion to predict the physical process of closing the eyes is an alternative to improving the accuracy of predicting human biophysical states.

The merging of data in the theory of evidence D-S requires the definition of the structure of recognition of the state of the eyes. This structure can be defined as $\Omega = \{N = \text{“normal”}, C = \text{“close”}\}$, $N \cap C = \Omega$.

The function of the base probability assignment (BPA) of the value of $m(0, 1)$ can be determined as follows: $m(0, 1)$ can be defined as: $m(\Phi) = 0$, $m(\{N\}) + m(\{C\}) + m(\{N, C\}) = 1$. $m(\{N\})$ means trust assigned to the “normal” state of a certain EEG electrode, taking evidence into account. $m(\{C\})$ means trust assigned to a closed state by a specific EEG electrode taking into account the proof. $m(\{N, C\})$ means that the evidence cannot maintain the “normal” or “closed” state of the eyes, that is, the trust assigned to the unknown state of the eyes. In our study, $m(\{N, C\})$ is accepted about 0. The confidence in any eye condition, or $m(\{S\})$, is in the range from 0 to 1. To estimate the value of $m(\{C\})$, the function of the object probability distribution is used.

Using the combined rules of the theory of evidence D-S, the probabilistic merger $m_1 \oplus m_2 \oplus \dots \oplus m_n(\{C\})$ allows determining the

occurrence of a closed eye state, using different sources of evidence, as the probability of its occurrence (0, 1).

Different sources of evidence may contradict each other and such states should be resolved to achieve lasting confidence in a closed eye based on data from EEG electrodes.

At the next stage, the remains of each signal of the EEG electrode are obtained and analyzed. In fig. 46.13, 46.14 the example of the curves of the residuals of these signals of the electrodes AF3, F7 for the first 250 copies is presented. Residual curves make it possible to isolate anomalous deviations of values after prediction, while random changes will be attenuated.

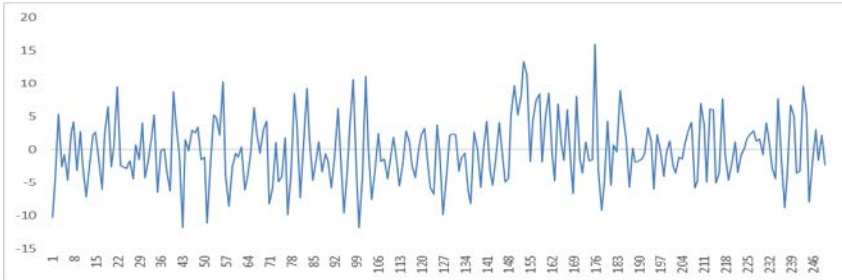


Fig. 46.13 – Residual Electrode Data AF3

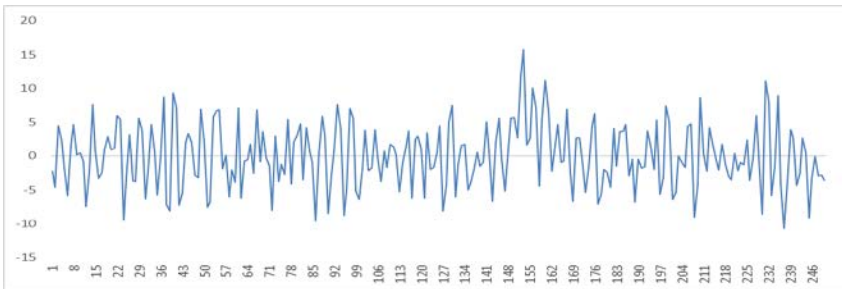


Fig. 46.14 – Residual Electrode Data F7

The calculation of the base probability distribution (BPA) by the formula (46.15) has been carried out. The probability of the closed state of the eyes is determined using expression (46.16). The F coefficient in this study is assumed to be 2.

Graphs for estimating the probability of the closed state of eyes $m(\{C\})$ with the studied values of the signal of electrodes AF3, F7, F3 for the first 250 copies are presented in Fig. 46.15.

At the next stage, the probabilities of these electrodes were merged. For the presented estimates of the probabilities of each parameter, the conflict between them is checked separately. In the absence of a conflict of probabilities of data residues, Basic D-S fusion is used, which is calculated by the formula (46.17). The coefficient K is determined using expression (46.18), and the coefficient of consistency of evidence using formula (46.19).

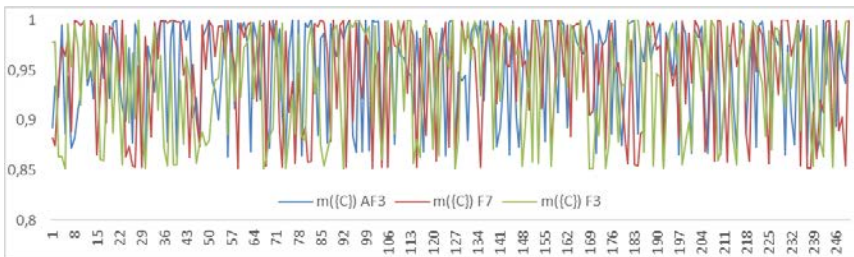


Fig. 46.15 – Graphs for estimating the probability of the closed state of the eyes with the studied values of the signal of electrodes AF3, F7, F3

In Figure 46.14 it can be seen that the data of the AF3 electrode shows a low probability of closed eyes at step 144, which causes an assumption about open eyes. Suppose that the eyes are in fact in the closed state, so the other data of the signals of the electrodes remain stable. The resolution of the contradiction between the data of the electrode AF3 and the electrodes F7, F3 is analyzed. For step 144, the probabilities of the studied data are defined as follows:

$$m_{AF3}(\{C\}) = 0,86; m_{AF3}(\{N\}) = 0,14.$$

$$m_{F7}(\{C\}) = 0,95; m_{F7}(\{N\}) = 0,05.$$

$$m_{F3}(\{C\}) = 0,98; m_{F3}(\{N\}) = 0,02.$$

In the presence of a conflict of probabilities of residual data, Time-series D-S fusion is used. An additional test is introduced, which is calculated by the formula (46.23). And further, subject to the condition, a merger is carried out using expression (46.24).

The probability values of the electrode data AF3 and electrode F7 indicate a conflict of probabilities. The probabilities of the data of the electrode AF3 and electrode F3 also indicate a conflict of probabilities. Consider the next steps for the data of the AF3 electrode and the F7 electrode. Since the remnants conflict, we use the formula (46.23). A fragment of these probabilities of the state of closed eyes for calculating the probabilities is presented in Table 46.3. The threshold value of P is set to 0.9.

Table 46.3 – Fragment of the data of probabilities of the parameters of the critical state of the database system

Time Series	Probabilities of the condition of closed eyes for these electrodes	
	AF3	F7
141	0,892032	0,996966
142	0,939556	0,992565
143	0,987368	0,95673
144	0,865843	0,953394
145	0,998742	0,997956
146	0,904366	0,919334
147	0,87293	0,992776

We carry out a check of the fulfillment of the condition (46.23) for conflicting parameters. Below are examples of the verification of the fulfillment of the condition for the AF3 electrode with the highest probability AF3 at time step 144 with the threshold value set $P=0,9$.

AF3

$$0,86 \oplus 0,99 > 0,9 \text{ and}$$

$$0,99 \oplus 0,94 > 0,9 \text{ and}$$

$$0,94 \oplus 0,89 > 0,9$$

The condition is fulfilled and therefore it is possible to proceed to the determination of the probability of the state of open eyes using the D-S fusion method using (46.24). Calculate the coefficient K^* follows (46.22).

$$K^* = 0,86 \times 0,05 + 0,14 \times 0,95 = 0,043 + 0,133 = 0,176$$

$$1 - K^* = 0,824$$

$$m(\{N\}) = \frac{0,86 \times 0,95}{0,824} = 0,29,$$

$$m(\{C\}) = \frac{0,14 \times 0,05}{0,824} = 0,008.$$

From the calculations, it can be concluded that the probability of the state of open eyes at step 144 in the face of the conflict of these two EEG electrodes = 0.29.

At the next stage, we classify the data using the obtained probability of the state of the eyes. Solving this problem implies the use of a two-class classification with the classes “normal” and “close”, which define the normal and closed state of the human eye. Teaching a model involves defining the state as open or closed eyes.

For training model, the Random Forest algorithm and 5-fold cross-validation are used.

Estimate A accuracy rating is used to assess the quality of results. It is calculated as follows.

$$A = \frac{7900 + 6068}{14980} = 0,93$$

46.4 Work related analysis

In the preparation of this part, the information from our partner universities was used. The core collection of related courses from EU universities includes but not limited the following ones.

Our partners from University of Newcastle upon Tyne developed a several course that cover unique aspects of health application in IoT.

One of their courses EEE8064: “Biometrics and Recognition” [32] includes follow knowledge. Overview of biometrics: definitions, biometric modalities, basic applications, access control, security. biometric system architecture: scanning/digitizing, enhancement, feature extraction, classification, matching, searching and verification. probability, statistics and estimation. Random variables, discrete and

continuous distribution - pattern classification and recognition - signals in time and frequency domain – multivariate statistical analysis. Algorithms face recognition, voice recognition, fingerprint recognition, iris recognition. Other biometric modalities: retina, signature, hand geometry, gait, keystroke. Quantitative analysis on the biometrics. Performance evaluation in biometrics – false acceptance rate; false rejection rate. Multimodal biometric systems. Biometric system integration, multimodal biometric systems: theory and applications, performance evaluation of multimodal biometric systems. Biometric system security: biometric attacks/tampering; solutions; biometric encryption; cancellable biometrics.

The course EEE8092 “Internet of Things and Sensor Networks” focuses on a wireless sensor networks in IoT” [33]. The “Zigbee” 2.4GHz wireless communication standard is used, together with a PIC microcontroller architecture, to provide a very flexible platform for the development of wireless sensor networks.

The concept of real-time computing and an overview of popular embedded platforms is present on EEE8068 “Real Time Embedded Systems”[34]. Design metrics and Roadmap documents. Real-time schedulers, models, implementations, analysis. Hardware design methods for security applications resistant to side-channel attacks (SPA, DPA). Coursework – design and analysis of a real-time application.

Another one is EEE8085 “M2M Technology Internet of Things”[35] includes follow topics. Interfaces of sensors/actuators and their connectors to the IoT router; internet interfaces for IoT routers, their representation in OSI reference model; IoT router architecture, framework and framework connectors; architectures, platforms and applications for M2M IoT systems; coursework: design of a simple M2M IoT system, physical implementation, experimentation, analysis and report.

Related courses from Royal Institute of Technology focuses on medical aspects of information technology: HL1016 “Medical Measurement and Monitoring” [36].

The University of Coimbra proposed course “Medical Informatics” [37]. The course includes basic concepts in medical informatics, standards for clinical information representation and transmission,

electronic patient record, services and technologies for telemedicine, clinical information analysis algorithms for clinical decision support.

Questions

1. What classification of sensors does you familiar with?
2. The difference between physiological sensors and wearable activity sensors.
3. What are the key parameters of biomedical sensors?
4. The main stages of designing a person's ECG signal monitoring system.
5. What challenges arise from the analysis of medical data?
6. Are biomedical signals discrete or continuous?
7. What are the main requirements for analytics of integrated biomedical data?
8. How aggregated time series can be defined?
9. What is temporal correlation?
10. In trend analysis, an observed time series can be decomposed into three components. List them.
11. The scope of an applications based on wearable biomedical sensor.
12. List area of application for embedded and wearable IoT-based systems.
13. What is WBAN?
14. What a wearable ECG device is responsible for?
15. How QRS complex can be identified?
16. List the main steps to classifying real-time data from several sources.
17. How to calculate base probability assignment?
18. How to estimate classification accuracy?

References

1. C. Bhatt, N. Dey, A. S. Ashour (eds.) "Internet of Things and Big Data Technologies for Next Generation Healthcare-Springer", 2017.
2. G. Zhou, Y. Wang, L. Cui, "Biomedical sensor, device and measurement systems", *Advances in Bioengineering*. 2015.
3. D. Terrance and M. McGrath. "Wireless sensor networks for healthcare applications", *Artech House*, 2010.

4. C. K. Reddy, C.C. Aggrawal Chapman and Hall/CRC, "Healthcare Data Analytics", 2015.
5. M. Xiao, Z. Wang, S. Zhou, H. Wen and Y. Zhang. "Intelligent healthcare systems assisted by data analytics and mobile computing", *Wireless Communications and Mobile Computing*, January 2018.
6. D.H. Lee, A. Rabbi, J. Choi and R. Fazel-Rezai, "Development of a mobile phone based e-health monitoring application", *Development*, vol. 3(3), 2012.
7. Z. Yang, Q. Zhou, L. Lei, K. Zheng, W. Xiang, "An IoT-cloud Based Wearable ECG Monitoring System for Smart Healthcare". *Journal of Medical Systems*, vol. 40(12), October 2016.
8. Y. Tao, B. T. Ren, "Improvement of evidence compound rule based on partial conflict allocation strategies", *Comput. Eng.*38268–70, 2012.
9. L. Fan and L. Xiong, "An adaptive approach to real-time aggregate monitoring with differential privacy", *IEEE Transactions on knowledge and data engineering*, vol. 26(9), pp.2094-2106, May 2014.
10. N. Jiang, G. Jiang, H. Chen, K. Yoshihira, "Correlating real-time monitoring data for mobile network management", *In World of Wireless, Mobile and Multimedia Networks*, June 2008.
11. M. Arsalan, "Addressing Security and Privacy Challenges in Internet of Things", arXiv preprint arXiv:1807.06724, 2018.
12. W. Y. Wong and M. S. Wong, "Smart garment for trunk posture monitoring", *A preliminary study, Scoliosis and Spinal Disorders*, vol. 3, no. 1, p. 1, 2008.
13. A. Crane, S. Doppalapudi, J. O'Leary, P. Ozarek, and C. Wagner, "Wearable posture detection system", *Annual Northeast Bioengineering Conference*, pp. 1–2, 2014.
14. E. Sardini, M. Serpelloni, and M. Ometto, "Smart vest for posture monitoring in rehabilitation exercises", *IEEE Sensors Applications Symposium*, pp. 1–5, 2012.
15. H. Harms, O. Amft, G. Troster, M. Appert, R. M'uller, and A. Meyer-Heim, "Wearable therapist: Sensing garments for supporting children improve posture", *ACM Int. Conf. Ubiquitous Computing*, pp. 85–88, March 2009.
16. A. K. Dey, D. Salber, G. D. Abowd, and M. Futakawa, "The conference assistant: Combining context-awareness with wearable computing", *IEEE Int. Symp. Wearable Computers*, pp. 21–28, 1999.
17. E. Keyes, M. P. Johnson, and T. Starner, "Magnetometer-based gesture sensing with a wearable device", 2015.
18. X. Li, B. Hu, J. Shen, T. Xu, and M. Retcliffe, "Mild depression detection of college students: An EEG-based solution with free viewing tasks", *J. Medical Systems*, vol. 39, no. 12, pp. 1–6, 2015.

19. T. O. Meservy, M. L. Jensen, J. Kruse, J. K. Burgoon, J. F. Nunamaker, D. P. Twitchell, G. Tsechpenakis, and D. N. Metaxas, "Deception detection through automatic, unobtrusive analysis of nonverbal behavior", *IEEE Intelligent Systems*, vol. 20, no. 5, pp. 36–43, September-October 2005.

20. P. S. Teh, A. B. J. Teoh, and S. Yue, "A survey of keystroke dynamics biometrics", *The Scientific World Journal*, August 2013.

21. A. Mosenia, S. Sur-Kolay, A. Raghunathan, N. K. Jha, "Wearable medical sensor-based system design: A survey". *IEEE Transactions on Multi-Scale Computing Systems*, vol. 3(2), pp.124-138, 2017.

22. Slideshare.net. (2019). "Dynamic Data Analytics for the Internet of Things: Challenges and Opp...." [online] Available at: <https://www.slideshare.net/PayamBarnaghi/dynamic-data-analytics-for-the-internet-of-things-challenges-and-opportunities/8> [Accessed 17 Jan. 2019]

23. Y. K. Kim, H. Wang, M. S. Mahmud, "Wearable body sensor network for health care applications", *Smart Textiles and Their Applications*, pp. 161–184, 2016.

24. P. Botano, D. Rossi D, "IEEE EMBS technical committee on wearable biomedical sensors & systems: position paper", *Proceedings of the international workshop on wearable and implantable body sensor networks*, 2006.

25. S. Pooranchandra and N. Kumaravel, "A novel method for elimination of power line frequency in ECG signal using hyper shrinkage function", *Digital Signal Processing*, Vol. 18, No. 2, pp.116-126, March 2008.

26. A. K. Ziarani and A. Konard, "A nonlinear adaptive method of elimination of power line interference in ECG signals", *IEEE Trans. Biomed*, Juny 2002.

27. G. Mihov, I. Dotsinsky, and T. Georgieva, "Subtraction procedure for powerline interference removing from ECG: improvement for nonmultiple sampling", *Journal of Medical Engineering & Technology*, Vol. 29, No. 5, pp.238-243, September-October 2005.

28. J. Pan, & W. J. Tompkins, "A real-time QRS detection algorithm", *IEEE Transactions on Biomedical Engineering*, Vol. 32, No. 3, pp.230-236, March 1985.

29. D. P. Coutinho, A. L. N. Fred, and M. A. T. Figueiredo, "One-lead ECG based personal identification using Ziv-Merhav cross parsing", *20th International Conference on Pattern Recognition*, pp. 3858-3861, August 2010.

30. Archive.ics.uci.edu. (2019). "UCI Machine Learning Repository: EEG Eye State Data Set". [online] Available at: <https://archive.ics.uci.edu/ml/datasets/EEG+Eye+State> [Accessed 17 Jan. 2019]

31. Rösler, O. and Suendermann, D., "A first step towards eye state prediction using eeg", *Proc. of the AIHLS*, 2013.
32. "Biometrics and Recognition Postgraduate - Newcastle University", *Ncl.ac.uk*, 2019. [Online]. Available: <https://www.ncl.ac.uk/postgraduate/modules/EEE8064/> [Accessed: 20- Feb- 2019].
33. "Internet of Things and Sensor Networks- Postgraduate - Newcastle University", *Ncl.ac.uk*, 2019. [Online]. Available: <https://www.ncl.ac.uk/postgraduate/modules/EEE8092/> [Accessed: 20- Feb- 2019].
34. "Real Time Embedded Systems - Postgraduate - Newcastle University", *Ncl.ac.uk*, 2019. [Online]. Available: <https://www.ncl.ac.uk/postgraduate/modules/EEE8068/> [Accessed: 20- Feb- 2019].
35. "M2M Technology Internet of Things - Postgraduate - Newcastle University", *Ncl.ac.uk*, 2019. [Online]. Available: <https://www.ncl.ac.uk/postgraduate/modules/EEE8085/> [Accessed: 20- Feb- 2019].
36. "HL1016 Medical Measurement and Monitoring", *Kth.se*, 2019. [Online]. Available: <https://www.kth.se/student/kurs/kurs/HL1016?l=en> [Accessed: 20- Feb- 2019].
37. "Medical Informatics", *Apps.us.pt.*, 2018 [Online]. Available: <https://apps.uc.pt/courses/EN/unit/9791/15102/2017-2018?type=ram&id=5041>. [Accessed: 20- Feb- 2019].
HL1016 "Medical Measurement and Monitoring"

47. DEVICES WITH RECONFIGURABLE ARCHITECTURE FOR BIOMEDICAL IOT BASED APPLICATIONS

Prof., DrS I. S. Skarga-Bandurova,
Assoc. Prof., Dr. T.O. Biloborodova (V. Dahl EUNU)

Contents

47.1 A Personal Mobile Sensing System for Motor Symptoms Assessment of Parkinson's Disease.....	578
47.2 Medical Aspect	578
47.3 Sensors and devices for Parkinson's disease assessment	579
47.4 System Architecture.....	582
47.5 Basic system components utilized and launched on the smartphone.....	583
47.6 A mobile application of the personal health monitoring system	585
47.7 Cloud infrastructure	585
47.8 Implementation and Results.....	587
47.9 Work related analysis.....	592
Conclusions and questions	593
References.....	594

Abbreviations

ANOVA – Analysis of Variance
E – Energy
Gb – Gigabit
HTTP – Hyper Text Transfer Protocol
JSON – Java Script Object Notation
M – Mean
MB – Mbyte
PC – Pearson Correlation
RAM – Random Access Memory
SD – Standard deviation
SoC – system on a chip
TS – Time Step

47.1 A Personal Mobile Sensing System for Motor Symptoms Assessment of Parkinson's Disease

Monitoring of certain physiological parameters allows tracking the disease's symptoms at an early stage. It helps to take timely measures to prolong the early stage and maintain the quality of life.

Long-term monitoring at home can be useful for obtaining an objective assessment of health state and identifying changes according to Parkinson disease that cannot be observed in the clinic. However, the main inconvenience in the long-term recording is a large amount of the generated data. Analysis and processing of these data can take a whole lot of the time [2].

The further development of information technology provides new opportunities in biomedical monitoring. A wide variety of biomedical sensors is used to obtain various physiological signals from patients [3]. Processing and analysis of these signals to monitor the health status can be performed via personal mobile devices or cloud storage.

47.2 Medical Aspect

According to WHO [1] the prevalence and “rejuvenation” of such neurodegenerative diseases such as Parkinson’s disease, has noted. This disease is asymptomatic for a long time. The brain areas, which control the motor function, destruct. Early diagnosis makes it possible to fix the **patient’s** condition in the primary stages and prevent severe cognitive disorders.

Parkinson’s disease is characterized by four main motor disorders: tremor, slowness of movement (bradykinesia), rigidity, and postural instability.

Muscular rigidity is a uniform increase in muscle tone. The limbs, while flexing and unbending, get into a certain position. Hypokinesia is the reduction of spontaneous motor activity. Dyskinesia and bradykinesia are varieties of spontaneous motor activity. Postural instability develops in the late stages of the disease. The patient has a loss of confidence and reduced mobility. Tremor is the most common symptom of movement disorder at the early stage of diseases. It is also the most obvious symptom, easy to detect, and includes coarse slow

tremor of the hand at rest which disappears during voluntary movement, and other tremor types.

The physiological indicators of the health status can be used for early diagnosis and progression of Parkinson's disease. In this case, a personal sensing system based on the smartphone is a rich source of input data about the specific motor activity. From there, methods of data acquisition, pre-processing, transmission, as well as data mining techniques to determine the predictors of the pathological state according to Parkinson's disease, should be defined and implemented.

There are many researches done in this area, but the measures for determining, diagnosing and treating Parkinson's disease do not have enough complexity. The monitoring system should include sensors, devices for recording signals of physiological parameters of a person health, the data transmitting, processing and analyzing and main disease symptoms founding. Nowadays, designing the systems for monitoring the physiological parameters to determine symptoms of Parkinson's disease is relevant for profiling health care department.

47.3 Sensors and devices for Parkinson's disease assessment

The most common sensors and devices for Parkinson's disease assessment are accelerometer, electromyography, magnetic tracking system, gyroscope, digitization of the tablet; video, motion detection, and depth sensor are among the existing methods for measuring and analyzing.

Signals processed and analyzed using various methods for the assessment of the person health. They are wavelet transforms, principal component analysis, fast Fourier transforms, spectral analysis, methods of machine learning technique. Machine learning in assessing the symptoms of Parkinson's disease often includes methods for assessing the magnitude of the symptom in question.

Table 47.1 – Devices and techniques for assessment of the symptoms of Parkinson's disease

Symptoms	Devices	Measure Type	Data Analysis Technique
Tremor	Smartphone (3D accelerometer, timer, touchscreen) [4]	X, Y coordinates, time duration, 3D acceleration	Machine learning technique using Random forest
	Stylus [5]	Acceleration	Non-parametric methods
Rigidity	Wearable sensor [6]	Acceleration	Spectral Analysis
	Goniometer [7]	Angular velocity	Spectral Analysis of vertical leg acceleration
	Stride monitor system [8]	Angular velocity	Extension-flexion-component analysis
	Isokinetic dynamometer Biodex System [9]	Angular velocity, anatomical zero	Spearman correlation
Dyskinesia	Digitized tablet with spirometry [10]	Velocity of drawing movements	Standard deviation analysis of drawing velocity
	Wrist accelerometer [11]	Acceleration, velocity	Machine learning technique using Support Vector Machine
	Wrist-worn inertial sensor [12]	Median angular velocity of rotation	Linear discriminant analysis
Postural instability	MTX Xsens sensor with accelerometer and gyroscope [13]	Acceleration, direction, distance	Antero-posterior, Medio-lateral, Vertical directions analysis

	Motion detector, depth sensor, Vicon, motion capture system and force plate [14]	Ground reaction force, the body center of mass, displacement, velocity	Segmentation, «zero-point-to-zero-point» integration
	Digital angular velocity transducer [15]	Body velocity, time	Linear discriminant analysis, ANOVA
	Accelerometer [16]	Acceleration	Posture contextualization algorithm
Tremor, dyskinesia	Accelerometer, IR-camera, gyroscope [17]	Acceleration, time, angular velocity	Genetic Algorithm spectral classification
Tremor, bradykinesia	Miniature uni-axial gyroscope [18]	Angular velocity in roll, yaw, and pitch direction	Spectral Analysis
Tremor, postural instability	Accelerometer [19]	Mean velocity, acceleration range, mean acceleration	Hilbert–Huang transformation of postural parameters
Bradykinesia, dyskinesia	Digitized tablet Pocket PC [20]	Radius, time, mean speed of correct the proportion of taps	Wavelet transform and principal component analysis
	Multichannel accelerometer, Video recorder [21]	Acceleration, body position, time, gravitational force, body segment angel	Direct current component, discriminant, variance (ANOVA), regression
	Accelerometer [22]	Time, wrist acceleration	Expert system
Rigidity, bradykinesia, dyskinesia	Digitized tablet with touchscreen and spirometry [23]	Speed, accuracy, a standard deviation of radial drawing velocity	Principal component analysis

The processes of monitoring, diagnosing, and treating Parkinson's disease include several issues. First of all, the monitoring system for the determination of signs, observation, and treatment of Parkinson's disease lacks complexity and mobility. Secondly, a set of alternative interpretations, the strong interconnection, and interdependence of specific parameters hobble the feature recognition for determining the symptoms of Parkinson's disease. Finally, diagnostics of Parkinson's disease symptoms, one often encounters the need for long-term objective monitoring of physiological parameters of the person. Given these issues, continuous monitoring for obtaining, processing, transmitting, and analyzing data of health status is essential. It makes it possible to get an accurate quantitative assessment without considering a subjective patient assessment of their state.

From this perspective, the current goal is developing an effective monitoring system for the assessment of neurodegenerative changes using tremor detection. The system can be used for determining the signs of Parkinson's disease. The main objectives are:

1) *analysis* of monitoring systems for symptoms of Parkinson's disease, including the analysis of sensors, devices, determination parameters and methods for analyzing the data obtained;

2) *research and analysis* of methods and hardware for detection the symptoms of Parkinson's disease

3) *development* of the architecture and functionality of the personal health monitoring system;

4) *development* of a mobile application for monitoring and obtaining physiological parameters of the personal health status;

5) *the development of approach* for data processing: data processing, data mining and checking of a health status.

The developed system can be used to assess the personal health status according to diagnosis, observation, treatment of Parkinson's disease.

47.4 System architecture

The personal mobile sensing system for monitoring and analysis signs of a Parkinson's disease utilizes the built-in sensors of the smartphone. More specifically, the built-in smartphone sensors are used to detect tremor. The development of the architecture and functional

scheme of the monitoring system, the development of a mobile application for monitoring and obtaining the person health state parameters are presented below.

The overall system architecture encloses three layers and represents the most straightforward system based on IoT, as shown in Figure 47.1.

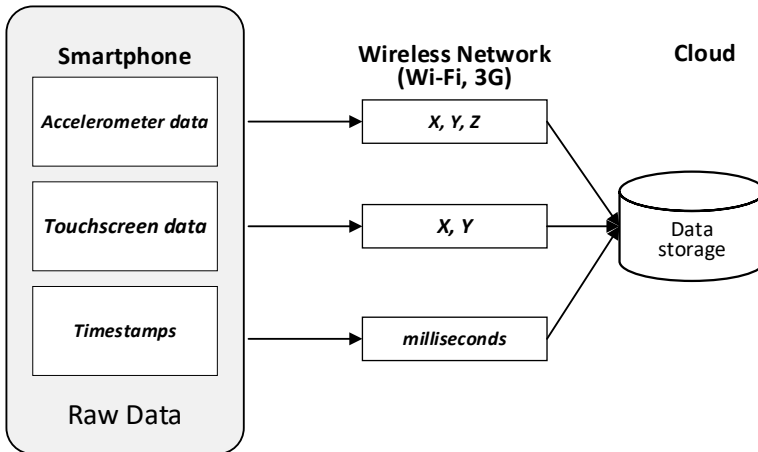


Fig. 47.1 – The architecture of personal mobile sensing system for motor symptoms assessment of Parkinson's disease.

The bottom layer includes the sensing equipment for data acquisition, in our case, it is a smartphone; the middle layer is the wireless network for data transmission, while the top layer is designed for applications and middleware.

47.5 Basic system components utilized and launched on the smartphone

The system includes the following components run on the smartphone: sensors, services for sensor data processing, data storage, mobile application, data transfer.

Sensors. Measuring sensors are planned by the main service. The sampling rate of the sensor depends on the type of sensor.

Processing block is the main full-time operating part of mobile phone. Processing block works as a scheduler for all services to control the start or stop them. The core service does not require heavy computing and has very few I / O operations. In the developed system, the processing unit is responsible for obtaining and storing sensors data on the device.

Memory. The application includes several services and operations, but only one primary service resides in the main memory of the phone while the mobile application is in operation for obtaining and transmitting health state parameters - early signs of Parkinson's disease. The developed mobile application requires 256 MB in the phone memory.

Data store. The sensor data are stored in the internal phone memory. These files are indicated by a digital extension, which indicates the time they were collected. As soon as the recorded data is successfully uploaded to the server, local files are deleted from the phone, which reduces the required amount of internal phone memory.

Data transfer. The application offers automatic mechanisms for uploading data to the server to make the data transfer process more energy efficient and user-friendly. Transmitting data to the server is performed when there is Wi-Fi or 3G connections while passing each test.

In this work, an accelerometer and a touchscreen are used for tremor detection.

Accelerometer. An accelerometer measures the linear acceleration of a moving body along three axes of coordinates. Measurement data is collected and processed using SoC (system on a chip) or a dedicated microcontroller. Further, a mathematical calculation is carried out and the position of the smartphone in space is recorded in real time. In modern devices, each accelerometer calculates the acceleration in its axes: (X, Y, Z). This allows you to get information about the position of the body in three-dimensional space.

Touchscreen. A touchscreen has used the fact that the subject of large capacity conducts alternating current. Electrodes, located at the corners of the screen, supply a small alternating voltage (the same for all angles) to the conducting layer. The current in all four corners is recorded by the sensors and transmitted to the controller, which calculates the coordinates of the touch point. After measuring both

coordinates, the voltage is removed from the plates, and the screen returns to the low-power mode.

47.6 A mobile application of the personal health monitoring system

The mobile application of the personal health monitoring system is used to obtain data on the presence or absence of tremor symptoms. Data acquisition occurs when conducting two tests using the built-in mobile phone sensors described above. The tremor test is performed using an accelerometer and a capacitive touchscreen.

Also, the mobile application is used for preliminary processing of the obtained data. It consists of assigning timestamps to test data. The mobile application store obtained data and processed it in the internal memory of the phone (in the absence of an Internet connection). It is transmitted data to the cloud using a wireless Wi-Fi or a mobile 3G network.

The system requirements of the mobile application are defined. The application module for a smartphone should work on Android version 4.4 and higher. Requirements to the smartphone characteristics are presented in Table 47.2.

Table 47.2 – Smartphone Characteristics

Characteristics	Requirements
Display	5.5 "
RAM	2 Gb
Internal storage	16 Gb

47.7 Cloud infrastructure

The Back4App platform [24] is used as cloud storage. The platform provides the following functions: real-time database, import, and export of JSON files using Parse Dashboard, server version control, command line interface. This platform also allows us to summarize data from different users and monitor changes in their health status.

The system includes cloud storage that is responsible for secure data storing and processing. The user transmits their data (name, sensor data, time and date of the test). The collected data is stored locally in the smartphone memory, then transferred to the server through the device, by initiating an authenticated HTTP push request.

The data processing method was proposed by calculation the statistical data parameters of the data. The next one is classifying on the basis of the calculated statistical parameters, and obtaining a classification model for the next tremor detection. The data processing is carried out on a sliding window. Each window is partially overlapped with the acceleration sampling procedure is processed separately.

For accelerometer data for each acceleration component (X, Y, and Z measurements), the following statistical features were extracted:

- 1) *mean*;
- 2) *standard deviation*;
- 3) *energy of the sequence*: $\sum_i i^2 / w$, where i represents each reading and $w=100$ - the window length;
- 4) *Pearson's correlation* between each pair of acceleration components (X-Y, X-Z, Y-Z).

As a result of the data processing, we obtained 13 variables for each sample window. Further, data can be classified. The classification is carried out using labeled data with three classes output variable - no tremor, middle tremor, heavy tremor.

For touchscreen data for each acceleration component (X, Y, and Z measurements), the 1), 2), 3) statistical features are used, and the Pearson's correlation between each pair of touch components (X-Y, Y-X).

As a result of the data processing, we obtained 8 variables for each sample window. Further, data can be classified. The classification is carried out using labeled data with three classes output variable - no tremor, middle tremor, heavy tremor.

Later, received data are sent from the smartphone to the cloud storage where the severity of the symptoms is analyzed and long-term data storage and analysis is provided. Wi-Fi or 3G networks are used to transmit and obtain data.

47.8 Implementation and Results

In the current release, the personal mobile sensing system includes two tests for evaluating motor symptoms of Parkinson's disease. They are tremor tests using an accelerometer and tremor test using a touchscreen.

Implementation of tremor tests using an accelerometer can be present as follow. This is the simplest test performed with the smartphone at arm's end. The software for tremor testing via accelerometer performs the following functions: data acquisition from the smartphone accelerometer; time-series data preprocessing; sampling; data transformation for processing and analysis; transferring to the cloud storage; normalizing the values of the accelerometer data array to gravity "g." Test implementation enables determining the tremor occurrence in accordance with three states: no tremor, middle tremor, heavy tremor.

Implementation of tremor tests using a touchscreen can be present as follow. The software for tremor testing via the touchscreen assumes the following operations: user login; data acquisition from the results of spiral test execution; data processing; data transferring to the cloud storage.

The target object on the screen is a spiral line. User actions during the spiral test using a touchscreen are as follows. At the first stage, it is necessary to go over the spiral on the screen. The person should perform flowing motion by their index finger and avoid sharp movements as much as possible. On the second stage, the spiral line becomes flashing. The task is the same, to run the finger along the spiral line.

The tremor tests user interface can be present as follow. A graphical user interface has been developed in accordance with a user-oriented approach to the design of a mobile application. It includes the visualization of the obtained accelerometer data during the test, as shown in Fig. 47.2.

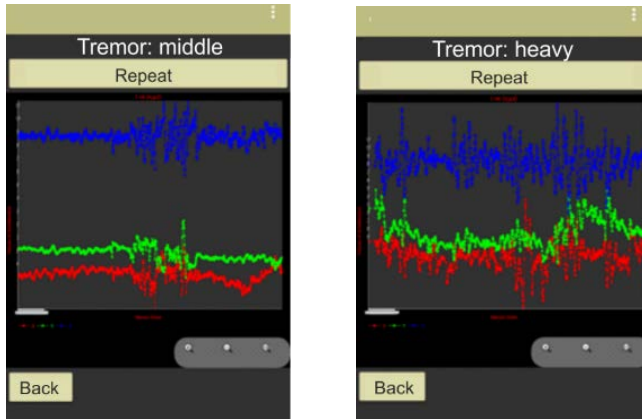


Fig. 47.2 – Tremor test data visualization using accelerometer.

The user interface of a mobile application is shown in Fig. 47.3. It presents the performing of the tremor test using a touchscreen.

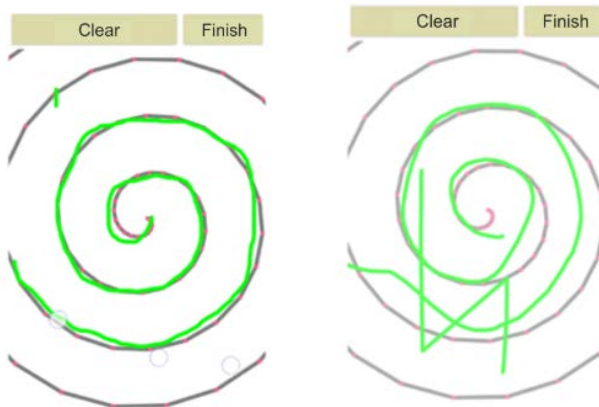


Fig. 47.3 – Tremor test using a touchscreen.

The tremor tests data acquisition can be present as follow. As a result of the tremor test using an accelerometer, the time stamp and accelerometer data are obtained in three axes (X, Y, Z) (see Table 47.3).

Table 47.3 – The fragment of accelerometer data

TS	X	Y	Z
924802121	0.009	8.293	4.539
924802355	-0.086	8.619	4.146
924802362	-0.057	8.466	4.079
924802369	-0.114	8.581	4.52
924802378	-0.086	8.676	4.52
924802387	-0.105	8.715	4.462

As a result of the tremor test using a touchscreen, the time stamp and touchscreen data are obtained in two axes (X, Y) (see Table 47.4).

Table 47.4 – The fragment of touchscreen data

TS	X	Y
510571037	368.44385	446.5152
510571063	368.44385	446.5152
510571090	368.44385	446.5152
510571113	368.44385	446.5152
510571132	368.44385	447.3401
510571158	367.35187	449.60626

Implementation of the data transfer to the cloud storage can be present as follow. We also developed a program code for connecting between smartphone and cloud storage. A dashboard for viewing data in a web browser is shown in Fig. 47.4.

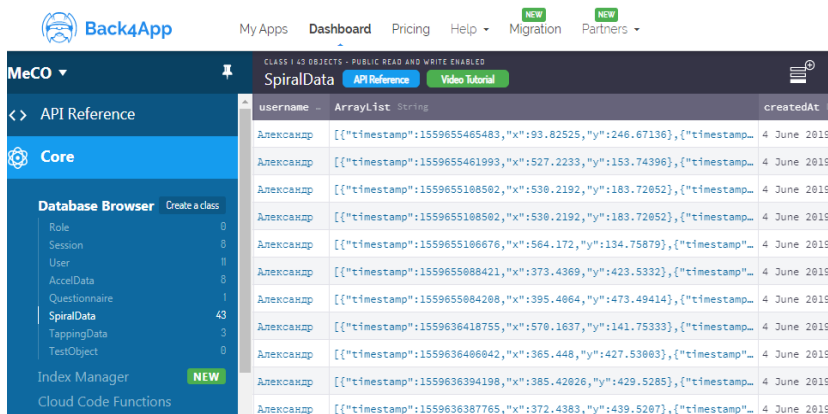


Fig. 47.4 – Viewing cloud data using a web browser. Data is transmitted to the cloud after each passing of the test.

Tremor tests data processing can be present as follow. Data processing is carried out on a sliding window. Each window is partially overlapped with the acceleration sampling procedure is processed separately.

For accelerometer data, for each acceleration component (X, Y, and Z measurements) statistical characteristics were determined, with which a data set was obtained, consisting of 13 incoming and outgoing variables for each sample window. The output variable is represented by three classes - no tremor, middle tremor, heavy tremor. A fragment of the data set is presented in Table 47.5.

Table 47.5 – Generated accelerometer data set (Class H)

TS	M _X	M _Y	M _Z	SD _X	SD _Y	SD _Z	E _X	E _Y	E _Z	PC Y-Z	PC X-Z	PC X-Y
555	-0,06	1,159	9,85	0,07	0,34	0,17	0,01	1,46	97,01	0,12	-0,12	0,39
565	-0,06	1,170	9,85	0,07	0,34	0,18	0,01	1,49	97,11	0,17	-0,12	0,38
575	-0,06	1,18	9,85	0,07	0,35	0,18	0,01	1,52	97,15	0,19	-0,12	0,37
585	-0,06	1,19	9,85	0,07	0,36	0,18	0,01	1,55	97,12	0,16	-0,13	0,38
595	-0,06	1,20	9,85	0,07	0,36	0,18	0,01	1,58	97,07	0,14	-0,13	0,39
605	-0,05	1,21	9,85	0,07	0,37	0,18	0,01	1,62	97,06	0,10	-0,15	0,40

For each component of the touch (X and Y measurements) statistical parameters were determined. It presents by 8 input variables

for each sample window. The output variable is represented by three classes: (N) no tremor, (M) middle tremor, (H) heavy tremor. A fragment of the data set is presented in Table 47.6.

Table 47.6 – Generated touchscreen data set (Class H)

TS	M _X	M _Y	SD _X	SD _Y	E _X	E _Y	PC X-Y
510571037	453,346	383,746	140,1742	215,3732	224975,2	193182,6	0,2795679
510571063	454,854	389,185	138,3105	218,9119	225831,1	198908,4	0,2548802
510571090	456,394	394,503	136,2287	222,3829	226668,3	204592,4	0,2294744
510571113	457,972	399,762	133,9639	225,706	227505,3	210243,6	0,2035836
510571132	459,518	405,046	131,6623	228,8306	228318,6	215902,1	0,1765344
510571158	460,962	410,428	129,4885	231,7206	229085,4	221608,3	0,1479459

47.8 Classification of test data

The original and generated tremor test data set was classified using the proposed data processing method. The 10-fold cross-validation method was used to classify the data. Classification carried out using the Random Tree algorithm. As a result, the confusion matrixes by classification of original and generated data sets are obtained.

The evaluation of the classification was carried out using the following parameters: accuracy, sensitivity, specificity. To calculate these parameters, we used classification assessment by matrix confusion. Based on the matrix confusion the sensitivity, the specificity, and the accuracy are calculated as follows using true positive ζ_{00} , false negative ζ_{10} , true negative ζ_{11} and false positive ζ_{01} results of n observations.

$$\text{Sensitivity} = \frac{\zeta_{00}}{\zeta_{00} + \zeta_{10}} * 100\%,$$

$$\text{Specificity} = \frac{\zeta_{11}}{\zeta_{11} + \zeta_{01}} * 100\%,$$

$$\text{Accuracy} = \frac{\zeta_{00} + \zeta_{11}}{n} * 100\%.$$

The classification comparison results are presented in Table 47.7.

Table 47.7 – Classification comparison results

Model	Sensitivity (%)	Specificity (%)	Accuracy (%)
Original tremor test data	100	99,3	43,7
Generated tremor test data	100	64,9	89,7

The classification accuracy of the proposed data processing approach is 46% higher than the classification accuracy of the original data set.

47.9 Work related analysis

There are different approaches to human biophysical parameters obtaining, processing and analysis in the IoT systems. A common sensor for symptom detection of Parkinson's disease was the accelerometer that was mostly used for detecting the tremor, dyskinesia, and postural instability. Smartphone [4] and Microsoft Kinect [14] are the latest devices in the market used for this.

Angular sensor detectors are used to detect rigidity and postural instability as single symptoms, and they are also used to detect bradykinesia and dyskinesia together with tremor [9]. Video recording is often required for clinicians' observational analysis [21]. Wearable sensors are preferred for Parkinson's disease since it's a progressive chronic disease and symptoms need to be assessed continuously throughout the day [6]. For this, the mobile applications and wristwatches are more preferred as they are currently part of almost everyone's daily accessories. However, their analysis methods and their validations are important and a question is whether the devices or clinical ratings will become the gold standard. Machine learning is a good technique in the development of assessment systems to human state estimation [6].

The relative course from EU universities are include course from colleagues of Newcastle University. The course EEE8085: M2M Technology Internet of Things from Newcastle University is targeted on a deep understanding of interface of sensor an connection to the IoT

gateway, architectures, platforms and applications for M2M IoT systems [25].

Conclusions and questions

The chapter focuses on the personal mobile system for recurrent symptoms assessment of Parkinson's disease development. The mobile devices and methods for objective self-assessment of the symptoms of Parkinson's disease as well as parameters and approaches for data gathering and analysis are discussed. The system architecture, characteristics, and data processing techniques are described. The stages of system design for testing personal health status using the built-in sensors of the smartphone are presented. The proposed solution includes several tests that can be carried out by the user on their mobile phone and integrated data management technique based on the periodic motor symptoms assessment. The implementation of personal mobile sensing system is presented. The analysis of the monitoring systems for the symptoms of Parkinson's disease including the analysis of sensors, devices, detection parameters, and data mining methods, has been carried out. The data processing method is proposed and classification is described.

1. What sensors and devices can be used for health state estimation according to Parkinson's disease?
2. Describe the architecture of IoT-based system for health state estimation.
3. What mobile application requirements must be taken into account when mobile application design?
4. What data are obtained from accelerometer?
5. What data are obtained from touchscreen?
6. What test can be used for tremor estimation?
7. What health state parameters can be used for health state estimation through sensors?
8. What requirements to the application interface design must be taken into account?
9. What the platform can be used for sensors data transfers, storage, visualization and analysis?
10. How can we improve classification accuracy through data processing?

11. What statistical measure can be used for raw data processing?
12. What classification of sensors does you familiar with?
13. How can classification accuracy can be calculated?
14. How can classification sensitivity can be calculated?
15. How can classification specificity can be calculated?

References

1. World Health Organization, 2006. Neurological disorders: public health challenges. The World Health Organization
2. O.M. Manzanera, J.W. Elting, I.H. van der Hoeven, and N.M. Maurits, "Tremor detection using parametric and non-parametric spectral estimation methods: A comparison with clinical assessment", *PloS one*, vol. 11, no.6, pp. e0156822.
1. P. Schwab, W. Karlen, "PhoneMD: Learning to Diagnose Parkinson's Disease from Smartphone Data", *Arxiv.org*, 2019. [Online]. Available: <https://arxiv.org/pdf/1810.01485.pdf> [Accessed: 23- Feb- 2019].
3. S. Arora, V. Venkataraman, A. Zhan, S. Donohue, K.M. Biglan, E.R. Dorsey, M.A. Little, "Detecting and monitoring the symptom Parkinson disease using smartphones: a pilot study", *Parkinsonism & related disorders*, vol.21, no.6, pp. 650-653.
4. B.K. Scanlon, B.E. Levin, D.A. Nation, H.L. Katzen, A. Guevara-Salcedo, C. Singer, S. Papapetropoulos, "An accelerometry-based study of lower and upper limb tremor in Parkinson's disease", *ournal of Clinical Neuroscience*, vol.20, no.6, pp. 827-830.
5. M.Bachlin, M. Plotnik, D. Roggen, N. Giladi, J.M. Hausdorff, G. Tröster "A wearable system to assist walking of Parkinson s disease patients", *Methods of information in medicine*, vol.49, no.01, pp. 88-95.
6. C. Moreau, S. Cantiniaux, A. Delval, L. Defebvre, J.P. Azulay, "Gait disorders in Parkinson's disease: and pathophysiological approaches", *Revue neurologique*, vol.166, no.2, pp. 158-167.
7. S.T. Moore, H.G. MacDougall, W.G Ondo, "Ambulatory monitoring of freezing of gait in Parkinson's disease", *Journal of neuroscience methods*, vol.167, no.2, pp. 340-348.
8. R. Cano-de-la-Cuerda, L. Vela-Desojo, J.C. Miangolarra-Page, Y. Macías-Macías, "Isokinetic dynamometry as a technologic assessment tool for trunk rigidity in Parkinson's disease patients", *NeuroRehabilitation*, vol.35, no.3, pp. 493-501.

9. X. Liu, C.B. Carroll, S.Y. Wang, J. Zajicek, P.G. Bain, "Quantifying drug-induced dyskinesias in the arms using digitized spiral-drawing tasks", *Journal of neuroscience methods*, vol.144, no.1, pp. 47–52.
10. A. Samà, C. Pérez-López, J. Romagosa, D. Rodriguez-Martin, A. Català, J. Cabestany, D.A. Perez-Martinez, A. Rodríguez-Molinero, "Dyskinesia and motor state detection in Parkinson's disease patients with a single movement sensor", In *2012 Annual International Conference of the IEEE Engineering in Medicine and Biology Society*, 2012, pp.1194–1197.
11. G. Lopane, S. ellone, L. Chiari, P. Cortelli, G. Calandra-Buonaura, M. Contin, "Dyskinesia detection and monitoring by a single sensor in patients with Parkinson's disease", *Movement Disorders*, vol.30, pp. 1267.
12. M. Mancini, F.B. Horak, C. Zampieri, P. Carlson-Kuhta, J.G. Nutt, L. Chiari, "Trunk accelerometry reveals postural instability in untreated Parkinson's disease", *Parkinsonism Related Disorders*, vol.17, no.7, pp.557–562.
13. L.F. Yeung, K.C. Cheng, C.H. Fong, W.C. Lee, K.Y. Tong, "Evaluation of the Microsoft Kinect as a clinical assessment tool of body sway", *Gait Posture*, vol.40, no.4, pp. 532–538.
14. A.L. Adkin, B.R. Bloem, J.H.J. Allum, "Trunk sway measurements during stance and gait task in Parkinson disease", *Gait Posture*, vol.22, no.3, pp. 240-249.
15. C. Ahlrichs, A. Samà, M. Lawo, J. Cabestany, D. Rodríguez-Martín, C. Pérez-López, D. Sweeney, L.R. Quinlan, G.Q. Laighin, T. Coughlan, P. Browne, "Detecting freezing of gait with a tri-axial accelerometer in Parkinson's disease patients", *Medical & biological engineering & computing*, vol.54, no.1, pp. 223–233.
16. T.O. Mera, D.A. Heldman, A.J. Espay, M. Payne, J.P. Giuffrida, "Feasibility of home-based automated Parkinson's disease motor assessment", *Journal of neuroscience methods*, vol.203, no.1, pp. 152–156.
17. A. Salarian, H. Russmann, C. Wider, P.R. Burkhard, F.J. Vingerhoets, K. Aminian, "Quantification of tremor and bradykinesia in Parkinson's disease using a novel ambulatory monitoring system", *IEEE Transactions on Biomedical Engineering*, vol.54, no.2, pp. 313–322.
18. S. Mellone, L. Palmerini, A. Cappello, L. Chiari, "Hilbert-Huang-based tremor removal to assess postural properties from accelerometers", *IEEE transactions on biomedical engineering*, vol.58, no.6, pp. 1752-1761.
19. J. Westin, S. Ghiamati, M. Memedi, D. Nyholm, A. Johansson, M. Dougherty, T. Groth, "A new computer method for assessing drawing impairment in Parkinson's disease", *Journal of neuroscience methods*, vol.190, no.1, pp. 143–148.

20. R.J. Dunnewold, J.I. Hoff, H.C. van Pelt, P.Q. Fredrikze, E.A. Wagemans, B.J. van Hilten, "Ambulatory quantitative assessment of body position bradykinesia, and hypokinesia Parkinson disease", *Journal of Clinical Neurophysiology*, vol.15, no.3, pp. 235-242.

21. R.I. Griffiths, K. Kotschet, S. Arfon, Z.M. Xu, W. Johnson, J. Drago, A. Evans, P. Kempster, S. Raghav, M.K. Horne, "Automated assessment of bradykinesia and dyskinesia in Parkinson's disease", *Journal of Parkinson's disease*, vol.2, no.1, pp. 47-55.

22. J. Westin, M. Dougherty, D. Nyholm, T. Groth, "A home environment test battery for status assessment in patients with advanced Parkinson's disease", *Computer methods and programs in biomedicine*, vol.98, no.1, pp. 27-35.

23. "Back4App", *Back4app.com*, [Online]. Available: <https://www.back4app.com> [Accessed: 28- Jul- 2018].

24. "EEE8085: M2M Technology Internet of Things (Inactive)", *Ncl.ac.uk*, 2019. [Online]. Available: <https://www.ncl.ac.uk/postgraduate/modules/EEE8085/> [Accessed: 28- Jul- 2018].

**PART XIII. IOT FOR ECOLOGY, SAFETY AND SECURITY
MONITORING SYSTEMS.**

**48. IOT SYSTEMS FOR CONTROLLING SMALL
ARTIFICIAL ECOLOGICAL SYSTEMS**

Assoc. Prof., PhD, S.V.Morshchavka (ZNTU)

Contents

Abbreviations	598
48.1 Sensors for monitoring artificial ecosystems, the basics of work and physical principles	599
48.1.1 Artificial ecosystems overview, demands and automation possibilities	603
48.1.2 Physical principles of sensors for ecology monitoring	604
48.1.3 Examples of sensors and their implementation	605
48.2 Features of the collection and analysis of information about the state of ecosystems by using IoT devices	608
48.2.1 Networks for collecting ecological information from IoT devices	609
48.2.2 Principles of information analysis about the state of artificial ecosystems	612
48.3 Examples of control systems for small artificial ecosystems .	615
48.3.1 Smart greenhouses	616
48.3.2 Irrigation systems under IoT control	620
48.3.3 Weather monitoring systems	623
48.4 Work related analysis	624
Conclusions and questions	625
References	626

Abbreviations

6LoWPAN – IPv6 over Low power Wireless Personal Area Networks
BLE – Bluetooth Low Energy Protocol
CEA – Controlled Agriculture Technologies
CCCI – Canopy Chlorophyll Content Index
CWSI – Crop Water Stress Index
DB – Database
GIS – Geographik Information System
GPS – Global Positioning System
LED – Light Emmiting Diod
NDVI – Normalized Difference Vegetation Index
NIR – Near Infrared
PAR – Photosynthetically Active Radiation
RF – Radio Frequencies
PPFD – Photosynthetic Photon Flux Density
SMS – System Message on mobile phone
UAV – Unmanned Airborne Vvehicle
VIS – Visible Light
WSN – Wireless Sensor Network

In recent decades, a number of technological changes have taken place in agriculture. Thanks to various “smart” agricultural gadgets, farmers have gained complete control over the process of growing livestock and producing crops.

Analysts from the Goldman Sachs Group argue that most countries, actively developing their agriculture, are moving smoothly from the "analogue" to the "digital". According to their forecasts, the use of new technological solutions is able to increase global agricultural production by 70% by 2050, which will bring additional agricultural products by almost \$ 800 billion.

One of these digital technologies that can transform agriculture in many ways is IoT [1,2].

There are 5 ways that IoT can help improve agribusiness:

Method 1. A huge array of data that can be collected using smart sensors: information about weather conditions, soil quality, progress in crop growth or livestock health. This data can be used both to monitor the state of your fields or farms as well as for real-time changing of conditions for growing.

Method 2. Improving business efficiency [3] by automating processes in the production cycle: irrigation, fertilization or plant protection.

Method 3. Better production control and support higher standards of quality and crop growth through automation [4].

As a result, all of these factors may ultimately lead to increased incomes.

In any case, to obtain information about the current state of agricultural land, livestock, plants, it is necessary to have a system, which must provide objective information at a real- or quasi-real-time pace. The basis of such a system for collecting information is different types of sensors.

48.1 Sensors for monitoring artificial ecosystems, the basics of work and physical principles

There are many types of IoT sensors (Fig. 48.1) for agriculture, as well as IoT applications in agriculture in general [5].

1 SENSORS & ACTUATORS

We are giving our world a digital nervous system. Location data using GPS sensors. Eyes and ears using cameras and microphones, along with sensory organs that can measure everything from temperature to pressure changes.

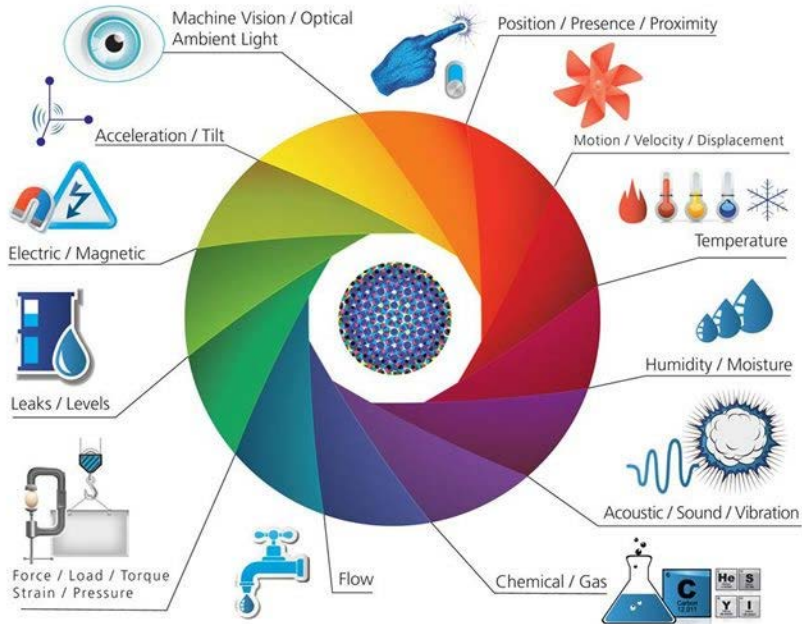


Fig. 48.1. IoT sensors map – source: IoT infographic Postscapes and Harbor Research

Consider the principal part of them by category and their physical principles of working [6]:

1. Climate Monitoring Sensors.

The popular smart gadgets in agriculture are meteorological stations consisting of various intelligent sensors. Located across the field, they collect data from the environment. The obtained measurements can be used to compare climatic conditions, help select appropriate crops and take the necessary measures to increase their productivity.

Most of sensors for such stations has well known principles of working that uses in many industrial sensors (Table 48.1). But an

interesting feature of some IoT sensors is the use of relative or uncalibrated measurements.

Table 48.1 – The comparison of the most popular wireless protocols

Sensor type	Typical range	Accuracy	Physical realization
Solar irradiance (IR + visible)	0~100%	16bit or 8 bit	Si diod or photovoltaic device with sensitivity in range 300~1100nm
Atmospheric pressure	760 ± 200 mmHg	10 mmHg	Barometric or Hall based sensors
Rainfall	0~100 mm/h	<10%	Rain gauge with optical, mechanical or ultrasound measurement of liquid flow
Air Humidity	0~100%RH	1..5%	Dew point temperature measurements
Air Temperature	40~ 125°C	<1°C	Resistor or thermocouples temperature detectors
Soil Temperature	10~85°C	<1°C	Infrared light sensors
Capacitive Soil Moisture	0~100%	28bit	Sensor of omnic resistance with 2 electrodes
Wind speed	0~100 kmh	<10kmh	Mechanical/electrical convertors
Wind direction	0~360°	<5°	Optical or electromagnetic measurements of angles

As examples of such agricultural IoT meteostaions can be allMETEO, Smart Elements, Libelium and Pycno.

2. Greenhouse automation.

In addition to determining climatic conditions, meteorological stations can also automatically adjust them according to the parameters to be set. In particular, greenhouse automation systems use this principle. Some following sensors that connected to actuaror are specific for such systems: sensors for opening and closing of ventilation slots, sensors for electromotors, etc.

For example, Farmapp and Growlink are also IoT agricultural products offering, among other things, such opportunities.

GreenIQ is also an interesting product that uses IoT sensors. It is an intelligent sprinkler controller that allows you to remotely control irrigation and lighting systems.

But for greenhouse also can be used some chemical sensors as like gas (CO₂) or liquid (compounds of nitrogen, potassium, phosphorus) concentrations sensors. Such information also can be collected in hydroponic systems. Hydroponics can be considered as a subsystem in a greenhouse with a part of functions to ensure an adequate level and quality of plant nutrition. For large greenhouse complexes, this preparation of liquid mixtures can be provided by much more expensive and proprietary systems. However, the principle of operation remains the same.

3. Plant Management and Monitoring.

Another type of IoT in agriculture is devices that are placed directly in the fields for collecting data related to agriculture: from temperature and precipitation to the water potential of the leaf and the general state of plant health.

Thus, crop growth and anomalies are controlled. This allows you to effectively prevent any disease that may harm the crop. Arable and Semios are a good example of applying these technologies in real life.

The sensors that use for such purposes can be as ground-based as well as air-based (now more often uses unmanned airborne vehicles – UAV) [7,8].

4. Control and management of cattle

There are sensors attached to animals on the farm to monitor their condition and performance. For example, Allflex and Cowlar SCRs use similar sensors (labels for collars) to obtain data on temperature, health, activity, and nutrition information for each individual cow, as well as collective information about the herd.

5. Integrated Farm Management Systems

A more complex approach to IoT in agriculture is farm productivity management systems. They usually include a number of IoT devices [9] and sensors installed on the farm's territory, as well as a powerful monitoring panel with analytical capabilities and built-in accounting functions.

This provides the ability to remotely monitor a farm and optimizes most business operations. Similar solutions are presented by FarmLogs and Cropio.

In addition to these areas, IoT is used for vehicle tracking (or automation), storage management, and logistics.

48.1.1 Artificial ecosystems overview, demands and automation possibilities

Some of the important characteristics of artificial ecosystem and are as follows:

1. In an artificial ecosystem, the diversity must be lesser compared to natural systems. Unfavourable species must be controlled or eliminated. And this is one from areas to using IoT for controlling such ecosystems.

2. Unlike natural systems, in which the basic idea is the surviving, an artificial ecosystem is pragmatic with certain and a priori known goals. But this means that most self-regulation mechanisms in artificial systems are absent, and IoT can be used as such a mechanism.

3. Artificial ecosystems are more productive in realizing its main goals. The optimization task is improving land yield, farm productivity and greenhouses yield, etc., are typical for systems that use the same loop as IoT: ecosystem->sensors->controller->actuator->ecosystem.

4. Artificial ecosystems have some border between internal space and the external environment. This shell can be more or less tangible. But in any case, it can make possible to use artificial ecosystem in areas that were unsuitable for production before. And in this direction, IoT (for example - meteostations) can be used as a system that maintained differences between external and internal areas.

5. Artificial ecosystems have their own cost of implementation. And to optimize the ratio of productivity and cost often required systems with scalable cost, which linearly depends on the scale of the ecosystem. And IoT meets these requirements.

The examples of artificial ecosystems are: Modern cities, hydroponics (cultivation of plants without soil and sunlight), skylabs

and spaceships, mechanized agricultural farms, bio reactors in the industry and many others.

48.1.2 Physical principles of sensors for ecology monitoring

Drones are used to gather a variety of image-based data about the condition of crops, fields, livestock and other ecosystems [10, 11] – including:

- plant height;
- plant count;
- plant health;
- presence of nutrients;
- presence of disease;
- presence of weeds;
- relative biomass estimates;
- 3D / volumetric data (piles, patches, holes and hills).

For livestock operations, drones can be used to monitor the location, status and movement of animals over time with more frequency and at a lower cost than other means.

Drone data is used to do farming jobs more effectively and efficiently, including [8]:

- Crop Scouting – replace men with drones;
- Crop Health Monitoring – biggest area of interest, by far;
- Field Surveying/Scouting (before planting);
- Nitrogen Recommendation;
- Yield Monitoring;
- Plant Stress Monitoring;
- Drought Assessment;
- Senescence Analysis;
- Leaf Area Indexing;
- Phenology;
- Tree Classification;
- and more.

The sensors, in this case, will have electro-optical principles. The multispectral and hyperspectral image sensors available now for use on UAV. A good example of using multispectral cameras with a varied set of available ranges of spectra is in systems that provided by Cubert, PEAU Production, AgEagle, etc.

48.1.3 Examples of sensors and their implementation

Description of the examples of sensors is appropriate to start with one of the most famous popularizers and suppliers of IoT solutions for agriculture - the company Libellium. The solution promoted by it is characterized by complexity and openness, which allows the use of a wide range of sensors, some of which are described in the Table 48.2.

The Wasmote Plug & Sense! Smart Agriculture Xtreme sensor node (Fig. 48.2) includes a more reliable weather station to measure the wind and precipitations via optical technology. It also features a complete set of light and radiation sensors such as ultraviolet radiation, photosynthetically active radiation (PAR) and shortwave radiation. The soil morphology and the presence of fertilizers can be analyzed by measuring electrical conductivity, volumetric water content, soil water potentials and oxygen levels. To prevent frost, the new device allows customers to connect a special sensor to measure non-contact plants and fruits surface temperature. And for daily growth monitoring, there are a set of dendrometers to control the growing of the trunk, the stem and the fruit of the plant.



Fig. 48.2 Wasmote Plug & Sense! Smart Agriculture Xtreme

The new solution features 19 sensors from the most prestigious and reliable manufacturers of agricultural technology such as Apogee, Decagon, Ecomatik and Gill Instruments.

This integration enables the measuring of different parameters related to weather conditions, light and radiation levels, soil morphology, fertilizers presence, frost prevention, daily growth of plants and fruits and other environmental parameters to improve crop quality production and to prevent harvest losses.

Table 48.2 – The list of possible sensors for Libellium Waspnote

Manufacturer/Model	Measured parameters	Applications
Apogee SI-411	Non-contact surface temperature measurement	Plant canopy temperature measurement for plant water status estimation, road surface temperature measurement to determine icing conditions, and terrestrial surface (soil, vegetation, water, snow) temperature measurement in energy balance studies.
Apogee SF-421	Leaf and flower bud temperature	Leaf and bud temperature estimates in cropped fields, orchards, and vineyards. Leaf and bud temperatures returned by the detector can then be used to alert growers to the potential of frost damage to crops.
Apogee SO-411	Oxygen levels	Measurement of O ₂ in laboratory experiments, monitoring gaseous O ₂ in indoor environments for climate control, monitoring of O ₂ levels in compost piles and mine sailings, monitoring redox potential in soils, and determination of respiration rates through measurement of O ₂ consumption in sealed chambers or measurement of O ₂ gradients in soil/porous media.
Apogee SU-100	Ultraviolet radiation	UV radiation measurement in outdoor environments, laboratory use with artificial light sources (e.g. germicidal lamps), and monitoring the filter ability and stability of various materials.
Apogee SQ-110	Photosynthetically active radiation (PAR)	PPFD (Photosynthetic Photon Flux Density) measurement over plant canopies in outdoor environments, greenhouses, and growth chambers, and reflected or under-canopy (transmitted) PPFD measurements in the same environments. Quantum sensors are also used to measure PAR/PPFD in aquatic environments.

Table 48.2 – The list of possible sensors for Libellium Waspnote

Manufacturer/Model	Measured parameters	Applications
Apogee SP-510	Shortwave radiation	Shortwave radiation measurement in agricultural, ecological, and hydrological weather networks. Sensors are also used to optimize photovoltaic systems.
Decagon GS3	Electrical conductivity, volumetric water content and temperature of the soil	In potting soil and soilless medias, to maintain good soil contact and compensate for air gaps in the substrate. Greenhouse substrate monitoring. Irrigation management. Salt management. Fertilizer movement. Modeling processes that are affected by temperature.
Decagon 5TE	Electrical conductivity, volumetric water content and temperature of the soil	Greenhouse substrate monitoring. Irrigation management. Salt management. Fertilizer movement. Modeling processes that are affected by temperature.
Decagon 5TM	Temperature, volumetric water content of the soil	Soil water balance, irrigation management, modeling processes that are affected by temperature.
Decagon MPS-6	Soil water potentials	Deficit irrigation monitoring and control. Water potential monitoring in the vadose zone. Crop stress. Waste water drainage studies. Plant water availability.
Decagon VP-4	Vapor pressure, humidity, temperature and atmospheric pressure in soil and air	Greenhouse and canopy monitoring. Reference evapotranspiration calculations. Routine weather monitoring. Building humidity monitoring. Mold remediation. Modeling processes that are affected by vapour pressure or humidity.
Decagon Phytos-31	Leaf wetness	Usage decisions for crop fungicides. Predict crop diseases or infections.
Ecomatik DC2	Trunk diameter	Plants growth processes monitoring. Examination of the influence of environmental factors on plant growth. Precise dating of the beginning and end of the growing season.
Ecomatik DD-S	Stem diameter	Plants growth processes monitoring. Examination of the influence of environmental factors on plant growth. Precise dating of the beginning and end of the growing season.
Ecomatik DF	Fruit diameter	

Table 48.2 – The list of possible sensors for Libellium Waspnote

Manufacturer/Model	Measured parameters	Applications
Bosch BME280	Temperature, air humidity and pressure	Weather forecast, Control heating, ventilation, air conditioning in greenhouses.
AMS (taos) TSL2561	Luxes	Light presence detection for artificial lightning usage.
Maxbotix MB7040	Ultrasound	Tank level measurement.
Gill Instruments GMX-240	Wind speed, direction and precipitations	Weather forecast.

48.2 Features of the collection and analysis of information about the state of ecosystems by using IoT devices

Today, the wireless technologies of the IoT makes it possible with the help of various sensors to predict climate change and analyze the ecological state of almost any region of the Earth. A lot of them are already adapted to the processes of managing the elimination of the negative impact on nature in places of high concentration of people, in particular, in large and medium-sized cities.

The ability to receive a continuous stream of data allows you to take the necessary measures and avoid many of the threats associated with environmental anomalies. Among the well-known features of "smart" devices - monitoring of weather conditions, seismic hazards, the state of the atmosphere and water. These are, albeit important, by no means all areas of application of IT-technologies in the environmental field. Today, new products based on IoT systems are being actively developed and tested, aimed at solving environmental problems. Their mass implementation is hampered by certain technical problems, for example, various protocols of device operation, imperfect wireless infrastructure, but all of them are at the decision stage and will be removed in the near future.

In recent years, personal environmental sensors and mobile applications for removing data from them have been particularly

popular. The range of their capabilities is quite wide: from measuring environmental parameters (air quality, temperature, humidity, carbon dioxide content) to the level of radiation. There are those with which you can check the amount of nitrates in products. The small size and operation via Wi-Fi, Bluetooth and GPS modules allows you to monitor the environment using crowdsourcing technology, which greatly increases the accuracy of the data obtained. With the help of personal sensors it is possible to change the ways of obtaining information and its processing. Anyone can receive data from sensors and sensors both on a PC and a smartphone.

The huge potential of IoT technology, which has not yet been fully exploited, is capable of giving humanity new solutions to environmental problems. And today there are a lot of projects in the world, which are based on monitoring the state of the environment with the help of “smart” devices that can prevent man-made disasters or natural disasters.

48.2.1 Networks for collecting ecological information from IoT devices

If it need to understand how to build IoT devices, first it need to figure out how they will communicate with the rest of the world [12].

1. Local Network

The choice of communication technology directly affects your device’s hardware requirements and costs. Which networking technology is the best choice? IoT devices are deployed in so many different ways — in clothing, houses, buildings, campuses, factories, and even in your body — that no single networking technology can fit all bills.

Let’s take a factory as a typical case for an IoT system (Fig. 48.3). A factory would need a large number of connected sensors and actuators scattered over a wide area, and a wireless technology would be the best fit [13,14].

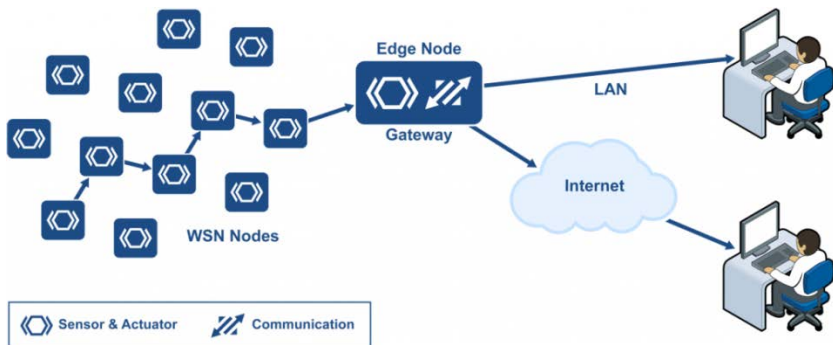


Fig. 48.3. The wireless networks and popular protocols

Wireless sensor network installed in a factory, connected to the Internet via a gateway. A wireless sensor network (WSN) is a collection of distributed sensors that monitor physical or environmental conditions, such as temperature, sound, and pressure. Data from each sensor passes through the network node-to-node.

2.WSN Nodes.

WSN nodes are low cost devices, so they can be deployed in high volume. They also operate at low power so that they can run on battery, or even use energy harvesting. A WSN node is an embedded system that typically performs a single function (such as measuring temperature or pressure, or turning on a light or a motor).

Energy harvesting [15] is a new technology that derives energy from external sources (for example, solar power, thermal energy, wind energy, electromagnetic radiation, kinetic energy, and more). The energy is captured and stored for use by small, low-power wireless autonomous devices, like the nodes on a WSN.

3.WSN Edge Nodes

A WSN edge node is a WSN node that includes Internet Protocol connectivity. It acts as a gateway between the WSN and the IP network. It can also perform local processing, provide local storage, and can have a user interface.

4.WSN Technologies

The battle over the preferred networking protocol is far from over. There are multiple candidates.

5.Wi-Fi

The first obvious networking technology candidate for an IoT device is Wi-Fi, because it is so ubiquitous. Certainly, Wi-Fi can be a good solution for many applications. Almost every house that has an Internet connection has a Wi-Fi router.

However, Wi-Fi needs a fair amount of power. There are myriad devices that can't afford that level of power: battery operated devices, for example, or sensors positioned in locations that are difficult to power from the grid.

6.Low-Power Solutions

Newer networking technologies are allowing for the development of low-cost, low-power solutions. These technologies support the creation of very large networks of very small intelligent devices. Currently [16], major R&D efforts include:

- Low-power and efficient radios, allowing several years of battery life
- Energy harvesting as a power source for IoT devices
- Mesh networking for unattended long-term operation without human intervention (for example, M2M networks)
- New application protocols and data formats that enable autonomous operation

For example, EnOcean has patented an energy-harvesting wireless technology to meet the power consumption challenge. EnOcean's wireless transmitters work in the frequencies of 868 MHz for Europe and 315 MHz for North America. The transmission range is up to 30 meters in buildings and up to 300 meters outdoors.

7.IEEE 802.15.4

One of the major IoT enablers is the IEEE 802.15.4 radio standard, released in 2003. Commercial radios meeting this standard provide the basis for low-power systems [17,18]. This IEEE standard was extended and improved in 2006 and 2011 with the 15.4e and 15.4g amendments. Power consumption of commercial RF devices is now cut in half compared to only a few years ago, and we are expecting another 50% reduction with the next generation of devices.

8.6LoWPAN

Devices that take advantage of energy-harvesting must perform their tasks in the shortest time possible, which means that their transmitted messages must be as small as possible. This requirement has implications for protocol design. And it is one of the reasons why

6LoWPAN (short for IPv6 over Low power Wireless Personal Area Networks) has been adopted by ARM (Sensinode) and Cisco (ArchRock). 6LoWPAN provides encapsulation and header compression mechanisms that allow for briefer transmission times.

Table 48.3 – The wireless radio technologies

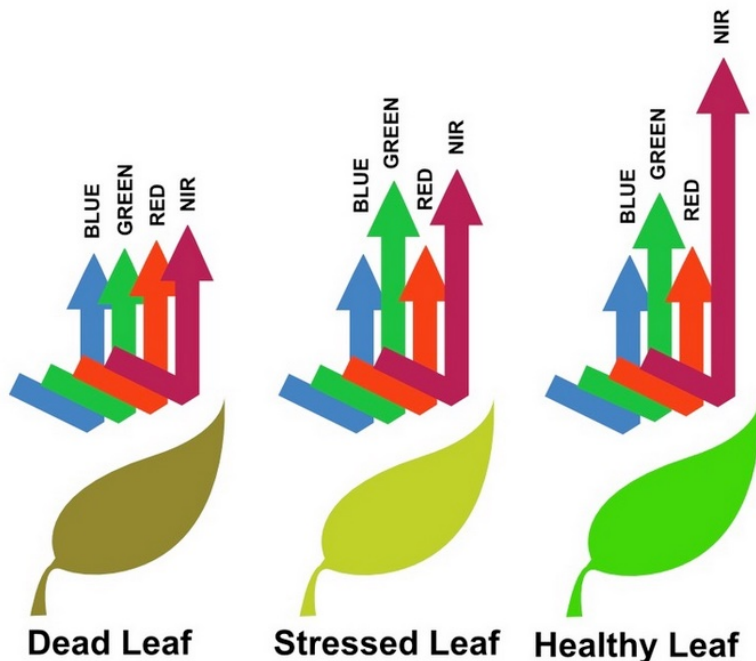
Technology	Bluetooth	IEE 802.15.4	Z-Wave	6LoWPAN	Wi-Fi	RF
Frequency, GHz	2,4	2,4; 0,915; 0,868	up to 1,0	1,0; 2,4	2,4; 5,0	0,433; 0,315
Speed, Mbps	up to 24	up to 0,25	up to 0,1	up to 0,250	up to 300	up to 0,01
Approx. range, m	up to 100	up to 100	30	800	up to 100	50
Power	Low	Very Low			High	

48.2.2 Principles of information analysis about the state of artificial ecosystems

Most agriculture drones depend on multi-spectral imaging to spot problems with a crop's health; specifically, they look at changes over time in visible light (VIS) and near-infrared (NIR) light reflected by crops. These images are taken over time by drones, manned aircraft or satellites.

It is possible to detect plant health from these images because plants reflect different amounts of visible green and NIR light, depending on how healthy they are. By measuring the changes in visible and NIR light reflected from a crop, we can spot potential health issues.

This image (Fig. 48.4) explains the general idea:



The basic principle of NDVI relies on the fact that, due to their spongy layers found on their backsides, leaves reflect a lot of light in the near infrared, in stark contrast with most non-plant objects. When the plant becomes dehydrated or stressed, the spongy layer collapses and the leaves reflect less NIR light, but the same amount in the visible range. Thus, mathematically combining these two signals can help differentiate plant from non-plant and healthy plant from sickly plant.

(image courtesy Agribotix.com)

Fig. 48.4. The basic principle of NDVI

To monitor changes in plant health over time, drone images are processed to calculate a tracking index called NDVI (normalized difference vegetation index), which is a measure in the difference between light intensity reflected by the field in two different frequencies:

NDVI is the ratio of near infrared (NIR) reflectivity minus visible red reflectivity (VIS), divided by NIR plus VIS:

$$\text{NDVI} = (\text{NIR} - \text{VIS}) / (\text{NIR} + \text{VIS})$$

Here is (Fig. 48.5) what you see when you compare a normal camera image of a winter wheat field to a NDVI-processed image of the same field:



Fig. 48.5. An example of using indexed images

VIS and NDVI images of winter wheat field (courtesy Agribotix)

Notice how the NDVI-enhanced image (right) does a great job separating the healthy wheat stalks (green) from dying edges (red) and the dry earth (black/brown).

There is some debate over whether NDVI is the right index or whether the simple difference between light spectrums ($NIR - VIS$) is more useful. Agribotix put together a great writeup on this debate and the misconceptions re. what NIR spotting can and cannot do today.

NDVI is the most popular index calculated using drone data, but there are many others. Some may be more or less important to your farm, depending on your situation. Some of the more popular indices include:

- CWSI (crop water stress index): measures temperature differentials to detect/predict water stress in plants. Requires a thermal imaging sensor and the use of a nearby weather station.
- CCCI (canopy chlorophyll content index): detects canopy nitrogen levels using three wavebands along the red edge of the visible spectrum. Requires visible and near infrared cameras.etc.).

48.3 Examples of control systems for small artificial ecosystems

The project team Drone.ua launched an automated system for monitoring and analyzing farmland for small and medium-sized entrepreneurs Zemli.online (Fig. 48.6). This system allows the use of real-time field data obtained from Landsat and Sentinel satellites for comparing productivity maps and evaluating the performance of the current year to the results of previous years of operation of enterprises. Regular monitoring will identify problem areas. Information about them will come in the form of SMS or e-mail. This will provide a higher decision-making speed and the ability to create operational task cards for equipment.

All data can be exported and used in any convenient or existing GIS. Monitoring solutions allow you to implement a complex of various tasks of an enterprise: from the assessment of a land bank to the formation of maps for differential fertilization. Satellite monitoring data is supported by information obtained from meteorological stations, drones or ground laboratories. The system uses decision-making help modules based on machine learning and intelligent forecast generation algorithms.

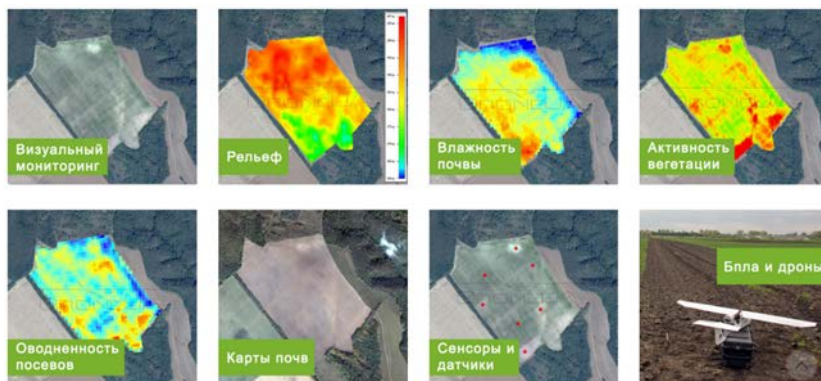


Fig. 48.6. The system Zemli.online

While drones are currently used to take hyperspectral images by attaching the appropriate sensor, it's the future use of drones and IoT connected devices that is particularly exciting. As with any process,

hyperspectral image analysis will become more routine, computing power will increase, and the location of computing can go from the desktop or cloud to being done on device. That is to say, the drone itself will have the computational horsepower to analyze the data obtained from the onboard sensor taking the image and determine the problem. At that point, a drone that is network connected can transmit this information to an agronomist for further analysis and consideration, or in the future it may relay that information to another drone. That drone can be tasked with collecting a sample plant and delivering it to an agronomist for analysis. In this scenario, the time it takes to determine the existence of plant pathogens is decreased and the treatment time is sped up. This reduces the cost to the grower in terms of chemicals used for treatment and lost yield due to crop damage. Additionally, with this type of technology an agronomist can support a larger number of acres and save both time and money.

To get a second perspective, consider the scenario of drought. In the event a field has a dry spot, a drone flies over and captures a hyperspectral image. The hyperspectral image analysis can be done on the drone (it could still be uploaded to the cloud for historical purposes). The drone can then communicate over the network to an irrigator. The irrigator, with its remote computing power from onboard electronics, uses the mapping information and connected GPS sensor data on device to automatically plot a path and plan for irrigating the dry land. All done without the need for interaction from an individual except for the occasional software update. While not the reality right now, this level of sophistication is where the future of precision agriculture is headed as it leverages drones and IoT.

48.3.1 Smart greenhouses

A smart greenhouse is a fully automated system designed to facilitate the process of growing crops and minimize the use of manual labour. This agricultural system includes microcontrollers, sensors and IoT applications [19] (Fig. 48.7).

The emergence of smart greenhouses and hydroponics has revolutionized agriculture, allowing, for example, to more effectively grow exotic fruits in northern latitudes. At the heart of any smart greenhouse are sensors, actuators, monitoring and control systems,

which together can optimize many factors and growth conditions of agricultural crops.

Often, smart greenhouses work in sync with other technological solutions, such as automatic irrigation technologies and HVAC systems. Intelligent sensors record data on plant growth, irrigation, the presence of pests and lighting, and send them to a local or cloud server. The web-based admin console allows farmers to customize system settings and integrate it with other solutions. The mobile application generates alerts and reports on the performance of the IoT greenhouse.

By type, smart greenhouses can be divided into those that use hydroponics (growing crops without soil) and the usual cultivation of crops in the ground.

Technologies such as are key for smart greenhouses:

- LED projectors for plant growth;
- connection technologies;
- irrigation systems;
- valves and pumps;
- monitoring systems;
- control systems.

What technologies make greenhouses smart and the key features of greenhouses explained in follows:

1. Illumination

With the help of LEDs, additional illumination of cultivated crops in the greenhouse or greenhouse is easily provided. The best lighting systems have a compact design and a long service life (from 30 to 50 thousand hours) and consume less energy.

2. Sensors

Depending on the needs of farmers, any combination of sensors is possible: temperature sensors, humidity sensors, exposure meters, soil composition sensors (acidity, chemical composition), dew point sensors, water quality control sensors for irrigation, etc.

3. Networks

To connect the sensors using wired or wireless networks. LPWAN, such as LoRaWAN, RF, NB-IoT, etc., may be involved in remote areas. As a rule, networks of the non-licensed range are used for communication, which in many cases reduces the cost of using

equipment, subscription fee for service, etc. One of the connection options can be as on Fig. 48.7

4. Desktop and mobile applications

Monitoring systems, as a rule, have an intuitive and intuitive interface. You can control all processes using a tablet, smartphone, laptop.

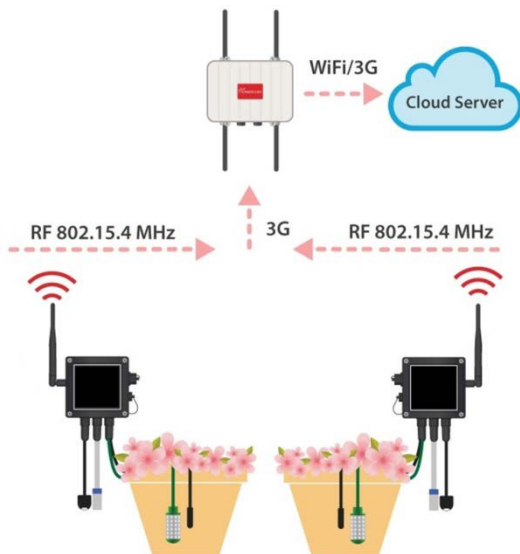


Fig. 48.7. Experiment Solart station web-page

The benefits of greenhouse automation:

1. Protection against temperature extremes. Maintaining and controlling the temperature range in a greenhouse environment is crucial. Temperature fluctuations can damage or kill plants for several hours. Remote monitoring systems protect valuable plants from extreme temperature fluctuations.

2. Control of inventory and other equipment. In addition to maintaining the optimum temperature, it is necessary to ensure the safety of inventory and efficient operation of air conditioning systems, maintain humidity, etc.

The sooner a farmer detects a drop in temperature or equipment failure, the more likely it is to save property and plants. Remote monitoring systems send updates in real time, so employees can quickly respond to threats.

3. Situation monitoring

If a condition falls outside the pre-established range, the device or system immediately alerts the responsible employees by phone, email or SMS. Emergency notifications usually notify farmers of:

- lowering the temperature;
- Poor ventilation;
- High carbon dioxide levels;
- Changes in humidity;
- Equipment failure;
- Water leakage.

Disease prevention during the growing season

During the growing season, systems in smart greenhouses can control various environmental conditions. Both wired and wireless sensors are used for this. Maintaining temperature, humidity, light, and air circulation parameters is critical to prevent mold, disease, and maximize plant yields.

The stages of design of smart greenhouse is as follows:

The supplier selects the right technology stack for the project based on many factors:

- the size of the greenhouse;
- type of crops;
- implemented technical solutions.

The required number of IoT sensors is calculated individually. As a rule, depending on the destination, one sensor can cover up to 30 square meters. meters of arable land. Sensor microcontrollers consume very little power (150 ma with active data transfer in BLE and Wi-Fi networks and only 5 ma with deep sleep enabled).

The next step is to provide communication between the microcontrollers that are part of the IoT system. To do this, select the type of connection. Then you need to configure the server that controls the sensors and systems in the smart greenhouse. The next step is setting up the software. Advanced systems use an intuitive interface in which sensors are added at the touch of a button. Each sensor can be given a name, and the territory of a smart greenhouse can be divided into sectors. Information can be tracked both by sector and as a whole. The last step in creating a smart greenhouse is setting up mobile or web applications and the frequency of notifications about

the operation of sensors in normal mode and emergency warnings about emergency situations.

China has created an application for smartphones that manages many processes (watering, fertilization, temperature and humidity control) in a smart greenhouse. The area of the complex is 0.5 ha. The developers noted that the system delivers water and nutrients directly to the roots of the plants. Every half hour the system notifies of the microclimate in the greenhouse complex and the identified pests of agricultural crops.

It is expected that the segment of intellectual agriculture will develop at a high rate. But the high cost of deploying solutions and high initial investment costs can lead to slower market growth in the developed countries of the Middle East and Africa. Europe will remain the market leader for the forecast period. The Netherlands, Spain and Italy have large areas for greenhouses.

Controlled Agriculture Technologies (CEA) are mainly used in the Netherlands and Scandinavian countries. Indoor gardening is gaining rapid momentum in some of the largest countries in Europe. Rapid adoption of technology is expected in emerging economies like Japan, China and India. ”

According to analysts, key technologies used for smart greenhouses: lamps for plant growth, connection technologies, irrigation systems, valves and pumps, monitoring and control systems. In 2016, there was a sharp increase in demand for LED lamps for growing plants.

Key players in the market: Rough Brothers, Heliospectra, Terrasphere Systems, Argus Control Systems, LumiGrow, Ceres Greenhouse Solutions, Hort Americas, JFE Engineering Corporation, Nexus Corporation, Logiqs, Certhon и GreenTech Agro.

48.3.2 Irrigation systems under IoT control

California farmers are facing high labor costs and also difficulty in even finding enough workers. So there is considerable interest in finding ways to cut down on the time consuming job of monitoring, controlling and maintaining irrigation systems [20,21]. At the same time growers are once again dealing with water shortages after last year's unusually abundant rains and snow. A company called

WaterBit is working with AT&T to set up autonomous systems (Fig 48.8) that monitor the water status in farmer's fields and then connect that with automated valves and pumps that control water delivery.

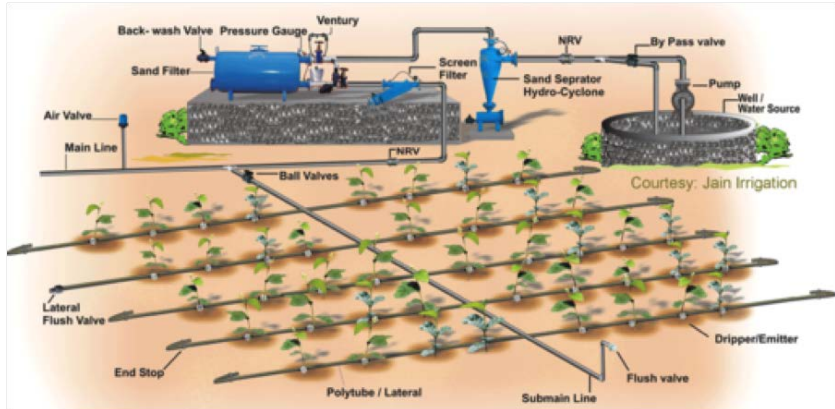


Fig. 48.8. Real scale small irrigation Line project

Electronic probes that measure the moisture content of soil have been available for some time, but what is particularly attractive about this offer is the means of connecting that data with the workings of the irrigation system without the need for someone to be physically present at either site or to spend the time driving between them. The probes typically are set up to give readings at several depths so that the farmer can know where the roots of the crop are extracting water and even if water is going below the root system – something to be avoided both for water conservation and for ground water protection. There can be significant variations in soil type across a field, so growers can add more probes to capture that variation. Some fields can be reasonably managed in 20-25 acre sub-sections while in other cases growers would ideally manage the water down to even a 1/4acre “microblocks. The solar powered sensors use long-range radio to transmit their data from small telemetry boxes 1.5 feet, or less, above ground in the field. This is needed because cellular signals won't travel well through the dense leaves of a crop canopy. From several hundred of those boxes the signal is sent to a 30-foot tower for telemetry to the Cloud. The farmer can then use that information to

make irrigation decisions and send those instructions out to the pipes or canals from which water is drawn.

In the agriculture field, sensors are used like soil moisture. The information received from the sensors need be sent to the Server (cloud) DB through the Android device. Also, this system is automatically activated when the soil moisture is low, the pump is switched ON based on the moisture content.

But smart irrigation it isn't only big fields. As this often happens in using IoT the home flower irrigation also can be realized on this basis (Fig. 48.9).

The application has a feature like taking some time from the user and water the agriculture field when the time comes. In this system, there is a switch used to turn off the water supply if the system fails. Other parameters such as the moisture soil sensor demonstrate the threshold price and the level of water in the soil.

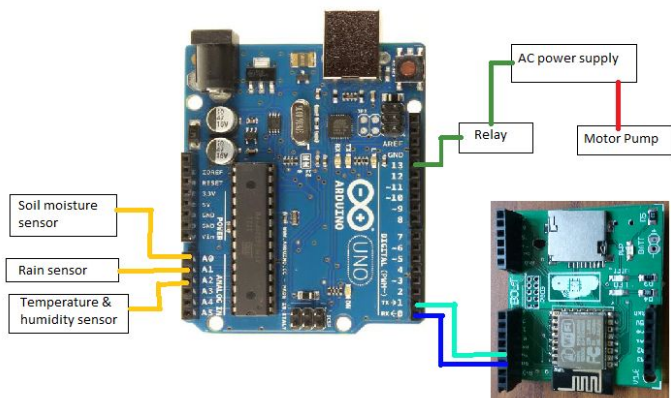


Fig. 48.9. Small scale irrigation project

Further, this project can be enhanced by designing this system for large acres of soil. Also, this project can be incorporated to make sure the value of the soil and the expansion of harvest in each soil. The microcontroller and sensors are successfully interfaced and wireless communication is attained between a variety of nodes.

Also, further this proposed system can be enhanced by adding up machine learning algorithms, which are capable to study and

recognize the necessities of the crop, this would aid the agriculture field to be an automatic system.

48.3.3 Weather monitoring systems

Responding to the growing demand of precision from the smart agriculture devices market, Libelium releases a new version of its Smart Agriculture sensor node improving maximum accuracy for crop monitoring. The enhanced Waspote Plug & Sense! Smart Agriculture Xtreme device includes top market performance sensors for the most exigent field applications such as vineyards, fruit orchards and greenhouse cultivations, among others.

Libelium has developed a project to test the accuracy of weather stations that includes its IoT platform in comparison with the professional station of AEMET. In order to do this, Libelium's engineering team installed two Plug & Sense! nodes in the Sustainable Urbanism Center of Zaragoza (Spain) requesting permission from AEMET to carry out the measurements in the same location and under the same conditions as its reference station.

This Libelium-EXM Weather Forecast Kit (Fig. 48.10) includes a Weather Station Maximet GMX600 connected to Libelium Plug&Sense!. The MaxiMet range of compact weather stations is designed and manufactured by Gill Instruments. MaxiMet products use reliable, high quality instruments to provide accurate meteorological information in a wide variety of applications. Temperature, Humidity, Pressure, Wind and Precipitation are the main parameters measured by this kit. All this data is sent to EXM platform. EXM's Smart Weather Forecast solution develops a profile for the particular microclimate the sensors are placed in. Combining it with 3rd party weather forecasts it creates a custom and highly accurate weather forecasting service for that designated location [22].



Fig. 48.10. Experiment Wi-Fi security web-page

48.4 Work related analysis

The benefits of IoT usage in agriculture are presents in [3-5, 18].

The issues of agri-IoT development are given in [5,8-10,16,17].

Communication technologies and protocols for agri-IoT are presented in [11-15].

The review of different applications of IoT for agriculture and ecomonitoring was made in [16,17,19-23].

The issues of agri-IoT security and cyber security are presented [11].

A few well-known universities including ALIOT project partners conduct research and implement education in the practical using IoT technologies. In particular, the following courses and programs have been considered as education with practical emphasis:

- School of Agriculture and Food Science of the University of Queensland, Australia [24];
- Precision and Automated Agriculture Lab, University of Missouri [25].

Listed courses and educational projects focuses on the Internet of Things in smart systems which can be used for monitoring and control of the artificial ecological systems;

And, of course, must be suggested more basic courses that can be used for deeper education on after-graduated basis or as whole-life-education approach:

- KTH University, Sweden: three MSc programs including IoT related topics in Information and Network Engineering [26];
- Newcastle University, United Kingdom: MSc Programme on Embedded Systems and Internet of Things (ES-IoT) MSc [27].

Conclusions and questions

The IoT agricultural applications are making it possible for ranchers and farmers to collect meaningful data. Large landowners and small farmers must understand the potential of IoT market for agriculture by installing smart technologies to increase competitiveness and sustainability in their productions. The demand for growing population can be successfully met if the ranchers as well as small farmers implement agricultural IoT solutions in a successful manner.

In order to better understand and assimilate the educational material that is presented in this section, we invite you to answer the following questions.

1. Is Internet of Things (IoT) the future of agriculture?
2. What are the IoT sensors useful in Sensor Fusion in agriculture Application?
3. Is the range of Internet of Things capabilities including drones and sensor nets?
4. How we could manage huge data from different IoT sensors in agricultural Science?
5. What are the ways for using IoT in mechanization and automation in Precision Agriculture?
6. What IoT collects in greenhouses applications?
7. What impacts will the Internet of Things (IoT) have on Agriculture Sector?
8. How Safety issue might affect the Development and Implementation of the Internet of Things (IoT)?
9. How we can improve sharing and exchange of information on farm?

10. What is the best way to monitor varying plant's nutrient levels in hydroponics in "real time"?
11. Which sensor measure the pressure relative to atmospheric pressure?
12. How many and what are the parts that are present in the accelerometer sensor?
13. What is ESP8266 and how it can help in IoT applications for Artificial Ecosystems?
14. Which sensors measure the moisture level using humidity?
15. Which proximity sensor detects positioning of an object?
16. How can be used the hyperspectral remote sensing for agricultural applications?
17. A sensor uses which network?
18. Does IOT gateway provide security for the network?
19. Which challenge comes when we use many devices on the same network?
20. How much wireless range is necessary for Iot applications?
21. Where is the power source coming from?
22. What type of sensors are necessary, and how will they be interfaced?
23. What is Bluetooth Low Energy (BLE) Protocol for Internet of Things (IoT)?
24. What is ZigBee Protocol for Internet of Things (IoT)?
25. What are some interesting internet of things (IoT) projects in agriculture?
26. Are digital technologies the future of Agriculture?

References

1. Internet of Things (IoT), <http://www.cisco.com/web/solutions/trends/iot/overview.html>
2. Stage 1 - Introduction to the Internet of Things: What, Why and How, <http://www.codeproject.com/Articles/832492/Stage-Introduction-to-the-Internet-of-Things>
3. D. Pimentel, B. Berger, D. Filiberto, M. Newton, B. Wolfe, E. Karabinakis, S. Clark, E. Poon, E. Abbett, S. Nandagopal, "Water resources: agricultural and environmental issues", BioScience, vol. 54, no. 10, pp. 909-918, 2004
4. J. Zhao, J. Zhang, Y. Feng, J. Guo, "The study and application of the

IOT technology in agriculture", 2010 3rd International Conference on Computer Science and Information Technology, pp. 462-465, 2010.

5. A. Elsts, R. Balass, J. Judvaitis, R. Zviedris, G. Strazdins, A. Mednis, L. Selavo, "SADmote: A Robust and Cost-Effective Device for Environmental Monitoring", ARCS LNCS, vol. 7179, pp. 225-237, 2012

6. S. Ivanov, K. Bhargava, W. Donnelly, "Precision Farming: Sensor Analytics", IEEE intelligent Systems, vol. 30, no. 4, pp. 76-80, July-Aug. 2015.

7. M. Ammadudin, A. Mansour, D. Le Jeune, E. H. M. Aggoune, M. Ayaz, "UAV routing protocol for crop health management", 2016 24th European Signal Processing Conference (EUSIPCO), pp. 1818-1822, 2016.

8. P. Lottes, R. Khanna, J. Pfeifer, R. Siegwart, C. Stachniss, "UAV-based crop and weed classification for smart farming", 2017 IEEE International Conference on Robotics and Automation (ICRA), pp. 3024-3031, 2017

9. C. Park, J. Liu, P. H. Chou, "Eco: an Ultra-Compact Low-Power Wireless Sensor Node for Real-Time Motion Monitoring", IPSN Fourth International Symposium on Information Processing in Sensor Networks, pp. 398-403, 2005

10. K. O. Flores, I. M. Butaslac, J. E. M. Gonzales, S. M. G. Dumlao, R. S. J. Reyes, "Precision agriculture monitoring system using wireless sensor network and Raspberry Pi local server", 2016 IEEE Region 10 Conference (TENCON), pp. 3018-3021, 2016

11. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, "Internet of Things: A Survey on Enabling Technologies Protocols and Applications" in IEEE Communications Surveys & Tutorials, Fourthquarter, vol. 17, no. 4, pp. 2347-2376, 2015.

12. S. Dementyev, S. Hodges, and J.-S. Taylor, "Power Consumption Analysis of Bluetooth Low Energy, ZigBee and ANT Sensor Nodes in a Cyclic Sleep Scenario", International Wireless Symposium, 2013, pp. 1-4.

13. A. Makarenko, A. Parfenova, and S. Mogilny "Wireless technologies of data transfer Wi-Fi, Bluetooth and ZigBee" Bulletin of the National Technical University of Ukraine "KPI" Series - Radio Engineering. Radio Apparatus Building, 41: 171-181, 2010

14. L. Šťastný, L. Franek, P. Fiedler "Wireless communications in smart metering", 12th IFAC Conference on Programmable Devices and Embedded Systems, 2013, pp. 330-335

15. A. Ouadjaout, N. Lasla, M. Bagaa, M. Doudou, C. Zizoua, M. Amine Kafi, A. Derhab, D. Djenouri, N. Badache, "DZ50: Energy-Efficient Wireless Sensor Mote Platform for Low Data Rate Applications", 5th International Conference on Emerging Ubiquitous Systems and Pervasive Networks (EUSPN), 2014.

16. A. Khattab, A. Abdelgawad, K. Yelmarthi, "Design and implementation of a cloud-based IoT scheme for precision agriculture", 28th International Conference on Microelectronics (ICM), pp. 201-204, 2016

17. Y. Liu, C. Zhang, P. Zhu, "The temperature humidity monitoring system of soil based on wireless sensor networks", 2011 International Conference on Electric Information and Control Engineering, pp. 1850-1853, 2011.

18. O. Georgiou, U. Raza, "Low Power Wide Area Network Analysis: Can LoRa Scale?", IEEE Wireless Communications Letters, vol. 6, no. 2, pp. 162-165, April 2017.

19. P. Kumar, S. R. N. Reddy, "Design and development of M3SS: A Soil Sensor Node for precision agriculture", 2016 International Conference on Recent Advances and Innovations in Engineering (ICRAIE), pp. 1-10, 2016

20. Y. Kim, R. G. Evans, W. M. Iversen, "Remote sensing and control of an irrigation system using a distributed wireless sensor network", IEEE transactions on instrumentation and measurement, vol. 57, no. 7, pp. 1379-1387, 2008

21. J. Gutiérrez, J. F. Villa-Medina, A. Nieto-Garibay, M. A. Porta-Gandara, "Automated Irrigation System Using a Wireless Sensor Network and GPRS Module", IEEE Transactions on Instrumentation and Measurement, vol. 63, no. 1, pp. 166-176, Jan. 2014.

22. I. F. Akyildiz, T. Melodia, K. R. Chowdury, "Wireless multimedia sensor networks: A survey", IEEE Wireless Communications, vol. 14, no. 6, pp. 32-39, December 2007.

23. Huan Zhan, Hui Wang, Chen Li, Caiyan Wan, "The soil moisture sensor based on soil dielectric property", Personal and Ubiquitous Computing, vol. 21, no. 1, pp. 67-74, 2016

24. Bryceson K. P., Borrero A. N., Gunasekera K. Internet Of Things (IoT)–Smart Agriculture Education At The University Of Queensland //Proceedings of EDULEARN16 Conference. – 2016. – C. 8036-8044.

25. Course number: AG_S_M 4160 (3 credits)
(<http://faculty.missouri.edu/zhoujianf/4160.html>)

26. MSc Programme in Information and Network Engineering [<https://www.kth.se/en/studies/master/information-and-network-engineering/master-s-programme-in-information-and-network-engineering-1.673817>]

27. MSc Programmes to Embedded Systems and Internet of Things [<https://www.ncl.ac.uk/postgraduate/courses/degrees/embedded-systems-internet-of-things-msc/relateddegrees.html>]

49. IOT BASED WATER QUALITY MONITORING SYSTEM

DrS., Prof. I. S. Skarga-Bandurova,
Ph.D. student Y. O. Kritska (V. Dahl EUNU)

Contents

Abbreviations	630
49.1 IoT based Water Quality Monitoring System: Basic framework	632
49.1.1 WQMS: Purposes, strategies, challenges	633
49.1.2 IoT based WQMS: Architecture and components.....	633
49.2 Parameters and data management in IoT WQMS	639
49.2.1 Key parameters and challenges in IoT water monitoring system	639
49.2.2 The management of sensor data in real-time	644
49.2.3 Water quality real-time data acquisition, aggregation, and analysis techniques	645
49.3. IoT WQMS evolution: from collecting data and data visualization to real-time predictive analytics	647
49.4 Case study.....	649
49.4.1 Defining WQMS goals	650
49.4.2 Designing a basic configuration of water monitoring stations	654
49.4.3 Construction of immersion-type device for water quality monitoring	656
49.5 Work related analysis	665
Conclusions and questions.....	667
References	668

Abbreviations

AP – Access Point

BOD – Biochemical Oxygen Consumption

COD – Chemical Oxygen Demand

CS – Compressive Sensing

DO – Dissolved Oxygen

DOC/TOC – Dissolved Organic Carbon / Total Organic Carbon

EC – Electrical Conductivity

GPRS – General Packet Radio Service

GSM – Global System for Mobile Communications

GW – Gateway

IaaS – Infrastructure as a Service

i.i.d. – independently and identically distributed

IoT – Internet of Things

ISFET – Ion-Sensitive Field-Effect Transistor

TOC – Total Organic Carbon

ORP – Oxidation Reduction Potentials

PLC – Power Line Control

SMS – Short Message Service

RFID – Radio Frequency Identification

WSN – Wireless Sensor Network

WQMS – Water Quality Monitoring System

PART 49. IoT BASED WATER QUALITY MONITORING SYSTEM

Development and implementation of information technology, in particular the Internet of Things (IoT), has opened the new horizons in environmental monitoring. Monitoring of water bodies covers the observation and assessment of the ecological status of various aquatic biological systems located on the earth's surface: rivers, lakes, transitional or coastal waters, artificial or substantially modified water bodies. A feature of modern monitoring is the extensive use of various instruments, sensors and communication infrastructures capable of transmitting and processing data in real-time. At the same time, a data collection system with low energy costs and the ability to simultaneously service a large number of IoT devices are necessary for efficient collection and processing of data on end nodes of information systems based on IoT. The inconsistency and inconsistency in the work of various monitoring subsystems greatly complicate the actual assessment of the status of water bodies and the ability to respond to their changes.

The module aims to create a knowledge base for multidisciplinary research on IoT systems and to provide prerequisites for practical use of these devices for industrial and municipal water monitoring. The study will expand the current research on IoT sensors for environmental monitoring and analytical methods for different IoT based systems for water monitoring applications.

The chapter addresses perspectives and challenges during developing IoT-based system for water quality monitoring and includes the following tasks:

- Parameters that are measured for all types of water objects;
- Data collection tools and coexistence possibilities of various IoT systems involved in the control of water objects;
- Development of models for simultaneous processing of large volumes of heterogeneous information from massive IoT devices.
- Development of proprietary IoT-system: device, hardware and software tools, a dashboard for on-line monitoring water objects;
- IoT water resource management: water quality real-time data acquisition, aggregation, and analysis

- Application of data management systems for analysis of large datasets.
- Explore the state of surface water in Ukraine, the influence of seasonal fluctuations, weather and industrial infrastructures on the parameters of water quality.

The technology is primarily targeting the following water-based sectors, although not limited by them: Environmental monitoring (Open water bodies in ecologically sensitive areas; Water reservoirs; Rivers, lakes; Wastewater monitoring, Groundwater monitoring); Aquaculture (Extensive, semi-intensive aquaculture farms; Land-based aquaculture; Controlled environment aquaculture).

At the end of the module, the successful student will be able to:

1. Explain and discuss the basic concepts and architecture of IoT water quality monitoring systems (WQMS)
2. Compare the different approaches and methods for collecting, aggregating and analyzing water quality data in real-time
3. Perform adjustment of sensors and configure ad-hoc IoT water monitoring solution
4. Explain the main parameters and stages of constructing integrated and block solutions in water monitoring tasks
5. Perform the fusion of sensors for remote water monitoring applications
6. Analyze data from IoT sensors, build reporting and water quality prediction algorithms
7. Create own IoT WQMS for industrial or municipal water data.

49.1 IoT based Water Quality Monitoring System: Basic framework

Water quality monitoring is an important and hot research subject because water is essential to the health and well-being of both people and the environment. Monitoring is the systematic and routine collection of data at set locations and at regular intervals to provide data which may be used to define current conditions, establish trends, etc. Main objectives of online water quality monitoring include measurement of critical water parameters to identify pollutants and provide early warning identification of hazards. Also, the monitoring

system provides real-time analysis of data collected and suggest suitable remedial measures.

49.1.1 WQMS: Purposes, strategies, challenges

To date, pollution of the water basin by the dumps of industrial enterprises is taking on alarming proportions. The situation is complicated by the lack of modern means of observation, monitoring and rapid response to changes in the state of water basins. One of the most difficult sites for monitoring is the river basins. A solution to the problem of ensuring the rational use of water resources and protection of the natural environment is the development and implementation of new approaches to water resources control and management. In this direction, the team of ALIOT project was involved in interdisciplinary research and development of a water quality monitoring system (WQMS) based on the IoT together with the real-time analytical software system using varies distributed sensors. There are several benefits of IoT in WQMS closely related to base paradigm of combination and utilization of new models of data storage, management and processing. The integration of different technologies in IoT assists in improving and developing water control programs to reduce the effect of water contamination. New solutions to the data transmission, storage and processing by IoT-cloud combination enables to better understand the sources of different water pollutants, effects of water control policies, and exposure of various substances in the water sources.

The proposed solution implements integrated water resources management based on the basin approach, providing an assessment of the individual characteristics of each section of the water body; improvement of the system for monitoring the aquatic environment - the state of surface and groundwater; constant observation; survey and determine the state of river basins; monitoring compliance with standards and discharge standards.

49.1.2 IoT based WQMS: Architecture and components

There are several approaches to development WQMS based on different architectures. In [1] six-layered architecture has been proposed

combining Web services, RFID and WSN whereas in [2], five-layer architecture has been suggested based on the telecommunication management network. Three layers can represent the most straightforward system based on IoT, as shown in Figure 49.1.

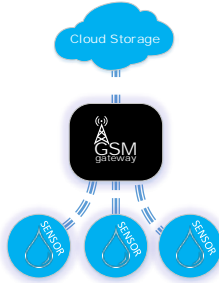


Fig. 49.1 – The simplified architecture of IoT based WQMS

The bottom layer includes the sensing equipment for information acquisition; the middle layer is the network for data transmission, while the top layer is designed for applications and middleware. In this chapter, we will focus on extended WQMS architecture suitable for IoT infrastructure from different domains. The overall system architecture of WQMS based on IoT is illustrated in Fig. 49.2.

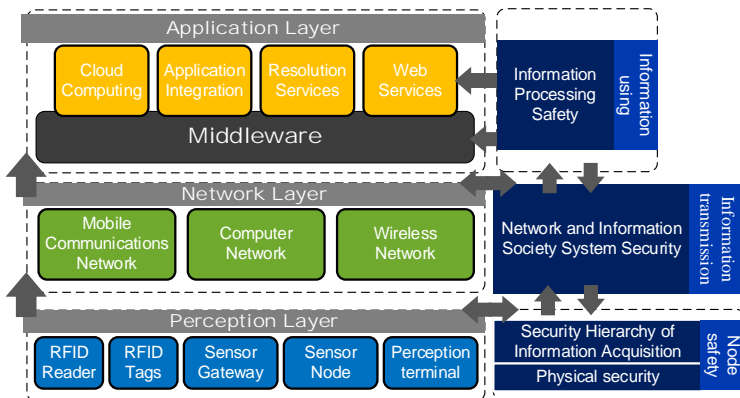


Fig. 49.2 – IoT based WQMS components

Perception layer: The main purpose of the perception layer is to collect data for the IoT network including information acquisition, capture and object identification. This layer consists of sensors, perception terminals, different water quality monitoring devices, self-organized network, short-range wireless communication, low power routers and energy harvesting apps in case if they are applied to WQMS.

There are different types of sensors used widely to detect water quality in real-time. Their choice highly depends on the cost, efficiency and water quality attributes required to analysis. Table 49.1 summarizes information about the new generation of smart in-line multi-parameter water sensor probes for real-time continuous potable water monitoring. For example, kapta 3000 AC4 [3] has been developed to enhance the management and control in the drinking water distribution network. It provides the measuring chlorine, conductivity temperature, and pressure and costs some 3 700 euro whereas spectro::lyser [4] has a more extended range, can be used to monitor multiple parameters from one sensor, BOD, COD, TOC, DOC, turbidity, color, or measure various parameters directly using the same sensor including NO3, NO2, UV254 and color. It is operated via s::can terminals and s::can software and will cost around 12 500 euro. Another example of complex water quality sensors is Smart water solution from Libelium [5]. It can detect water contaminants and will cost about 5 800 euro. The new IoT based Smart Water Xtreme Monitoring Platform from Libelium includes set of sophisticated sensors applicable for fish farms management, chemical leakage detection, potable water monitoring, remote measurement of swimming pools, and monitoring seawater pollution.

Table 49.1 – Commercially available multi-parameter water sensors
(Adapted from [6])

Water quality parameters	Sensor	Use-case
Temperature, turbidity, dissolved ions, pressure, color, UV254, BOD, COD, TOC	Spectro::lyser	a wide range of apps [7]
Temperature, turbidity, dissolved oxygen (DO), pH, conductivity, phosphate, water level	SmartCoast	freshwater, transition

		al and coastal waters [8]
Temperature, pressure, conductivity, chlorine	Kapta 3000 AC4	drinking water [9]
Temperature, dissolved oxygen (DO), pH, conductivity, oxidation reduction potential (ORP)	Smart water Libelium	sea, rivers, lakes [10]
Turbidity, color, UV254	I::scan	drinking water [11]
Any specific biochemical sensor	Lab-on-chip	[12]

Network layer: The WQMS network layer performs transmission, managing, and processing data passed from the perception layer and includes computer networks, wireless networks, and mobile communication networks.

To choose a communication standard for IoT network the following questions are to be answered and the next key aspects should be taken into account:

- Range: Where your network will be deployed, in the disposal works, ponds or rivers, big lakes, etc.?

- Frequency: What penetration is necessary and how resistant to interference? In some cases, it is also important to know the setting depth.

- Data transfer rate: What bandwidth is required? How often is the data updated?

- Power supply: Do devices operate on mains or battery?

- Security: Are devices involved in mission-critical applications? There are different approaches based on the type and level of protection required by each application.

The question of how the elements of the Internet of Things communicate with each other is one of the most important during the network design. Follow the range of transmission the communication technology can be classified into two types, long range and short range (see Table 49.2).

Table 49.2 – Performance attributes of network technologies

Parameter	Long range			Short range			
	LoRa WAN	GSM	LTE	BLE	Wi-Fi	Wi-Fi HaLow	Zig Bee
Max distance	2-5 km (city), 45 km (out)	35 km	200 km	80 m	100 m	1 km	100m/ Mesh
Frequency	≤ 1 GHz	License 8-900 MHz	License 7-900 MHz	2.4 GHz	2.4GHz 5GHz	900 MHz	915 MHz 2,4 GHz
Data transfer rate	0,3-50 kbps	70kbps	1Mbps	1Mbps	7Gbps 802.11a c	50kbps-18Mb/s	250 kbps
Energy consumption	Low	Medium low	Medium low	Reduced	High	Reduced	Low
Sensor location	known	known	known	unknown	known	known	-
Standard	LoRa WAN	Rel. 13	Rel. 13	Bluetooth 4.0	IEEE 802.11	IEEE 802.11ah	IEEE 802.15.4

When the long-distance transmission is required, the 2G, 3G, 4G [13] with the GSM, GPRS protocols can be used. They have more power consumption and in some cases not adequate for running in the wireless sensor network (WSN). The short range protocols include Zigbee, 6LoWPAN, Radio Frequency Identification (RFID). The RFID uses an electronically programmed tag used to collect data [14] while 6LoWPAN is adapted and can be used over a variety of other networking media including Sub-1 GHz low-power RF, Bluetooth Smart, Power Line Control (PLC) and low-power Wi-Fi [15]. 6LoWPAN supports both star and mesh topology. Another advantage of 6LoWPAN is low cost and power consumption.

Zigbee is a wireless 1494 protocol that provides low cost, low power consumption and high security during communication. It supports star, mesh and tree topology [13]. LoRa (Low Power Wide Area Network) is another protocol applied in IoT which has low power

consumption, cost and high data rate. It uses the star topology. For these reasons, we suggest LoRa, 6LoWPAN, and Zigbee as the best choices for development WQMS.

Cloud layer: It is a solution for the storage, processing and management of heterogeneous data from different wireless devices. In some cases, it can be considered as a part of the application layer or be a separate layer between the network and application layer [16].

Application layer: This layer manages the applications used in WQMS. Specifically, it is adopted to construct a series of obligatory platforms and services for information processing, support, management, intelligent computing, middleware, etc. Data analysis area for IoT covers data gathering sharing, and exchange, intelligent processing, analysis algorithms used for data abstraction, semantic representation and cognitive analysis, data management, data privacy and security. It also can be useful in the orchestration of smart objects.

It should be mentioned that data analysis for IoT is a complex issue; hence this part should be separated from other aspects. Due to the amount and heterogeneity of data generated by smart objects, it is recommended to use Big Data technologies [17] that support processing of data that have volume, velocity and variety properties [10].

Security layer: The overall security requirement of the IoT based WQMS in all levels from data gathering to information processing and visualization is to guarantee the confidentiality, integrity, authenticity and instantaneity of data and information. It should be performed on all hierarchy levels and include physical security, security of information acquisition, security of data transmission as well as data processing.

Physical Security means that information acquisition nodes in the IoT would not be cheated, controlled or damaged. Security of information transmission means that system guarantees the confidentiality, integrity, authenticity and instantaneity of data and information in the transmission process; this mainly refers to the security of telecommunication network and corresponds to the security of transmission hierarchy in the IoT. Security of information processing covers the privacy, confidentiality, as well as safe storage of information, middleware safety, etc., and corresponds to the security of application layer in the IoT architecture (see Fig. 49.2).

49.2 Parameters and data management in IoT WQMS

The study of water quality is carried out in different areas:

- dumping sites for wastewater and storm sewage water in populated areas, agricultural complexes;
- places of wastewater discharge of individual enterprises, power plants, large industrial complexes;
- places of discharge of collector-drainage waters discharged from irrigated or drained lands;
- large and medium-sized rivers flowing into the sea, inland waters;
- boundaries of regions, territorial units, transboundary water bodies;
- in areas of water use and adjacent areas;
- places of spawning and concentration of valuable/rare species of the fauna of water bodies;
- places of development and transportation of minerals.

There are many parameters to detect the water quality, but monitoring all of them will increase the workload on IoT-system and thereby influence the quality of analysis.

49.2.1 Key parameters and challenges in IoT water monitoring system

Parameters that tend to be used to identify water quality include chemical, physical and biological properties.

The most common chemical factors measured in water are aluminum, ammonia and ammonium ions, suspended solids, hydrocarbons, biochemical oxygen consumption (BOD), taste, pH, total iron, total hardness, odor (without heating), calcium, carbonates, heavy metals (copper, lead, zinc), nickel, frothiness, petroleum products, nitrates, nitrites, chemical oxygen demand (COD), permanganate oxidation, anionic surfactants, transparency, dry residue, sulphates, dissolved oxygen (DO), sulfurous sulfide genus (sulfides), phenols, phosphate (polyphosphates, total P), chlorides, fluorides, chromates (total), chromaticity. The ability of the water to remove the impurities by itself is called oxidation-reduction potential (ORP), a high value of ORP represents the good quality of water.

The physical parameters of water are temperature, turbidity and conductivity. Turbidity indicates the opacity due to the microscopic materials dissolved in the solution. High temperature affects the amount of oxygen in the water and disturbing the water quality.

The biological factors affecting the water quality include the presence of bacteria, virus, algae and pesticides forms [18].

Table 49.3 provides a list of the most frequently measured water parameters and related measurement techniques.

Table 49.3 – Most commonly measured water parameters and associated sensing technologies [adapted from 19]

Parameter	Measurement technology
Aluminum and other metals	Colorimetry; Atomic absorption spectrometry
Antimony	Atomic absorption spectrometry
Ammonia and its ions	Colorimetry (Manual measurement; Nessler Reagent; Automated; Berthelot Reaction); Ion selective electrodes
Active Chlorine	Colorimetry; Membrane electrodes; Polarographic membranes; 3-electrode voltametric method
Conductivity	Conductivity cells; ring electrodes; nickel electrodes; Electrodes of titanium or noble metal
Dissolved oxygen	Membrane electrodes; 3-electrode voltometric method; optical sensors; manual or automated titer
Ions (NO ₃ ⁻ , NH ₄ ⁺)	Ion-selective electrodes; Manual or automated colorimetry
Ions (Cl ⁻)	Ion-selective electrodes; Manual or automated triterometry
ORP	Potentiometers; Electrodes of platinum or noble metal
pH	Titration with Sodium Hydroxide; proton selective glass-block electrodes, proton-selective metal oxides; Ion-sensitive field-effect transistors (ISFET)
Phosphates	Ion selective electrodes; Manual or automated colorimetry
Temperature	Thermistor
Total Organic Carbon (TOC)	UV-persulfate digestion with near infrared detection; Membrane conductometric detection of CO ₂

Turbidity	Optical sensors; Nephelometric light scattering method
-----------	--

There are three types of values, depending on the measured parameter. Some parameters have “upper” threshold, meaning that this value should not be exceeded. For example, the upper threshold value for phosphate concentration is 0.035 mg P/l. Some indicators will have “lower” target values, meaning that the measured indicator should not be lower than this target value. An example is dissolved oxygen in rivers, where a value of 9.5 mg/l is the lower threshold for waters with temperatures below 20° C. Finally, some parameters will be characterized by a “limit” which is the standard acceptable range for this parameter. For example, a conductivity limit of 500 to 700 $\mu\text{S} / \text{cm}$ may be acceptable for a particular lake, and a deviation from this limit may become a symptom of a quality problem that may require further investigation.

When it comes to water parameters, it should be mentioned another group as the quantity factors. The quantity factors are water level, water flow pressure, and velocity. In the case of the flood disaster, measuring and monitoring these parameters is vital, as it can give a prior alert to nearby residents to perform some action like evacuation, contingency planning and so forth. The ultrasonic sensors and flow sensors can be used to detect the velocity and identify the changes in water flow [20].

Going back to the physicochemical characteristics, the basic parameters being measured for all types of water objects (rivers, lakes, transitional waters, coastal waters, artificial and heavily modified surface waters, etc.) are:

- temperature conditions;
- transparency;
- oxygen saturation;
- salt meadow;
- oxidation;
- the concentration of nutrients.

About specific pollutants, they can be selected depending on the types of contaminants found in certain water bodies subject to control. In this case, the methods of sampling also depend on the type of object. For example, for rivers, sampling is carried out taking into account the following requirements:

1. predefined points and depths of selection;

2. the selection is carried out downstream of the flow, positioning at the desired depth upstream at the point of full mixing of the water (in the places of maximal storm flow, where streams are well mixed);

3. during the selection, it is necessary to take into account the daily cycle, seasonality, regime of the period (floods, fluctuations);

4. to ensure reliable results of instrumental control, it is necessary:

- to comply with the requirements of the purity of sampling dishes;
- observe all guidelines for separate sampling to eliminate the effects of components that interfere with each other;

- adhere to all instructions regarding the preservation of specific components of water through the flow of samples of oxidation-reduction, sorption, sedimentation, and biochemical processes caused by the microorganisms' vital activity.

For the sampling of water from lakes, it is necessary to follow the following recommendations:

1. apply the planned statistical selection, taking into account the historical chronology of the reservoir;

2. to take into account the faintness and significant heterogeneity of water in the horizontal direction (in depth) - due to thermal stratification, which may be the cause of photosynthesis in the surface area, the heating of water, the influence of bottom sediments, etc., internal drainage may appear in large deep reservoirs.

3. comply with item 4) of the sampling requirements for rivers.

For groundwater:

1. determine the depth of the horizon;

2. estimate the gradients of underground flows, the composition of underground rocks through which the horizon proceeds to determine the concentrations of impurities, different in composition from the aquifer;

3. take into account the possibility of several aquifers, especially if samples are taken at different depths;

4. to pump the well for 10-15 minutes before the selection to renew the water with the accumulated pollutant, ensuring a mandatory discharge of water during pumping - not less than 3-5 volumes of a column of water in the well.

For drinking, water supply networks:

1. when choosing a place of selection:

- do not use end sections of networks and areas with pipelines of small diameter (less than 1,2 cm);

- use areas with the turbulent flow (cranes near valves, bends);
- 2. to lower the water for renewal within 10-15 minutes;
- 3. the selection is carried out with a slow flow of flow and a complete overflow of sampling capacity.

Traditional methods for collecting data based on laboratory analysis methods are presented in Table. 49.4.

Table 49.4 – Data collection tools

Type of water	Data collection tools
Surface waters	<ul style="list-style-type: none"> - stationary stations; - mobile posts; - automated surveillance systems; - remote zoning systems (geoinformation systems, etc.); - certified stationary instrument laboratories.
Underground sources including drinking water	<ul style="list-style-type: none"> - a network of observation wells at the water intake and adjoining area; - a network of observation wells on the site of industrial facilities and adjoining territory; - certified stationary instrument laboratories.
Seas, oceans	<ul style="list-style-type: none"> - Stationary stations; - mobile posts; - remote zoning systems.
Sewage	<ul style="list-style-type: none"> - Stationary stations; - mobile posts; - automated surveillance systems; - certified instrumental laboratories.

Observations for surface water are made taking into account the hydrometric conditions and morphological objects of water systems, data on the availability of sources of pollution, volume and parameters of the composition of sewage.

For seawater and ocean waters, the boundaries of the monitoring network are determined depending on the physical and geographical

features of each sea/ocean, taking into account the distribution of pollutants and the hydro-meteorological regime.

With regard to advanced online monitoring tools, most of them are based on IoT technology and include a variety of devices, sensors (fiber-optic sensors, lab-on-chip, biosensors, EM-sensors, including microwaves, etc.), web platforms, cloud servers, control centers, and information processing.

49.2.2 The management of sensor data in real-time

Obviously, a variety of parameters, tools and data collection conditions necessitate the use of various IoT platforms that require special methods of data collection, transmission and processing. Moreover, in real life, the various tools, environments and platforms IoT must coexist with other types of IT.

Assuming that several IoT platforms can be used simultaneously to measure parameters from rivers, lakes, seas, groundwater, etc., there is bound to be a simultaneous processing of large volumes of heterogeneous information from massive IoT devices. An example of the coexistence of different IoT systems is shown in Fig. 49.3.

Under the circumstances, when each IoT platform has a typical structure consisting of a target device, a concentrator, and a fusion center, it is possible to develop a unified technology for processing and transmission. Thus the scheme in Fig. 49.1, each end device captures information according to its own purposes, the hub is responsible for collecting data from many devices and redirects it to the data fusion center. Finally, all data is transferred to the fusion centers that perform their processing, management, and analysis. In the middle point, the hubs can operate in different ways with respect to IoT platforms, for example, either as an access point (AP), or as a gateway (GW). The general task of the end node IoT is to send data to a particular node or merger center. The management of sensor data in real-time is difficult as the centralized or distributed approach is used to handle them. A hybrid approach with an efficient compression technology could be used to manage and efficiency filter the real-time data based on the necessity and to reduce the cost of transmission in the network layer. That why, the question of how to efficiently collect, store and transmit data from a large number of source nodes remains a problem.

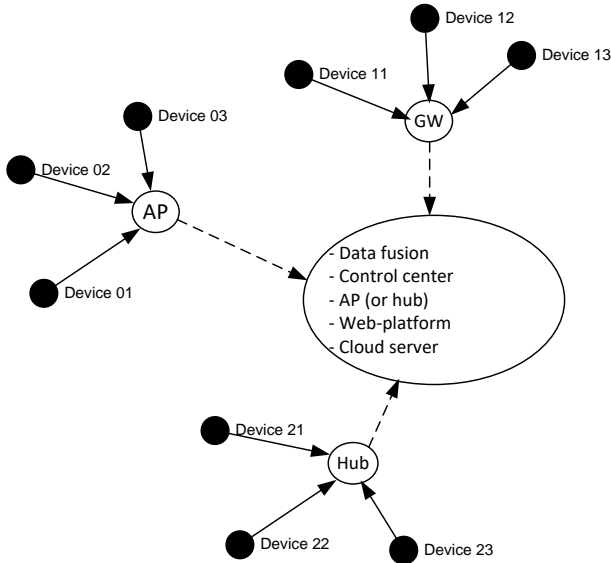


Fig.49.3 – Example of interaction of various IoT platforms (adapted from [21]).

49.2.3 Water quality real-time data acquisition, aggregation, and analysis techniques

To solve this problem it is possible to use Compressive Sensing (CS) models proposed in [21]. CS is a technology that allows a preliminary sampling of data at a rate lower than Nyquist's sampling rate [22, 23].

The theory of CS states that if the signal is diluted in the transform domain, then it can be reconstructed from a small set of linear measurements using simplified optimization algorithms. It is assumed that each node receives independently and identically distributed (i.i.d.) signals. In this case, compression measurement can be used to reduce the sampling rate without degrading the recovery performance effectively. Thus, the k -compressed signal can be described entirely by k nonzero components. In this case, x can be selected with a

diversifying matrix and a vector of measurement y can be obtained. The following model can explain the sampling process:

$$y = Ax + \delta,$$

where A denotes the matrix of measurement in the size $m \times n$, δ is the noise.

In the IoT networks, measurements y can be represented as:

$$y = [y_1, \dots, y_m]^T = \sum_{j=1}^n A_{i,j} x_j,$$

where y_m can be represented as a linear combination of a small-scale signal x_i .

Each node can calculate x_j by multiplying the corresponding element of the matrix $A_{i,j}$, which can be constructed by selecting records as i.i.d. implementations with a certain probability distribution [24].

Then, randomized values can be used for aggregation $A_{i,j} x_j$ in the center of the fusion. Thus, the y value becomes available in the data merge center.

Given that the network with n nodes at the location $\{p_i\}$, $i = 1, \dots, n$ monitors several events, we assume that the nodes $N_a(t)$ are in active mode, and $N_s(t)$ in hibernation in time t . Let x_i denotes the initial value for p_i . Then the dimension y_i of the odd node i can be represented as

$$y_i = \sum_{j=1}^n A_{j,i} x_j + \delta_i,$$

where $A_{i,j} = A_{i,j}$ - the effect of this event on the point of the sensor p_i , and δ_i is a random noise measurement of the zero mean. Here x is thinned, and $A_{i,j}$ is determined during deployment of the network.

Assume that the effect $A_{i,j} = 0$, if the distance from j to i is greater than the range of communication.

Then measure y_i can be defined as follows:

$$y_i = x_i + \sum_{j=1}^n A_{j,i} x_j + \delta_i.$$

Then, according to [21], for active nodes on the network we have:

$$y_a = MAx + \delta_a,$$

where A is a matrix $n \times n$, where (i,j) is the value of $A_{i,j}$, M is the matrix of measurements $m \times n$, which selects m lines of A corresponding to the active sensors, y_a and δ_a are respectively, the measurement vectors and noise in size $m \times 1$.

If some IoT devices on the network are more important than others, the data fusion center can take this value into account when reconfiguring the transmitted data by adding a weight vector to the base model.

The advantages of compression measurement models include the following: the number of specimens generated by each node can be greatly reduced without loss of recovery accuracy; which in turn can lead to a significant reduction in communications in the networks; the cost of computing on the nodes can also be reduced.

49.3. IoT WQMS evolution: from collecting data and data visualization to real-time predictive analytics

Data in itself is not terribly useful. To make them understandable and actionable additional work must be done. The WQMS based on IoT is highly dynamic, spatially expansive, and behaviorally heterogeneous. Things are getting more complicated due to environmental time series, in general, are complex and hard to model. They are fraught with highly non-stationary, highly non-linearity, with many changes in their dynamics and numerous outliers, anomalies, gaps, etc. For example, if we look at common water quality indicators (see Fig. 49.4) and calculate points for each parameter, one point every ~5-15 minutes gives us 30,000-100,000 points per year per signal. It is an immense amount of material.

These issues have opened a vast number of opportunities in expanding data mining, machine learning and other techniques. These techniques include a broad range of algorithms applicable in different domains and enable to find patterns and new insights from data.

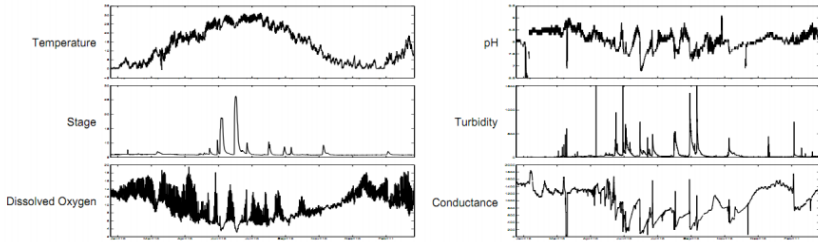


Fig. 49.4 – Examples of water time series data

Table 49.5 summarizes recent big data models utilized for water parameters. To understand what technique to choose and which algorithm is more appropriate for processing and decision-making on the data from the smart devices and things in IoT, please refer Chapters 5-8 in Volume 1. The comprehensive review on big data tools and technologies addressing the challenges of the water quality sector can be found in [25].

Table 49.5 – Big data models applied for water quality monitoring (adapted from [25])

Purpose and area of study	Big data model	Water parameters	Data-source	Case
Detection of Intentional Bacterial Spore Contamination	Real-time WQ sensor model	turbidity, pH, temp., TOC, conductivity	Deionized water	[8]
Detection and analysis of Trihalomethanes in drinking water	Pearson's coefficient Analysis Model	Temp., dissolved organic carbon, chloride	water treatment plants assessed from 2011-'13	[10]
Water quality monitoring	Fast fuzzy C-mean clustering	DO, CO ₃ , NH ₃ -N	ultra-large scale WSN	[11]
Spatial quality evaluation of drinking water	GIS and Ant-colony algorithm	chlorides, sulphates, total hardness	29 wells in China	[12]

Water quality monitoring with minimum supervision	Wireless System for WQ monitoring	pH, conductivity, temperature	Water quality monitoring sensors	[13]
To construct a novel water quality index and quality indicator	WQ Indicator Model	Physicochemical parameters and metal concentration	11 water sample stations located upstream	[14]
to evaluate the effect of water management	EEA 2001 Guidelines	NH ₄ ⁺ , NO ₂ ⁻ , NO ₃ ⁻	Historical data for the lagoon	[15]

49.4 Case study

In this paragraph, we discuss the key elements and milestones of a pilot project on the development and implementation of real-time WQMS in the IoT environment for surface water. The main stages of designing the online monitoring system for surface water are presented in the form of a series-parallel scheme (Fig. 49.5).

The design process includes the definition of the purpose; selection of target objects and locations for the location of online monitoring stations; designing of the base configuration of the monitoring station; real-time data access tools, data storage, processing, visualization, and analysis, etc.).

The procedures that provide system set up for the purpose, tasks and monitoring requirements can be attributed to the following steps. The justification for the need to control additional parameters; making changes to the structure and configuration of the base station, if there are other parameters; development of models and decision-making algorithms in non-emergency situations, such as emergency discharges, flooding, etc. development of systems and means of support for the adoption of operational decisions. The procedures below are described in more detail.

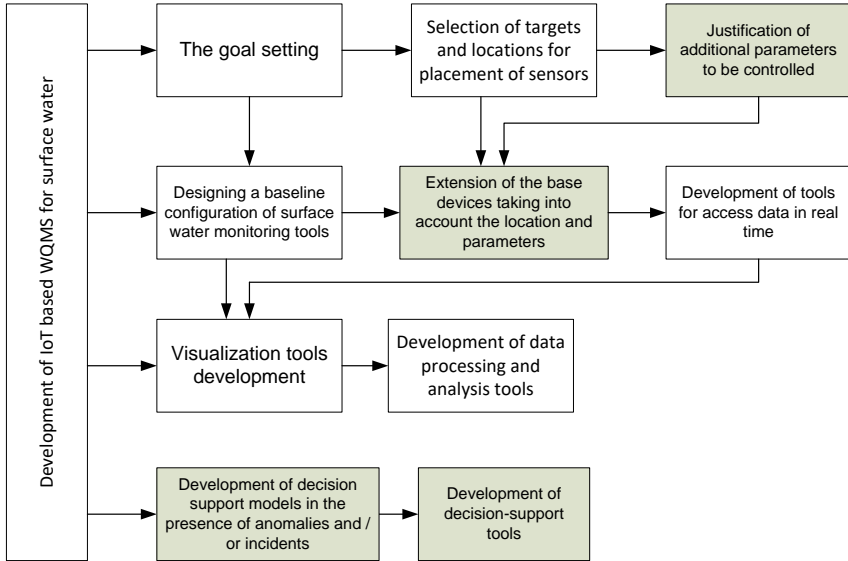


Fig. 49.5 – Designing IoT based WQMS for surface water

49.4.1 Defining WQMS goals

Depending on the customer and the current situation, the purpose of developing and implementing an online monitoring system can be:

- Identification of incidents of water pollution.
- Optimization of cleaning processes.
- Monitoring of threats and assessment of long-term trends in water quality due to natural changes and anthropogenic impact.

Each goal influences the choice of parameters that will be monitored by the system. At the same time, it is possible to allocate a group of parameters that can provide a basic level of water quality control and develop the basis for the formation of monitoring stations. Table 49.6 shows a list of basic options that can be useful for all applications for each of the three development goals.

Table 49.6 – Basic parameters of the surface water quality control system

Parameter	Description
pH	<p>The pH of the water is one of the most important parameters when investigating water quality, as it is a measure of the concentration of hydrogen ions and measures how basic or acidic the water is.</p> <p>The pH of the water directly influences living resources and may affect the toxicity and solubility of chemicals, heavy metals and other pollutants such as phosphorus and other nutrients.</p> <ul style="list-style-type: none"> - Changes in pH can mean an increase in dissolved nutrients, which will lead to an increase in plant growth and, ultimately, to eutrophic states. - Fluctuations in pH levels are often caused by anthropogenic sources of pollution, such as fossil fuel combustion, smelting and extraction, agricultural runoff, as well as waste and industrial emissions. - pH below 5.0 significantly impairs the livelihoods of many species of fish, and when the level reaches the mark below 4.0 leads to the mass death.
Temperature	<p>The degree of thermal energy in water. All processes of life directly depend on the temperature of the reservoir, the higher the temperature, the faster all processes occur therefore the temperature parameter is obligatory in the initial definition.</p> <ul style="list-style-type: none"> - Affects chemical equilibrium and kinetics. - May indicate the mixing of water from different sources (for example, the merging of sewage with river water). - The temperature sensor should be combined with water quality sensors that measure temperature-dependent parameters (for example, pH, specific electrical conductivity), which makes it possible to compensate for the temperature to measure these parameters.
DO	<p>Measurement of dissolved oxygen (DO) is important for aquaculture centers since this parameter determines</p>

	<p>whether or not a species can survive in the said water source. DO is consumed for the oxidation of organic substances, the processes of respiration of aquatic organisms and the oxidation of organic compounds during their vital activity, as well as chemical oxidation processes - nitrates, nitrites, ammonium nitrogen, iron, manganese, sulfides, etc.</p> <ul style="list-style-type: none"> - A deviation from the norm of this indicator may mean that the excess content of pollutants (nitrites, ammonium nitrogen, iron, manganese, sulfides, etc.) or existing oil products or surfactants, heavy metals are present in the water. They paralyze the metabolic processes oxygen for living things. As a result, they die off and form bottom sediments, which eventually rot. - When reducing the content of dissolved oxygen to a critical indicator of less than 4 mg O/l, there is a significant decrease in the population of aquatic fauna, in particular, it can lead to fish freeze. - Low DO concentrations can adversely affect the oxidation potential and efficiency of some refining processes, although mixing during transfer can lead to a near-saturated DO concentration. - The placement of the sensor DO may affect the measurement results. Since sampling from the surface or not deeply immersed in clear, warm and sunny weather can give overestimated oxygen levels, which are not true and are associated with the intensive development of algae, it is necessary to follow the standards and rules for sampling according to KND 211.1.0.009-94 "Hydrosphere . Sampling ... ", DSTU ISO 5667-2-2003, DSTU ISO 5667-3-2001, DSTU ISO 5667-10-2005" Water quality. Sampling ... ", Directive 2000/60 / EC.
EC	<p>Electrical conductivity (EC) is a measure of the ionic strength of a solution, which characterizes the level of the content of mineral salts in water. Conductivity gives an indication of the amount of impurities in the water, the cleaner the water, the less conductive it is.</p>

	<ul style="list-style-type: none"> - The value of conductivity is influenced not only by calcium and magnesium, but also by gases dissolved in water (CO₂), organic matter, ions of other metals, etc. - May indicate the presence of mineral salts in the water or the ingress of salt water. - May increase due to overflow of sanitary sewage, combined sewer networks and wastewater discharges. - May interfere with the osmotic balance of aquatic organisms. - Measurement of the total mineralization (salinity) in the main of the water purification system, to its purification and after, allows you to make an assessment of the effectiveness of the purification system.
ORP	<p>ORP is a measure of degree to which a substance is capable of oxidizing or reducing another substance.</p> <ul style="list-style-type: none"> - Measurement of the potential flow of electrons between deoxidizers and oxidizers, which characterizes the oxidizing or reducing power of the solution. - low ORP may reduce the efficiency of oxidation processes. - May serve as an indicator of natural processes in spring water (for example, circulation). - OOP may indicate the presence of a renewable substance in water

To meet the project objectives more effectively, it is necessary to use sensors for monitoring additional parameters.

1.1 Additional parameters for identifying pollution incidents.

Depending on the type of pollutant, in addition to the parameters listed in table 49.6, the following parameters can be used:

For inorganic industrial pollutants:

- Toxicity. Toxicity is a general indication of the presence of a potentially toxic substance and thus can detect the presence of toxic industrial chemicals. Toxicity monitors differ greatly in their response to various chemicals.

- Spectral absorption. The spectral absorption measurements can be used to estimate the concentrations of iron and manganese in water.

For organic industrial chemicals:

- Toxicity.
- Spectral absorption.
- Dissolved Organic Carbon/Total Organic Carbon (DOC/ TOC)

For wastewater:

- Toxicity.
- Ammonium.
- Nitrates and nitrites.
- Orthophosphate.
- Turbidity. An increase in turbidity may indicate an increase in the concentration of suspensions and microorganisms that may be present in the wastewater.

1.2 Additional parameters for optimizing water treatment processes

In addition to the parameters listed in table 49.6 to optimize conventional water treatment processes can be used:

- Spectral absorption.
- DOC / TOC.
- Photosynthetic pigments. The increase in photosynthetic pigments is a major indicator of increased algae activity.
- Turbidity can be used to determine the dose of coagulant needed to achieve water quality targets for wastewater.
- Ammonia. Changing the concentration of ammonia in water can influence the decisions on the addition of chlorine to disinfect drinking water.

1.3 Additional parameters for monitoring threats to long-term water quality

To control the waters in the long term to the indicators in table 49.6 and items 1.1, 1.2 other parameters can be added.

49.4.2 Designing a basic configuration of water monitoring stations

After selecting the monitored parameters and locations, the development stage of water quality monitoring stations begins. Each device consists of sensors used to measure selected parameters and auxiliary equipment necessary to provide power to the station, transmit data to the network and protect against unwanted interventions and environmental influences.

In fact, the design of the station will depend on:

- Parameters to be monitored at each site;
- Location;
- Practical considerations for installing and maintaining the station on site.

When designing online monitoring stations, it is necessary to solve a number of issues related to the implementation of the following set of required components:

- Devices and/or sensors for measuring the selected parameters;
- The method of placement of sensors that will be constantly in contact with water (see Fig. 49.5);
- Power supply sources;
- Data transmission facilities;
- Housing for installation and protection of measuring instruments and accessories;
- Tools to protect the station from possible interference and the environment.

Several technologies are available to measure a given parameter; in relation to online monitoring stations, one can use immersion of sensors and / or water injection into sensors located in the current cell.

For the system being developed, the first approach is used - immersing the devices directly in water, this ensures that the sensors measure the quality of water with minimal disruption without changing samples.

This sampling method is useful for parameters such as soluble oxygen, which may vary due to mixing and transport to the measurement site. A sensor designed for use in this way must be equipped with a protective housing and means for periodically cleaning the measuring surface (wipers, brushes or compressed air).

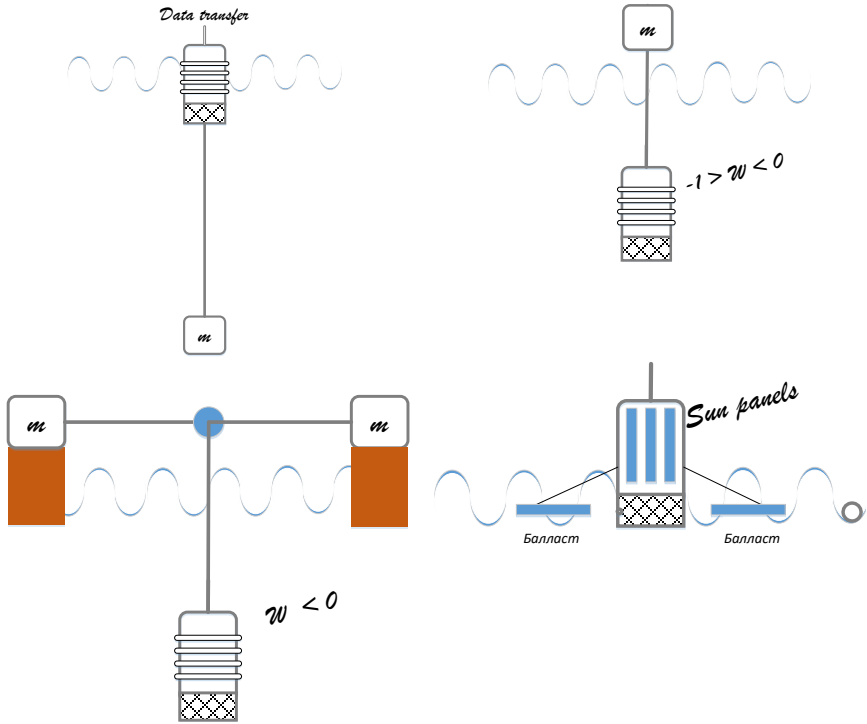


Fig. 49.5 – Examples of immersing the devices directly in water

49.4.3 Construction of immersion-type device for water quality monitoring

The underwater WQM device is designed as a tube (external capsule) and module stack with equipment supporting structure (internal capsule). The external capsule is hermetically sealed (See Fig. 49.6).



Fig. 49.6 – Assembly blueprint of the immersion device for WQMS

The basic idea is to place the capsule directly into the water and obtain data using preplanned sensors activation schedule. All instrumentation equipment is placed on the module stack inside the tube.

An electrical part of water quality monitoring device consists of three sub-modules they are sensor part, controller and battery part, and communication part as illustrated in Fig. 49.7.

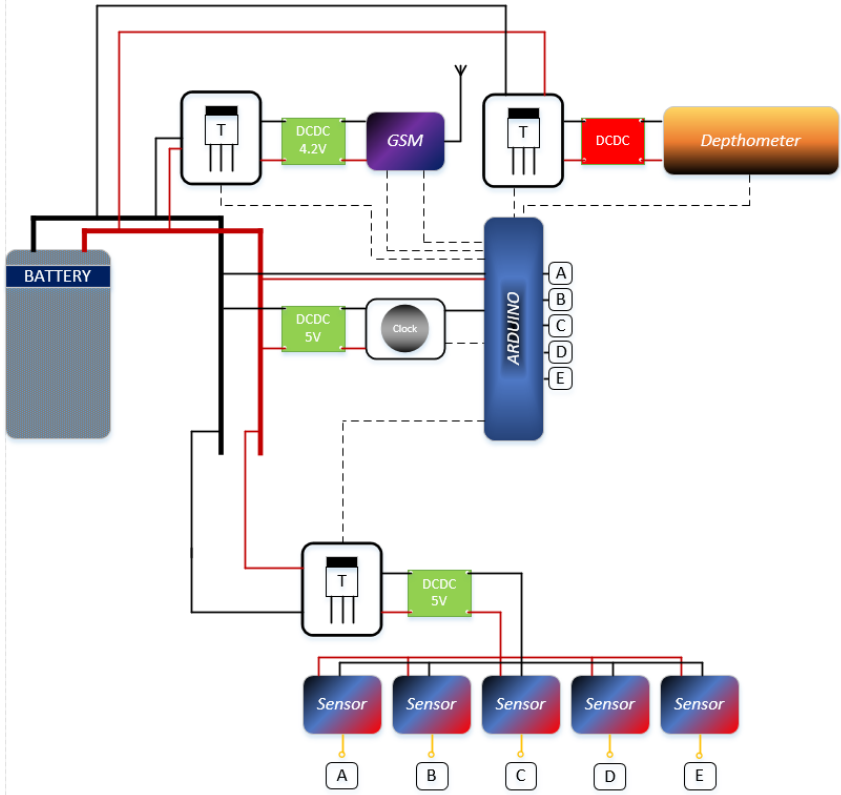


Fig. 49.7 – Electrical connections of the water quality monitoring device

Sensor part: The key parameters monitored in this system are pH, conductivity, turbidity, dissolved oxygen, and temperature (see table 49.7). These sensors supplied complete with open-source code and detailed tutorials and are suitable for different water projects.

Sensors are placed in the bottom part of the internal capsule and can be widely applied in many water quality applications, such as aquaculture, surface water monitoring and so on.

Table 49.7 – Sensors used in water quality monitoring device

Sensor	Cost, \$
Gravity: Analog pH Sensor / Meter Pro Kit For Arduino	57,00
Gravity: Analog Electrical Conductivity Sensor / Meter For Arduino	70,00
Gravity: Analog Dissolved Oxygen Sensor / Meter Kit For Arduino	169,00
Gravity: Analog ORP Sensor Meter For Arduino	90,00
Gravity: Analog Signal Isolator	20

The sensor parameters are measured with preplanned sequence. The data from the sensors are sent to the cloud using the controller and displayed on the dashboard. If the value exceeds the threshold SMS are sent from cloud to the user smartphone. The flow chart for sensor data update is presented in fig. 49.8.

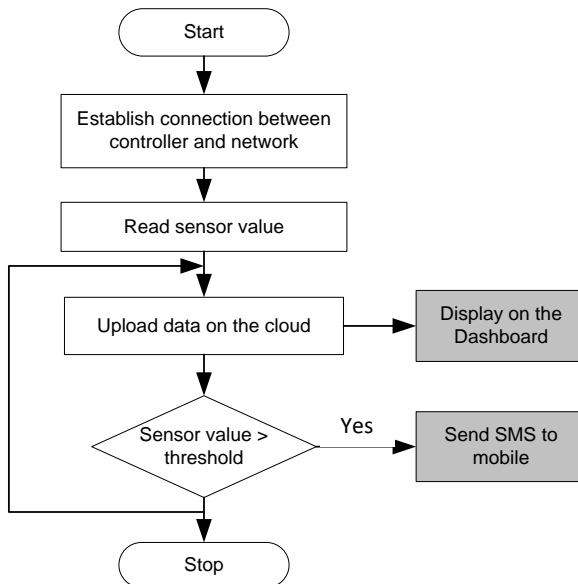


Fig. 49.8 – Flow chart for sensor data update

Controller and battery part: For water quality monitoring different controllers can be used. Though each controller has its own features most of them equipped with an external GPRS / Wi-Fi module for

connectivity to the data storage or application. For study purposes, Arduino controller can be used. All sensor kits from Table 49.7 are compatible with Arduino microcontroller.

The major constraint for WQMS based on IoT is power consumption because in this and many other designs it will operate on batteries. In [26] authors compared the power consumption of standalone microcontroller with Zigbee, Bluetooth Low Energy (BLE) modules and controller with inbuilt Wi-Fi device. As a result, they confirm that Wi-Fi inbuilt device consumes less power compared to standalone microcontrollers.

Communication part: For applications such as water quality monitoring based on IoT, data communication can be performed in two stages. One is the communication between sensors and the controller and other is the communication between controller and application [26]. For communication between sensor to controller and from the controller to cloud data storage a wireless technology is used.

Different techniques can be used in each of the communication scenarios. Table 49.8 shows the frequently used wireless communication technology for information transfer.

Table 49.8 Wireless communication technology used for different scenarios (Adapted from [27])

Communication	Technology used
Sensors and controller	Zigbee UART
Controller and application	GSM/GPRS Ethernet LAN IoT (using external WiFi Module) IoT (using inbuilt WiFi Module) LCD, Alarm, Actuators
Controller and data storage	3G and Internet (SMS about the water quality) External Wi-Fi module connected to the controller, which enables the controller to get connected to the nearest Wi-Fi hotspot and to the Internet cloud

Possible protocols for communication between sensor nodes and controller are Zigbee, Blue tooth, BLE and LoRa. According to [28],

Wi-Fi is not suitable for communication between sensor nodes and the controller because the power dissipation is high.

49.4.4 Development of tools for processing and visualizing information

In order to achieve the chosen design goals, the data received from the monitoring stations should be converted into useful information. Productive information is produced by analyzing the data along with providing relevant results to the end user in an accessible and understandable form. To achieve these goals, the information management system should provide the capabilities of storing, accessing, analyzing, reporting and visualizing data.

Moreover, the methods of analysis and visualization will be different for each project goal.

4.1 Analysis and visualization to identify pollution incidents

Two methods of data processing can be used to support the detection of contamination incidents: the analysis of threshold values and automated detection systems for anomalies. The analysis of threshold values is the easiest approach to detecting contamination. The thresholds are based on the normal variability of each parameter in each location, thus exceeding the threshold indicates an anomaly of water quality.

Thresholds can be established using a statistical analysis of historical data collected during the representative period. Thresholds are usually set in such a way as to avoid excessive invalid alerts while maintaining sufficient sensitivity to detect contamination incidents. If there are significant water changes, such as seasonal changes, for each period characterized by a significant difference in water quality, basic and unique thresholds can be set.

Automated detection systems use software algorithms that can usually analyze the behavior of several parameters measured at one monitoring station to detect anomalies.

To support real-time data analysis, water quality indicators should be updated regularly. In this case, it is useful to design dashboards. A dashboard is a graphical user interface that combines and displays data from various sources spatially and graphically.

The examples of the dashboard prototype and implementation are shown in Fig. 49.9 and 49.10. Available options include:

- Charts (Line chart, double axis, scatter ploy, histogram, bars);
- Metric parameters visualization (average, maximum, minimum, sum, count, last value);
- Map (location of device);
- Table (last value, historical value);
- Indicator panel (gauge, on/off display);
- Control panel (switch, slider).

Complementary to the main ones, additional information resources that support the interpretation of water quality data, such as weather data, may be included to the panel design.

The graph is based on the received data streams and plotted automatically. When anomalies are detected, the WQMS should generate alerts about changes in water quality.

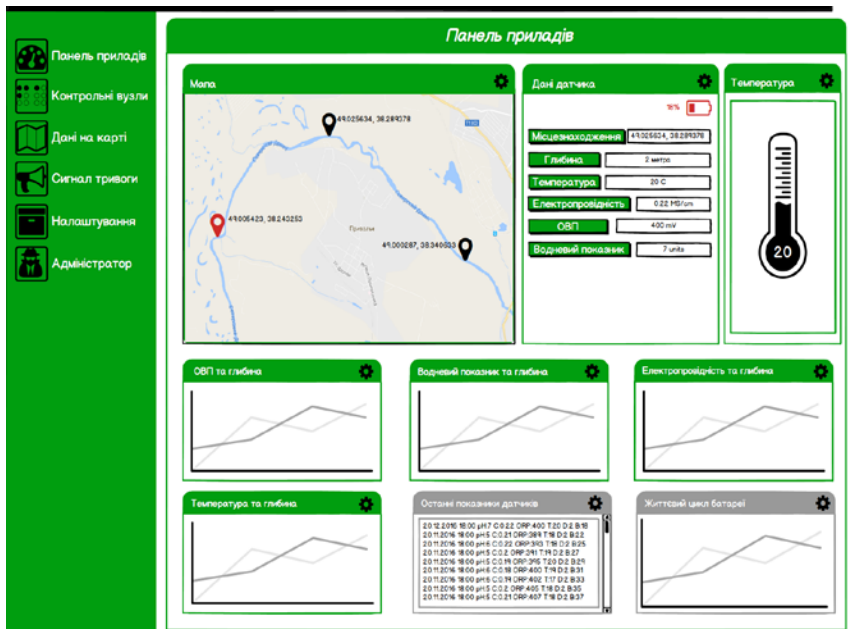


Fig. 49.9 – An example of WQMS dashboard prototype

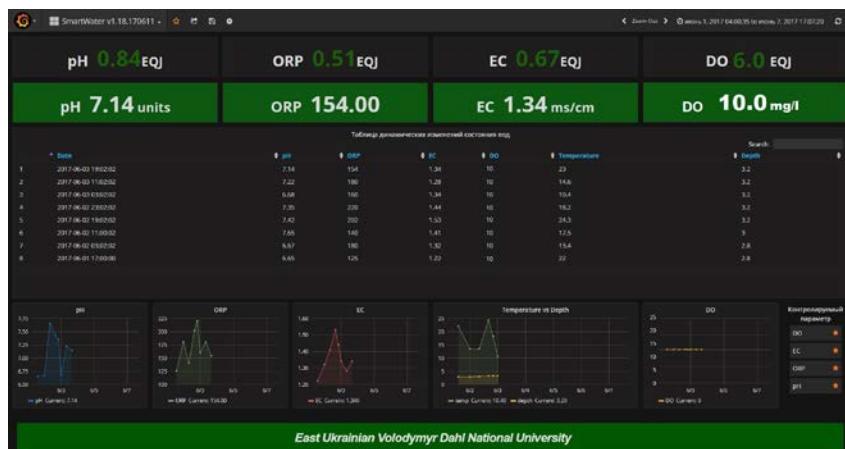


Fig. 49.10 – Graphical representation of parameters on the dashboard

Since operators may not have the time to view new data frequently, warning must be provided through special messages on the dashboard screen or text messages on a smartphone connected to the system. Notifications must include time, device / metering station location, parameter and its current value.

4.2 Analysis and visualization to optimize cleaning processes

The decision-making process for water purification from pollutants includes real-time data monitoring to detect changes in water quality. This requires a deep understanding of the relationship between the quality of water and the need for its adjustment.

Similarly, the task of detecting pollution incidents, to support the optimization of cleaning processes, can be used in two ways: the analysis of threshold values and the use of models to perform cleaning processes. The thresholds should be defined for each monitored parameter and each purge process. The approach of threshold values to optimize the purification processes involves real-time monitoring of parameters that affect the performance of the purification process and process setup, when the monitored metrics cross the previously defined thresholds. Since most processes affect multiple parameters, individual thresholds are generally not considered singly. In this case, a combination of statistical analysis of historical water quality data and knowledge of the effectiveness of the purification process can be used to establish thresholds.

In the simplest case, to help operators identify potentially significant changes in water quality, for the parameters crossing the thresholds (minimum or maximum), specified notification may be generated.

Threshold analysis is often displayed as time series graphs that show a moving window of recently measured values along with their minimum and maximum thresholds. Statistical analysis can be used to develop thresholds based on the typical variation of the water quality parameter over a period of time (for example, daily or weekly for highly variable parameters, monthly or seasonally for less variables). According to the recommendations [29], a five to ten percent safety factor should be used for thresholds, which gives operators time to study and respond to changes in water quality. The second, analytical approach involves the use of cleaning process models. All models can be classified as mechanical, statistical or knowledge models. Mechanical models include inputs and outputs to the main properties of processes and use empirically determined coefficients for calibrating the model for a specific purification installation. Statistical models are used when reliable mechanistic models are not available. The inputs are related to the results on the basis of statistical analysis of historical data. Knowledge-based models use methods such as machine learning and expert systems to describe complex systems, where there is a limited understanding of the specific principles governing the system. These models use knowledge and human experience to predict the state of the water in the future. The purification process models use proven data from the online monitoring system, current cleaning process parameters to determine the necessary steps to regulate the process, for example, chemical dosage of substances to support optimal purification.

4.3 Analysis and visualization for monitoring of threats to the long-term quality of water

The monitoring of the long-term threats to water quality is based on continuous analysis of data over several years to identify trends and ongoing changes in the baseline scenario. The information received from the monitoring system can help in developing strategies to respond to the deterioration of water quality. In the long run, a systematic analysis is performed to determine if the baseline for several parameters has been changed at a specific location where the metering station is located and how the baseline for this parameter has changed

in several places. These results can help to assess whether this change is widespread throughout surface water and water distribution or is isolated to a specific area.

49.5 Work related analysis

Online smart water quality has been proposed for several applications in literature for river and sea water monitoring [10, 30, 31], aquaculture centers [32, 33], drinking water distribution systems [9, 17], contamination in drinking water [11]. The detailed surveys on the approaches, tools and techniques employed in existing IoT-based water quality monitoring solutions can be found in [18, 27].

Application IoT for wastewater monitoring and treatment, and use it for household activities is discussed in [34]. In [35] authors have developed biosensors on Arduino microcontroller to monitor changes in animal behavioral because of water pollution.

Another interesting application of IoT is controlling water quality on natural and artificial fish farms [33, 36, 37]. An example of communication diagram for ASM smart water project implemented in Iran is presented in fig. 49.11, as you can see it very similar to the architectures discussed above. The list of major parameters for this project includes water temperature, pH, DO, ammonium and nitrite.

Application IoT in artificial water basins and aquariums help the aquatic farmers to control and recycle the water, increase productivity, and reduce environmental impacts.

Our partners from EU universities are actively involved in research and development for water monitoring, applying new knowledge in business and the educational process. For example, the University of Coimbra suggests a master course in the sustainable management of the urban water cycle. In this master course, it is expected that most students are already in the labor market, so their perspective is not that of a beginning a new professional area but, mainly, seeking of advanced knowledge to improve their competitiveness in this specific area of expertise [38].

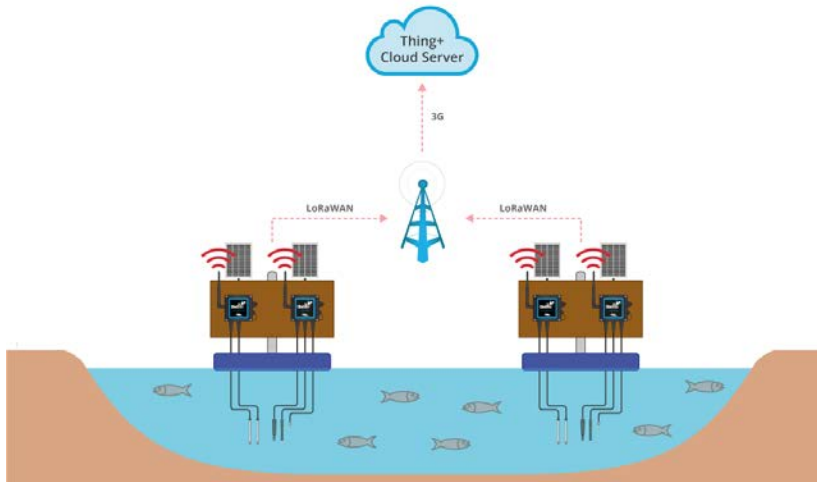


Fig. 49.11 – Communications diagram of ASM Smart Water project
(Source: [33])

School of Engineering at Newcastle University focuses on a broad range of communications, sensors and signal processing. One of their recent projects is Flood-PREPARED: Predicting Rainfall Events by Physical Analytics of REaltime Data NERC 2017-20121 [39]. The project is targeted on developing a leading international capability for real-time surface water flood risk and impacts analysis for cities and creating a digital twin of the water network in Newcastle, which will be used in conjunction with the flood models to simulate what would happen if an incident like a water main burst occurs.

IoT in Monitoring Water Networks Research is conducted in Department of Network and Systems Engineering, KTH. The project is carried out within the H2020: Water JPI – Sustainable management of water resources in agriculture, forestry and freshwater aquaculture sectors [40]. The main tasks include: system design and dealing with node deployment problem, networking sensing (tasks of scheduling and routing for prolonging network lifetime, wireless energy transmission, and developing machine learning algorithms for leakage/pollution detection [41]).

Conclusions and questions

IoT based water quality monitoring systems can be highly successful but they require intensive monitoring, control and management. To get a good solution, many issues and tasks must be solved, among them:

1. cost of the IoT solutions (initial costs, cost of IoT enabled sensors, instruments and technology for real-time monitoring and storage to the cloud or remote centers for analysis);

2. interoperability of the devices from different manufacturers or even from a single brand with different protocols;

3. availability of reliable electricity and mobile internet to the IoT based WQMS;

4. security issues (the absence of a secure and properly encrypted network, the adoption of IoT could lead to security challenges and vulnerabilities);

5. lack of highly qualified specialists in setting up and maintaining systems.

In order to better understand and assimilate the course content that is presented in this section, we encourage you to answer the following questions.

1. Why is water quality monitoring important?

2. What are the benefits of implementing IoT in water monitoring?

3. What difference between traditional monitoring and monitoring with IoT?

4. List the base components of the water quality monitoring system based on Internet of Things technology.

5. What parameters are important to choose sensors?

6. What issues should be taken into account to select a communication standard for IoT network?

7. How can the elements of the IoT communicate with each other in WQMS when the short-distance transmission is required?

8. How can the components of the IoT communicate with each other in WQMS when the long-distance transmission is needed?

9. What protocols can be used in different cases?

10. How to organize a cloud layer?

11. What are the main components of the application layer?

12. What the main points to arrange security layer?

13. What are groups of parameters used to detect water quality?
14. What the difference between physical and chemical parameters?
15. List the quantity factors of the water.
16. What are the basic parameters being measured for all types of water objects?
17. What are the challenges in management IoT data?
18. What techniques can be used to manage and filter the real-time data on the network layer?
19. Are there any advantages of compression measurement models?
20. Analyze the main stages of designing the online monitoring system for surface water and modify it for your case.
21. Find and discuss in groups different configuration of water monitoring stations.
22. What factors should be considered during the design of the water quality station?
23. What methods of data processing can be used to support the detection of contamination incidents?
24. How to perform monitoring of the long-term threats to water quality?

References

1. J.M.P. Martinez, R.B. Llavori, M.J.A. Cabo, and T.B. Pedersen. "Integrating Data Warehouses with Web Data: A Survey", *IEEE Trans. Knowledge and Data Eng.*, December 2007, doi:10.1109/TKDE.2007.190746.
2. J. Lin, W. Yu, N. Zhang, X. Yang, H. Zhang, W. Zhao. "A survey on internet of things: Architecture enabling technologies security and privacy and applications", *IEEE Internet of Things Journal*, vol.4 (5), pp. 1125-1142, October 2017.
3. "KAPTA™ 3000 AC4." Internet: http://technomaps.veoliawatertechnologies.com/kapta_3000/home_kapta-3000/ [Dec. 30, 2018].
4. "S::can. Intelligent. Optical." Internet: <https://www.pma.uk.com/spectrolyser/> [Jan. 18, 2019].
5. Libelium. "Smart Water." Internet: <http://www.libelium.com/libeliumworld/smart-water/> [Jan. 28, 2019].

6. V. Radhakrishnan and W. Wu. "IoT technology for Smart water system," *IEEE 20th Intern. Conf. on High Performance Computing and Communications; IEEE 16th Intern. Conf. on Smart City; IEEE 4th Intl. Conf. on Data Science and Systems*, pp. 1493-1498, 2018.

7. J. V.D. Broeke. "A short evaluation of the S::can Spectro::lyser", *Evaluation Report project*, January 2005.

8. B. O'Flyrm, R. Martinez, J. Cleary, C. Slater, F. Regan, D. Diamond, H. Murphy. "SmartCoast: A wireless sensor network for water quality monitoring", *32nd IEEE Conf. on Local Computer Networks*, October 2007.

9. T. Mcdougale, M. Maurel, C. Lemoine. "Smart sensor network case study for drinking water quality monitoring", *Conf. of International water association*, January 2012.

10. Libelium, "Smart water sensors to monitor water quality in rivers, lakes and the sea", March 2018. <http://www.libelium.com/smart-water-sensors-to-monitor-waterquality-in-rivers-lakes-and-the-sea/> [Feb. 12, 2019].

11. T. P. Lambrou, C. C. Anastasiou, C. G. Panayiotou and M. M. Polycarpou. "A Low-Cost Sensor Network for Real-Time Monitoring and Contamination Detection in Drinking Water Distribution Systems", *IEEE Sensors Journal*, vol. 14(8), pp. 2765-2772, 2014.

12. A. Tsopela, A. Laborde, L. Salvagnac, V. Ventalon, E. Bedel-Pereira, I. Seguy, P. Temple-Boyer, P. Juneau, R. Izquierdo, J. Launay. "Development of a lab-on-chip electrochemical biosensor for water quality analysis based on microalgal photosynthesis", *Journal of Biosensors and Bioelectronics, ScienceDirect*, vol. 79, pp. 568-573, December 2015.

13. Sarawi S. A., M. Anbar, K. Alieyan, M. Alzubaidi. "Internet of Things (IoT) communication protocols: Review," *IEEE International conf. on Information Technology*, October 2017.

14. M. U. Farooq, M. Waseem, S. Mazhar, A. Khairi, T. Kamal. "A Review on Internet of Things (IoT)," *Intern. Journal of Computer Applications*, vol. 113(1), March 2015.

15. J. Olsson. "6LoWPAN demystified" Internet: <http://www.ti.com/lit/wp/swry013/swry013.pdf> [Feb. 23, 2019].

16. S. K. Alshattnawi, "Smart Water Distribution Management System Architecture Based on Internet of Things and Cloud Computing," *IEEE Intern. Conf. on new trends in computing sciences*, pp. 289- 294, January 2018.

17. T. Mcdougale, M. Maurel, C. Lemoine. "Smart sensor network case study for drinking water quality monitoring," *Conf. of International water association*, January 2012.

18. M. Pule, A. Yahya, J. Chuma. "Wireless Sensor Network: A survey on monitoring water quality," *Journal of Applied Research and Technology*, vol.15(6), pp.562-570, December 2017.

19. S.C. Mukhopadhyay, A. Mason, "Smart Sensors for Real-time water quality monitoring", *Springer-Verlag*, 2013.

20. A.C. Niel, M. Reza, N. Lakshmi. "Design of Smart Sensors for Real Time Water Quality Monitoring." *Journal IEEE*, January 2016.

21. H.A Lee, N. Lee. "Compressive Sensing-based Data Processing Method for Massive IoT Environments," *IEEE Conference ICTC*, pp. 1242-1246, 2016.

22. D.L. Donoho. "Compressed sensing." *Journal IEEE Trans. Inform. Theory*, vol. 52, no. 4, pp. 1289 – 1306, April 2006.

23. E.J. Candès. "Compressive sensing." *Intern. Congress of Mathematicians*, vol. 3, pp. 1433 -1452, 2006.

24. Y. Ji, C. Bockelmann, A. Dekorsy. "Compressed sensing based multi-user detection with modified sphere detection in machine-to machine communications," *Intern. ITG Conf. on Systems, Communications and Coding*, pp. 1-6, 2015.

25. J.M. Romero, S.H. Hallet, S. Jude. " Leveraging Big Data Tools and Technologies: Addressing the Challenges of the Water Quality Sector." *Sustainability*, 2017; doi:10.3390/su9122160.

26. D. Thomas, E. Wilkie, J. Irvine. "Comparison of Power Consumption of Wi-Fi Inbuilt Internet of Things Device with Bluetooth Low Energy." *Intl Journal on Comput Electrical Automation Control Inf Eng*, vol. 10(10):1837–1840, 2016.

27. S. Geetha and S. Gouthami. "Internet of things enabled real time water quality monitoring system", *J. Smart Water*, 2017.

28. M. Shuker, A. Mahmoud, A. H. Mohamad. "A Study of Efficient Power Consumption Wireless Communication Techniques." *Modules for Internet of Things (IoT) Applications Advances in Internet of Things 6:19–29 Texas instrument CC3200 Internet: <http://www.ti.com/product/CC3200> [23.02.2019]*.

29. "Water Quality Monitoring for Water Quality Surveillance and Response Systems." Internet: https://www.epa.gov/sites/production/files/2016-09/documents/online_source_water_monitoring_guidance.pdf [20.12.2019].

30. K. Tomoaki, M. Masashi, M. Akihiro, M. Akihiro, L. Sang, "A wireless sensor network platform for water quality monitoring." *IEEE Sensors*, October-November 2016.

31. A. Francesco, A. Filippo, G.C. Carlo, "A Smart Sensor Network for Sea Water Quality Monitoring". *IEEE Sensors*, 2015. J 15(5):2514–2522.

32. W. Goib, Y. Yudi, P. Dewa, S. Iqbal, M. Dadin, "Integrated online water quality monitoring". *International conference on smart sensors and application*, May 2015.

33. Libelium. "Controlling fish farms water quality with smart sensors in Iran" <http://www.libelium.com/controlling-fish-farms-water-quality-with-smart-sensors-in-iran/> [23.02.2019].

34. M.V. Ramesh, K.V. Nibi, A. Kurup, R. Mohan, A. Aiswarya, A. Arsha, P.R. Sarang, "Water quality monitoring and waste management using IoT", *IEEE Global Humanitarian Technology Conference*, December 2017.

35. G. Gerson, B. Christopher, M. Stephen, O. Richard. "Real-time Detection of Water Pollution using Biosensors and Live Animal Behavior Models." *6th eResearch Australasia Conference*, October-November 2012.

36. M. Manju, V. Karthik, S. Hariharan, B. Sreekar, "Real time monitoring of the environmental parameters of an aquaponic system based on Internet of Things," *IEEE International conference on Science, Technology, Engineering and Management*, January 2018.

37. W. Kloas, R. Groß, D. Baganz, J. Graupner, H. Monsees, U. Schmidt, et al. "A new concept for aquaponic systems to improve sustainability, increase productivity, and reduce environmental impacts." *Aquacult. Environ. Interact.*, 7, pp. 179-192, 2015.

38. Master course in the sustainable management of the urban water cycle. <https://apps.uc.pt/courses/en/course/6641> [20.02.2019].

39. Flood-PREPARED NERC Reference: NE / P017134/1. Internet: http://gotw.nerc.ac.uk/list_full.asp?pcode=NE%2FP017134%2F1&cookieConsent=A [20.02.2019].

40. Water JPI. "Water challenges for a changing world". Internet: <http://www.waterjpi.eu/> [20.02.2019].

41. I. Rosborg et. all. "KTH Workshop presentations" Internet: https://www.water.abe.kth.se/polopoly_fs/1.722307.1550156808!/Work%20shop%20presentations_20170322_v2s.pdf (22 March 2017). [20.02.2019].

50. IOT BASED SYSTEMS FOR MONITORING OF SEVERE ACCIDENTS

Assoc. Prof., Dr. H. V. Fesenko, Prof., DrS V. S. Kharchenko (KhAI)

Contents

Abbreviations	673
50.1 General Information on systems for monitoring of critical industry objects/NPP accidents.....	675
50.1.1 Existing accident monitoring instrumentation guidance	675
50.1.2 Selection of NPP parameters for accident monitoring	677
50.1.3 Set of severe accident plant states and severe accident classification examples	679
50.1.4 Classification of radiation monitoring systems and analysis of their structures	681
50.2 Multi-version drone based Systems for monitoring of NPP severe accidents	690
50.2.1 Principles of design	690
50.2.2 Sensor and communication section	692
50.2.3 Drone fleets and Internet of Drones (IoD).....	693
50.2.4 Crisis centre and decision making system.....	695
50.3 Reliability of IoD based systems for monitoring of NPP severe accidents	696
5.3.1 Subsystems' reliability models.....	696
5.3.2 System models.....	701
5.3.3 Simulation.....	702
50.4 Work related analysis	706
Conclusions and questions.....	707
References	710

Abbreviations

ANS – American Nuclear Society
ARSMS – Automated Radiation Situation Monitoring System
ARMS – Area Radiation Monitoring System
BWR – Boiling Water Reactor
CG – Wired Network Communication Section
CrS – Crisis Center
DBA – Design Basis Accident
DEC – design extension conditions
DF – Drone Fleet
DL – Light Fidelity Drone based Communication Section
DMS – Decision-Making System
DMSS – Decision-Making Support System
DoT S – Drones-of-Things Subsystem
DS – Wi-Fi Drone based Sensor Section
DSL – Digital Subscriber Line
DW – Wi-Fi Drone based Communication Section
D/W – Drywell
EOP – Emergency Operating Procedure
EPRI – Electric Power Research Institute
GIS – Geographical Information System
GUI – Graphical User Interface
HPCI – High Pressure Coolant Injection
IAEA – International Atomic Energy Agency
IEC – International Electrotechnical Commission
IoD – Internet of Drones
IoT – Internet of Things
IoTS – Internet-of-Things Sensors
IoT S – Internet-of-Things System
LAN – Local Area Network
Li-Fi – Light Fidelity
Li-FiS – Light Fidelity Sensors
LOCA – Loss of Coolant Accident
LPECCS – Low Pressure Emergency Core Cooling System
MCR Main Control Room
NRC – Nuclear Regulatory Commission
MPSAMS – Multi-Version Post-Severe Accident Monitoring System

NPP – Nuclear Power Plant
PAMS – Post-accident Monitoring System
PCV – Primary Containment Vessel
PD – Personal Dosimetry
PFFO – Probability of Failure-Free Operation
RPV – Reactor Pressure Vessel
PWR – Pressurized Water Reactor
R/B – Reactor Building
RBD – Reliability Block Diagram
RCIC – Reactor Core Isolation Cooling
RMP – Radiation Monitoring of Premises
RMS – Radiation Monitoring System
RPM – Radiation Pollution Monitoring
RTM – Radiation Technical Monitoring
SA – Severe Accident
SAMG – Severe Accident Management Guideline
SBO – Station Blackout
S/C – Suppression Chamber
SG – Wired Network Section
SHF – Software and Hardware Facilities
SFP – Spent Fuel Pool
SL – Light Fidelity Sensor Section
SQL – Structured Query Language
SubD – Wi-Fi Drone based Subsystem
SubIoT – Internet-of-Things Subsystem
SubG – Wired Network
SubL – Light Fidelity Subsystem
SubW – Wi-Fi subsystem
SW – Wi-Fi sensor section
TCP – Transmit Control Protocol
TSC – Technical Support Centre
UAV – Unmanned Aerial Vehicle
UDP – User Datagram Protocol
URMS – Universal Radiation Monitoring System
VPN – Virtual Private Network
Wi-FiS – Wi-Fi Sensors
WireS – Wired Sensors

50.1 General Information on systems for monitoring of critical industry objects/NPP accidents

50.1.1 Existing accident monitoring instrumentation guidance

The Fukushima Daiichi accident in March 2011 highlighted the need to re-examine criteria for instrumentation provided to monitor accident parameters in nuclear power plants. This re-evaluation was required to respond to lessons learned from accident experience and to extend the applicability of criteria to design extension conditions (DEC).

The International Atomic Energy Agency (IAEA) has established an Action Plan on Nuclear Safety in response to the Fukushima Daiichi accident. One of the action items of this plan was to provide guidance to Member States on post-accident and severe accident monitoring systems. Historically, the terms ‘post-accident monitoring’ and ‘accident monitoring’ have both been used to mean the same concept. Accident monitoring is used in this publication because its use acknowledges that accident conditions can span a long period of time from the initiation of the event to the return to a controlled state. The major international standards organizations have also adopted this terminology.

Nuclear power plants currently have some form of accident monitoring instrumentation systems that are based on existing accident monitoring design criteria. These systems are largely designed using guidance that was developed in the early years of the nuclear industry, and then modified as necessary to include the impact of lessons learned through major nuclear plant upsets and accidents that occurred in the 1979–1986 time frame. For example, guidance for accident monitoring criteria for light water reactor technology plants is largely influenced by the principles inherent within their licensing bases (late 1960 vintage plants through to the mid-1990s), as modified by lessons learned from the accident at the Three Mile Island Unit 2 (TMI-2), in 1979, and the Chernobyl accident, in 1986. Ideally, the design criteria contained in existing guidance should now be augmented with criteria derived for the monitoring of severe accidents and DEC in light of lessons learned from the Fukushima Daiichi accident, which occurred in 2011.

Immediately following the accident at TMI-2, US industry experts

convened as a group under the auspices of the American Nuclear Society (ANS). Their members drafted ANS Standard 4.5-1980, Criteria for Accident Monitoring Functions in Light-Water-Cooled Reactors [1]. This effort resulted in a useful means for addressing accident monitoring instrumentation design in light of the functions that need to be implemented by plant operators and emergency responders in the event of an accident. ANS Standard 4.5-1980 provided a functionally based methodology for categorizing the various types of accident monitoring instrument based on the functions served and type of information provided, in a manner that allowed for the identification of the qualification requirements and duration requirements that need to be considered in the design of these instruments.

US Nuclear Regulatory Commission (NRC) Regulatory Guide 1.97, Revision 2 [2] endorsed the use of the criteria depicted within ANS Standard 4.5-1980, and provided guidance for applying these criteria for meeting US regulations. Subsequently, the Institute of Electrical and Electronics Engineers (IEEE) convened to develop IEEE Standard 497, IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations [3], which also adopted the same grouping based upon accident monitoring functions. Additionally, IEEE Standard 497 provided design standard requirements for qualifying such instrumentation to meet the harsh environmental conditions expected to be present during the course of a nuclear plant accident. Later revisions of US NRC Regulatory Guide 1.97 endorsed the use of IEEE Standard 497 and its subsequent revisions. The current version of IEEE Standard 497 was released in November 2010, just four months before the Fukushima Daiichi accident occurred. However, this event changed not only the general view on safety systems for nuclear power plants but also unveiled, in particular, the importance for reliable monitoring instrumentation suited to operate under such adverse conditions of a severe accident. This prompted the Nuclear Power Engineering Committee of the IEEE to initiate the next update of IEEE Standard 497, which is currently in progress.

Historically, the International Electrotechnical Commission (IEC) has not had a system standard for accident monitoring instrumentation design criteria. However, IEC Standard 61226 [4] identifies the

instrument functions, classifies them and defines the applicable requirements, and IEC Standard 60964 [5] defines requirements applicable to the human–system interface in the control room. The IEC also has standards dealing with specific functions that have a role in accident monitoring, such as monitoring of the radiation, containment and core cooling. It has been proposed that the IEC join with the IEEE for issuing a dual logo standard on accident monitoring systems for nuclear power plants based on a version of the IEEE Standard 497 that is now being revised. A small expert group of individuals from both organizations investigated the feasibility of this proposal in 2012 and did not come across any significant points of disagreement.

German standard KTA 3502 [6], from the Nuclear Safety Standards Commission (Kerntechnischer Ausschuss, KTA), addresses accident monitoring instrumentation. The current version of KTA 3502 was released in 2012. This standard establishes requirements for accident monitoring equipment for DBAs in non-mobile light water reactors. It does not refer to the monitoring instrumentation of the reactor protection systems, for nuclear remote surveillance systems, nor for instrumentation solely dedicated for normal operation. KTA has also published several standards dealing with monitoring of radioactive releases. The Electric Power Research Institute (EPRI) TR-102371 [7] provides guidance on identifying the capabilities of instruments that might be used as other available instruments and the development of operator aids for such instruments. EPRI TR-103412 [8] provides additional guidance on the identification of severe accident information needs, identification of severe accident environmental and process conditions, and evaluation of the capabilities of other available instruments.

50.1.2 Selection of NPP parameters for accident monitoring

Information Requirements. Accident monitoring instrumentation needs to provide the necessary information to support making operational decisions during implementation of emergency operating procedures (EOPs) and severe accident management guidelines (SAMGs).

SAMGs are the guidelines used for severe accidents and are typically meant for use by the technical support centre (TSC) staff or

equivalent support or crisis teams. The term guideline here is used to describe a fairly detailed set of instructions that describe the tasks to be executed on the plant, but which are less strict and prescriptive than the procedures found in the EOPs. SAMGs take plant specific details into account. These vary significantly between different types of reactor (e.g. reactor type, fuel type, coolant type and pressure, size and strength of the containment, number and capability of trains of safety equipment) and also between different reactors of the same type. The SAMGs may suggest actions that may not be appropriate for EOPs because of potential negative effects, operational and phenomenological uncertainties and the predominantly long term nature of these actions.

Examination of the EOP and SAMG strategies would identify the appropriate parameters. Furthermore, all major transitions within and between accident mitigating procedures or guidelines correspond directly to changes in information needs for plant operators and TSC staff.

Identification of Variables Monitored by Designated Accident Monitoring Channels. Accident monitoring that supports preventive accident management need to monitor the plant variables which give operators the information they need to accomplish the following:

- Take preplanned manual actions needed to bring the plant to a controlled state.
- Assess the status of the plant's fundamental safety functions.
- Determine whether there is a potential for breach, or an actual.
- Understand the status of plant systems so that appropriate decisions can be made as to their use. These will be parameters that: (a) indicate the performance of safety features and support features that are needed to mitigate design basis accidents (DBAs); (b) indicate the performance of other systems needed to bring the plant to a controlled state; (c) indicate the status of safety systems and their support features; (d) Support the determination of emergency action levels. These parameters will be typically identified in the EOPs, abnormal operating procedures, functional restoration procedures or plant licensing basis.
- Estimate the magnitude of any impending radioactive release. These variables will include those that monitor the: (a) magnitude of release through identified pathways; (b) environmental conditions (e.g.

wind speed and direction) used to determine the effect of release of radioactive material through the identified pathways; (c) radiation levels and radioactivity in areas surrounding the plant; (d) radiation levels and radioactivity in the MCR, in all personnel assembly points and in other areas of the plant where access may be needed for plant recovery.

Parameters to Support Mitigative Accident Management. Accident monitoring that supports mitigative accident management needs to provide the safety information required to appropriately respond to plant conditions as the accident progresses. This information is to enable plant operators and emergency response staff: (a) to terminate or limit further fuel degradation, if possible; (b) to maintain the integrity of the containment for as long as possible; (c) to minimize on-site and off-site releases and their adverse consequences; (d) to provide information for off-site management of the emergency; (e) to measure radiation levels and radioactivity in areas surrounding the plant; (f) to measure radiation levels and radioactivity in the main control room (MCR) and other areas of the plant where access may be needed for plant recovery.

Set of new measurement variables based on the Fukushima Daiichi accident analysis. Through an analysis of the Fukushima Daiichi accident, a set of new measurement variables has been identified that has the potential to support severe accident mitigation strategies. Furthermore, an analysis of the accident provides information that enables better identification of the environmental conditions that can result from a severe accident, which can be used to strengthen the environmental resistance of accident monitoring instrumentation.

The sequence of the accident and the existing and prospective variables to be monitored are shown in Fig. 50.1.

50.1.3 Set of severe accident plant states and severe accident classification examples

A set of severe accident plant states is defined as follows:

- SA1: The reactor core is damaged, but the core fuel remains inside the RPV (RV);

- SA2: An RPV (RV) failure has occurred, and the core fuel is outside the RPV (RV);
- SA3a: A PCV (CV) failure has occurred (assuming the success of the accident management action and the success of water injection within 24 h after the scram);
- SA3b: A PCV (CV) failure has occurred (assuming the failure of the accident management action and the failure of the ability to inject water within 24 h after the scram, but after that water injection is successful).

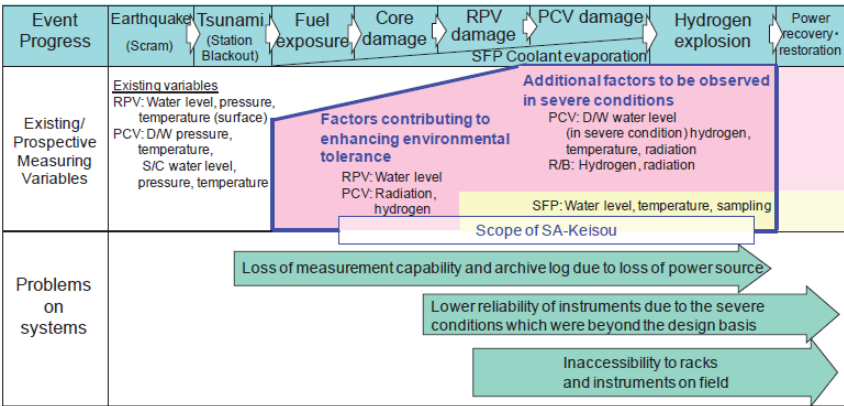


Fig. 50.1 – Sequence of the Fukushima Daiichi accident and existing and prospective variables to monitor: D/W – drywell; PCV – primary containment vessel; R/B – reactor building; RPV – reactor pressure vessel; S/C – suppression chamber; SFP – spent fuel pool

From the viewpoint of the concept of defence in depth, IAEA defence in depth level 4 corresponds to the state in which the equipment is intended for an event that is beyond design basis accidents (DBAs), but does not damage the PCV (containment vessel (CV)), preventing a major release of radioactive materials (i.e. SA1 or SA2). In addition, IAEA defence in depth level 5 corresponds to the state where the PCV (CV) is damaged and a major release of radioactive materials occurs (i.e. SA3a or SA3b).

Representative scenario and severe accident classification examples are shown in Figs 50.2 and 50.3.

Large Scale Earthquake + Tsunami	RCIC 8Hr + Depressurization	External Water Feeding after 8Hr	External Water Feeding after 24Hr	SA classification
	SBO RCIC and Depressurization	Water Feed to RPV and D/W Spray (Small LOCA)	D/Water Spray	SA1
		Water Feed to RPV (Small LOCA)	D/Water Spray Failed	SA2
		Water Feed Failed	D/Water Spray	SA1
		Water Feed Failed	D/Water Spray Failed	SA2
	TQUV Depressurization	Water Feed to RPV and D/W Spray (Small LOCA)	D/Water Spray	SA1
		Water Feed to RPV (Small LOCA)	D/Water Spray Failed	SA2
		Water Feed Failed	D/Water Spray	SA3a
		Water Feed Failed	D/Water Spray Failed	SA3b

Fig. 50.2 – Representative scenario and severe accident classification examples for a boiling water reactor (BWR) plant: D/W – drywell; HPCI – high pressure coolant injection; LOCA – loss of coolant accident; LPECCS – low pressure emergency core cooling systems; RCIC – reactor core isolation cooling; RPV – reactor pressure vessel; SA – severe accident; SBO – station blackout

50.1.4 Classification of radiation monitoring systems and analysis of their structures

Radiation Monitoring Systems (RMSs) comprises three major groups: an (PAMS), an Environmental Radiation Monitoring System (ERMS) (also known as an Area Radiation Monitoring System (ARMS) or an Automated Radiation Situation Monitoring System (ARSMS)) and a Universal Radiation Monitoring System (URMS) capable to perform functions both of a PAMS and an ERMS.

Accident and Post-accident Monitoring System. Accident monitoring systems support on-site staff in making decisions for the management of design basis accidents (DBAs) and DEC. Severe accidents are included in DEC [9-11].

Accident monitoring systems need to provide operators and TSC staff with the information that they need to develop an integrated understanding of the status of the reactor, containment and SFP in a

manner that allows for the greatest understanding of the nature of the accident, the status of the integrity of the barriers to fission product release, and the potential magnitude and pathways for such a release. Accident monitoring systems should ideally be composed of instruments that are specifically designated for the purpose. In general, the designated instruments are to be permanently installed and provide direct information necessary for accident management wherever the command and control of the accident is expected to occur (e.g. control room or TSC).

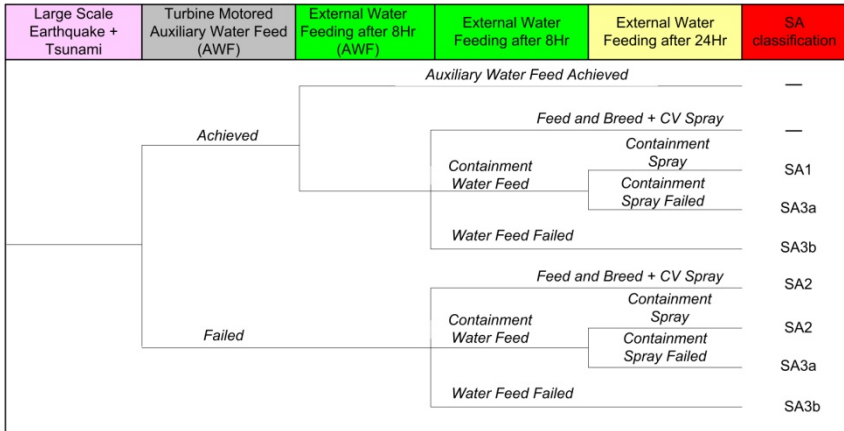


Fig. 50.3 – Representative scenario and severe accident classification examples for a pressurized water reactor (PWR) plant

A PAMS [12] assures functions of accident and post-accident monitoring at any, design-relevant, initial events, as well as beyond-design accidents (including those connected with severe damage of fuel) under conditions of a maximum design earthquake and full de-energization of a unit (Fig. 50.4).

The main functions of the PAMS:

- provision of operating personnel of NPP and emergency work headquarters with information on state of main safety functions and reactor facility’s systems with the help of PAMS hardware resistant to emergency conditions, as well as data received from standard systems when they keep their operability;

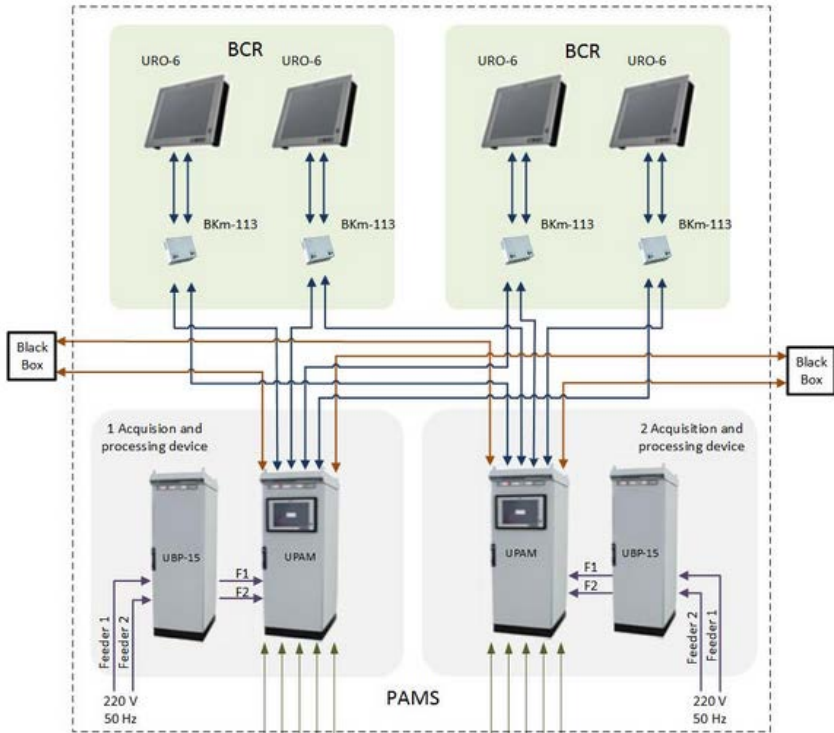


Fig. 50.4 – PAMS

- provision of information on state and efficiency of protective barriers based on direct readings of emergency instrumentation (AKIP) when standard monitoring systems fail in beyond-design accidents;
- PAMS data transmission into the “Black Box” system and crisis centres.

The PAMS system is implemented as a two-level structure using two independent channels to measure, process and provide data. The upper level of PAMS is implemented based on MSKU-4 industrial controllers and panel computers qualified according to application conditions. The lower level of PAMS is made of AKIP qualified for conditions of design and beyond-design accidents.

Power supply of PAMS equipment is carried out from a UPB-15 uninterruptible power supply device meant for connection of two

feeders for reliable power supply of a unit and built-in accumulator batteries assuring power supply of PAMS in case of full de-energization of a unit for a time up to 8 hours. AKIP of PAMS assures monitoring of the following parameters of RF: coolant level in a reactor; temperature of fuel assembly up to 1260 °C; level in a cooling pond; temperature in a cooling pond; temperature in a containment; radiation dose rate in a containment; pressure above a core; pressure in a containment; level in sumps of a containment.

Automated Radiation Situation Monitoring System (Environmental Radiation Monitoring System). According to [13], an ARSMS is intended to improve monitoring of NPP radiological parameters by computerizing their measurement, acquisition, processing, display, archiving and storage.

The ARSMS purpose is to:

- Continuously monitor radiological situation at NPP site, its sanitary protection zone and the radiation surveillance zone under all NPP operating modes (normal operation, design-basis and beyond design-basis accidents, and decommissioning activities) in the scope that is sufficient to decide promptly if radiological situation meets or does not meet regulatory requirements that define NPP radiological safety measures and procedure;

- Provide reliable information about radiological situation and predict its time-related changes, also for obtaining information needed to measure activity and define composition of radioactive nuclides that spread beyond NPP site;

- Provide recommendations to assist in decision-making for eliminating/mitigating radiological accident consequences.

- ARSMS main functions include:

- Automatic acquisition and processing of radiological parameters;

- Automatic acquisition and processing of meteorological and other non-radiological parameters;

- Verification of data reliability, alarm in case set-points are exceeded;

- Data storage in the long-term archive;

- Display of current and retrospective ARSMS parameters;

- Communication of ARSMS data to other interfacing systems.

ARSMS provides automatic measurement of the following radiological and meteorological parameters:

- gamma dose rate;
- volumetric activity of aerosols and volumetric activity of radioactive iodine in the air; volumetric activity of radioactive nuclides in water; wind velocity and direction;
- atmospheric pressure; relative air humidity; precipitations; radiation balance and total solar irradiance; atmospheric stability class.

Equipment of monitoring stations is located inside stationary container type stations equipped with intrusion and fire alarm systems, and also temperature control systems.

ARMS functions in two modes – monitoring of normal radiation situation, and monitoring of emergency radiation situation. Basic mode of normal radiation situation monitoring corresponds to normal operating mode of an NPP. Radiological data and meteorological parameters are sampled every 2 minutes.

Consider a ERMS proposed by Eran Vax et al. [14]. The ERMS main and topmost feature is the ability to monitor continuous gamma radiation fields through remote stations (Fig. 50.5). In the event of emergency, transportable stations are rapidly deployed along the wind direction, in addition to the existing fixed positioned stations.

A Control Center server continuously collects the data from the stations, stores it in a local database for future processing and transmits it to a Graphical User Interface (GUI) on remote PCs.

Communication between the Control Center server, the stations and the GUI PCs is performed using User Datagram Protocol (UDP) data packets over a Virtual Private Network (VPN), based on a combination of cellular, DSL and local Ethernet networks.

The GUI displays the received data on geographic maps (GEO), enables to view various types of graphs, activates alarms whenever a radiation threshold level is crossed or a station failure occurs, and creates reports over different cross sections.

The GUI remotely controls the stations operation mode and maintenance parameters. In addition, a simulation software module is included for training the system operators and radiation safety inspectors.

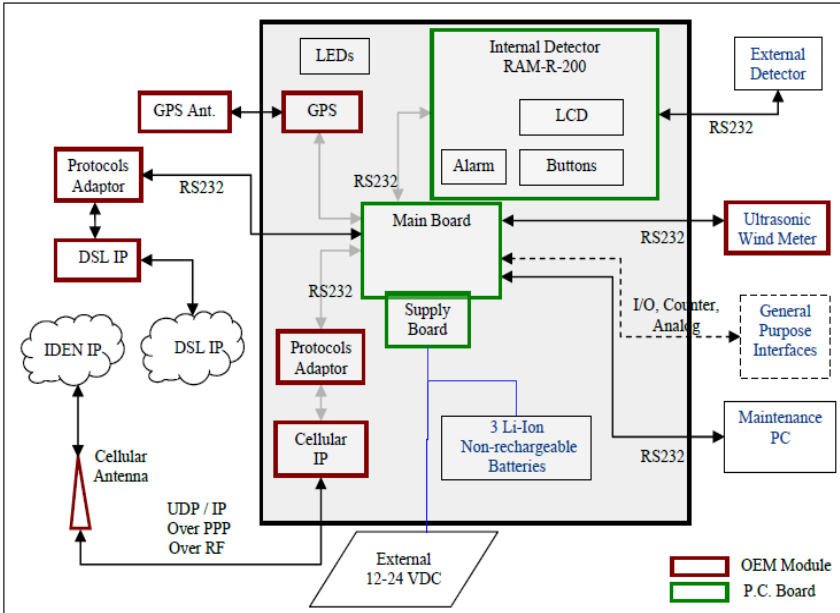


Fig. 50.5 – ERMS Block Diagram

The ERMS communication network is a VPN that consists of three IP Networks:

- IDENTM (cellular),
- DSL (over phone lines) and
- Local Area Network (LAN)

to provide redundancy and flexibility. Since all networks are IP based, transferring a station between networks is transparent to the Control Center enabling automatic switching in case one of the networks crashes in an emergency event.

Since IP network is in the mainstream technology, it is highly supported and unlikely to disappear in the near future. The UDP was preferred over the Transmit Control Protocol (TCP) since it has far less bytes overhead per packet.

This feature is useful when sending small data packets over relatively slow cellular data link, which already incorporates a built in

link control. Since UDP is a "connectionless" protocol, a message hand-shake is included at the high level ERMS protocol.

At the control center proximity a fast LAN (100 Mb/sec) is used to transfer data from the main Communication Server to the GUI PCs, thus allowing to install as many GUI PCs as necessary.

A GUI PC or a backup Communication Server can be installed anywhere using Digital Subscriber Line (DSL) network. The communication server acts as a gateway and connects all three networks as shown in Fig. 50.6.

The Control Center uses powerful server hardware with redundant power supplies and hard drives. The Control Center software contains two modules:

- Collector - controls all communication to the stations and GUIs,
- Structured Query Language (SQL) Data Base (DB).

The Control Center software main functions are:

- Polling and collecting environmental data from the stations.
- Retrieving Built In Test (BIT) results for maintenance needs.
- Sending alarms and current readings to the GUI.
- Sending reset commands to the stations upon request.
- Managing the SQL DB.
- Sending history records to the GUI upon request, using SQL queries.

- Data synchronization with the secondary server.
- DB backup.

The operator front-end interface to the ERMS is the GUI application, based on Windows XPTM. The GUI communicates with the Collector application at the main or secondary server (to the active one) retrieves the data and displays it on screen.

The collected radiation dose rate measurements are displayed using three different visual aids:

- a table of all the stations and their current dose rate,
- an electronic map - with each station location colored according to the radiation level, and
- real time graphs of the dose rate across a chosen time period for selected stations, with the intervals' calculated statistics.

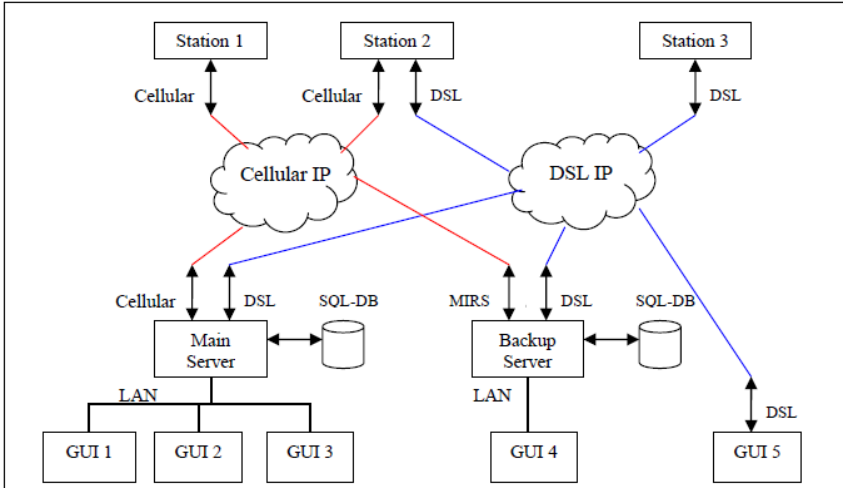


Fig. 50.6 – ERMS Network Structure

The GUI simulation software module generates real-time synthetic dose rate values per station.

These readings are produced by generating time dependent radioactive plume and sampling the radiation field of the plume at each station location. The plume is simulated with respect to parameters such as: sampling and eruption locations, wind properties, time and eruption rate. In the simulation mode the GUI retrieves the data from the simulation software module instead of the Control Center.

Universal Radiation Monitoring System. Consider an Automated System of Radiation Control for NPP ASRC-01 [15] as an example of a URMS. The system has the following features:

- Open two-level multiprocessor canal structure
- Consolidation and supply of the system depends on the project's specifications
- Complete set of detection assembly by ionizing radiation and required measurement range
- Possibility to add additional functions
- Informative software

System designation. The system is designed to get and process information about characteristics of radiation condition of NPP and environment in all working conditions including accidents within and beyond the design as well as NPP's condition after decommissioning.

Areas of application of the system

The system may be implemented at NPP with water-moderated power reactor. Systems' equipment may be installed at any sites with enhanced radiological hazard such as nuclear-fuel processing combines, research reactors, nuclear waste sites, etc.

Engineering model

The system has open apportioned two-level hierarchy structure where:

Lower level provides measurement and management of canals

Higher level provides information integration of measurement and management characteristics that allows overall control and evaluation of radiation safety at NPP.

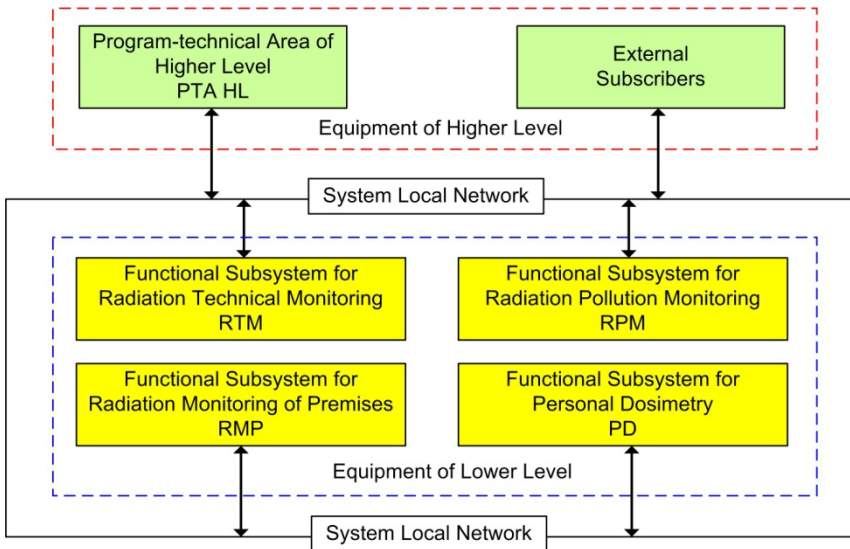


Fig. 50.7 – Functional structure of ASRC-01

Lower level of the system is composed of the following interdependent functional automated subsystems:

- Subsystem for radiation technical monitoring (RTM).
- Subsystem for radiation monitoring of premises (RMP).
- Subsystem for personal dosimetry (PD).
- Subsystem for radiation pollution monitoring (RPM).

Higher level of the system is implemented on the base of software and hardware complex of SHC BU-01R which provides information from software and hardware facilities (SHF) of lower level and external subscribers, data processing, archiving and presentation in display facilities, external data exchange and provides integral analysis of radiation safety of energy unit.

50.2 Multi-version drone based Systems for monitoring of NPP severe accidents

50.2.1 Principles of design

Existing NPP PAMSs are based on wired networks that connect sensor areas directly with the crisis center. Reliability and survivability of such systems are assured by redundancy of equipment, cable communications, and other components. However, in the case of severe accidents, wired network-based PAMS can experience damaged sensors or broken cable connections. Under such conditions, the NPP PAMS is partially or totally rendered useless.

To avoid such a problem, a multi-version approach is envisioned in which the wired network components and interfaces are expanded to include wireless communication components, which is more resilient to bridge physical failures.

To assure stability of a wireless network-based PAMS subsystem after an accident or a powerful jamming attack, a reliable transmission of data to support the possible failures of a wired network is deemed essential. Consequently, to improve the survivability of PAMS, the authors have introduced the use of a drone-fleet [16-20].

Finally, in a severe accident, it will be very important to minimize the power consumption of both the measurement and control modules, since both the wired and wireless microcontrollers can be activated. As a consequence, the power demands required by the wireless interfaces

that interact with the drones must be analyzed from a signal strength perspective.

The structure of the proposed multi-version, post-sever accident monitoring system (MPSAMS) is shown in Fig. 50.8. This system consists of the following components:

- 1) NPP;
- 2) sensors composed of drones, Wi-Fi sensors (Wi-FiS), *light fidelity* sensors (Li-FiS) based on a bidirectional wireless technology similar to Wi-Fi, and Internet-of-Things sensors (IoTS);
- 3) several drone fleets (DF1 and DF2);
- 4) communication interface to a crisis center decision-making system (DMS),
- 5) autonomous decision-making support system (DMSS; groups of experts) to assure crisis center functionality,
- 6) Internet cloud portal.

Finally, the Internet cloud portal is made up of one IoT subsystem (IoT S) and three drones-of-things subsystems labeled DoT S1, DoT S2, and DoT S3.

The underlying principles for creating the MPSAMS (see Fig. 50.8):

1. Diversity of sensor types: Wired and wireless sensors provide for greater flexibility under various failure modes. Three types of sensor modes are described here:
 - wired sensors (WireS), sensors derived from the Internet of Things (IoTS),
 - *light fidelity* sensors (Li-FiS), and
 - drone based wireless sensors that include drones employing Wi-Fi (Wi-FiS).
2. Diversity of transmission modes: wired, wireless drone based point-to-point and mesh routing.
3. Diversity of data types: Digital, light, and acoustic.
4. Mobility (drones) management.
5. Dynamical reconfiguration and redundancy (drone fleet).

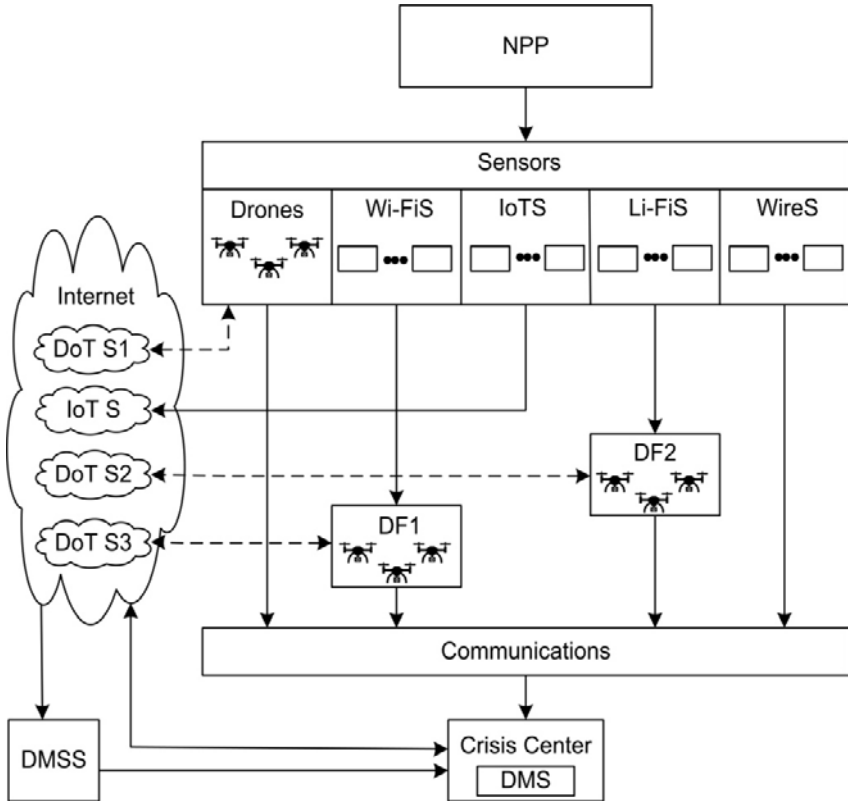


Fig. 50.9 – Structure of MPSAMS

50.2.2 Sensor and communication section

The primary task of sensors is to monitor physical parameters such as reactor temperature, reactor pressure, coolant flow, and radioactivity. Under a severe system failure, drone sensors replace the functionality of damaged wired sensors, which may monitor gamma dose rates within a 30-km radius of an NPP or provide views of inaccessible interior areas of a damaged NPP.

The Internet subsystems IoT S, DoT S1, DoT S2, and DoT S3 collect real-time data, ensure their long-term storage, and provide current and retrospective data about accident related parameters. More

importantly, DoT S1, DoT S2, and DoT S3 manage and coordinate the deployment and cooperation between drone-sensor fleets (e.g., DF1 and DF2) and ensure an additional channel for DMS or DMSS (groups of experts).

Fig. 50.10 illustrates a simplified structure (architecture) of a multi-version PAMS (MPSAMS) as a modified wired network that combines an IoT subsystem (SubIoT) with three wireless subsystems. The wired network is regarded as a subsystem denoted by SubG. In principle, the wireless components of the MPSAMS structure are divided into sensor components (left block) and their corresponding communication components (right block).

The Wi-Fi subsystem (SubW), Li-Fi subsystem (SubL), and Wi-Fi drone based subsystem (SubD) make up the wireless sensor components. Their corresponding data transmissions (communications) are indicated by arrows pointing to the right block. It should be noted that the drone fleet is integrated within the MPSAMS as both sensor components and communication components. The IoT subsystem provides additional sensor/drone capabilities not specified in the illustration. The MPSAMS architecture has the flexibility to easily incorporate *multi-version redundancy* of sensors and communication components.

50.2.3 Drone fleets and Internet of Drones

In the normal operational mode, data and command exchanges run through the wired network. If this process is damaged during an accident, a fleet of communication drones acting as an auxiliary wireless network is created to support these activities. Drones are launched in the event of a wired network failure or in the detection of a possible severe accident.

The drones are designed to autonomously form a stable flight formation, which is configured in a master/slaves' arrangement. In order to conserve battery power or in the case of node dropout, the master node (which is given command responsibilities) can be reassigned to other slave nodes when deemed appropriate. From this vantage point, the formation of drones will cooperate to maintain the following functions:

- 1) to monitor and collect all data from sensor modules that are equipped with wireless connections;
- 2) to form a reliable mesh network for optimal data streaming between point-to-point transmissions;
- 3) to provide surveillance imaging for damage control, and search and rescue;
- 4) to summarize areas of contamination;
- 5) to provide an unmanned observation platform for exploratory surveillance.

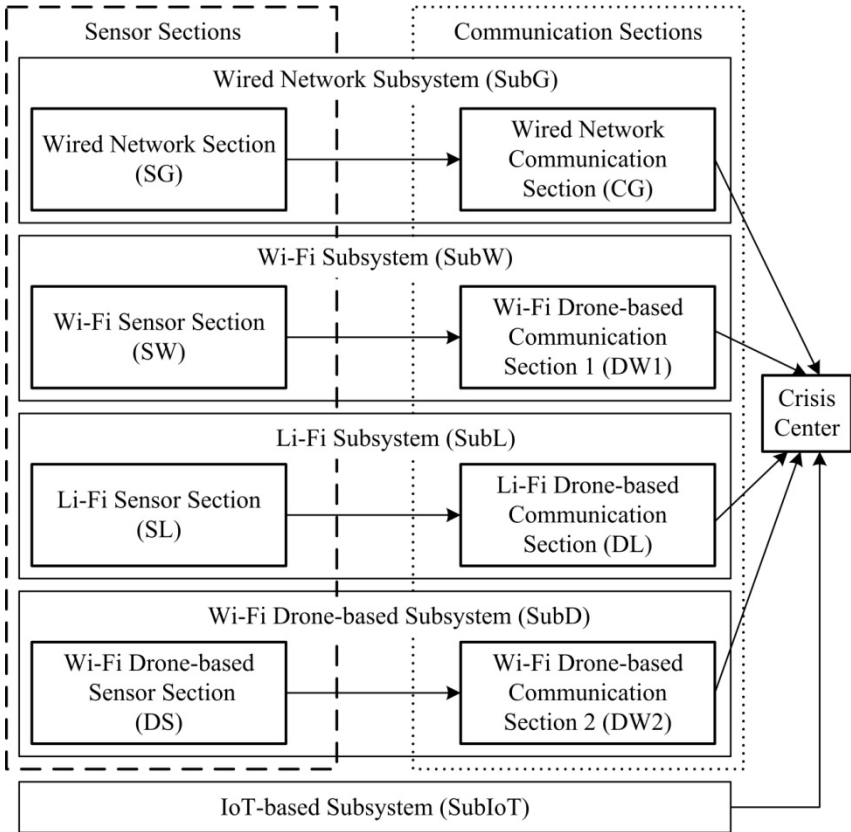


Fig. 50.10 – Simplified structure of MPSAMS

The drone fleet is located permanently at a considerable distance from the NPP and housed within the NPP as well. The communication network (wireless network and drone fleet systems) is deployed after the accident and drones fly to the designated accident zone. The drone fleet is divided into subsets:

1) repeaters (slave) that work together on a principle of “one leader.” If the “leading drone-repeater” (master) is damaged, then another drone-repeater takes over the previous master’s functions;

2) observers (equipped with a TV camera) when enabled runs the continuous visual monitoring of the accident location;

3) additional sensors that can be carried by drones or placed in certain locations. Drones should be able to change their role by upgrading equipment at their base station.

It is important to note that the subsystems SubIoT, SubW, SubL, SubD, and the SubG are all diverse in terms of capabilities among one another. This feature is critical in designing fail-safe systems. Also note that the communication sections for the Wi-Fi subsystem, the Li-Fi subsystem, and the Wi-Fi drone based subsystem are all drone based. Although not shown, portions of the IoT-based channels are also drone based. This drone based, communication capability is designed to support reliable transmission of data if the wired subsystem section happens to fail. Finally, to increase the MPSAMS’ survivability, both sensor and communication sections of wireless network subsystems should be equipped with backup batteries and multiple blocks of wireless communication modules as well as self-testing and self-diagnostic systems. Thus, such a multi-version subsystem can be considered as an Internet of Drones (IoD) based MPSAMS.

50.2.4 Crisis centre and decision making system

Crisis centre and DMS/DMSS shall perform the following main functions [21]:

- 1) receiving notifications and initiating the response to an accident;
- 2) coordination and direction of on-site response actions;
- 3) providing technical and operational support to those personnel performing tasks at a facility and those personnel responding off the site;

4) direction of off-site response actions and coordination with on-site response actions;

5) coordination of monitoring, sampling, and analysis;

6) coordination of communication with the public.

Crisis centre and DMS/DMSS can include the following emergency response facilities:

1) control room (CR);

2) onsite technical support center (TSC);

3) onsite operational support center (OSC);

4) nearsite emergency operations facility (EOF).

50.3 Reliability of IoD based systems for monitoring of NPP severe accidents

5.3.1 Subsystems' reliability models

Figures 50.11–50.14 illustrate a reliability block diagram (RBD) for each MPSAMS subsystem described above (note that the IoT subsystem RBD will be taken up in Section 50.3.2). From these RBDs, an equation for the probability of failure-free operation (PFFO) can be obtained. The construction of the RBD is based on the following assumptions for each subsystem:

- Subsystems are unrecoverable.
- Each subsystem (drones/sensors) has two states: operational and non-operational.
- Drone/sensor failures are independent.
- A traditional PAMS is a wired network subsystem with a parallel–series chain structure.
- The sensor and communication sections of the Wi-Fi subsystem, the Li-Fi subsystem, and the Wi-Fi drone based subsystem have a structure of type “k-out-of-n.”
- All drones/sensors within their own group are identical.
- The sensor and communication sections are made up of main (primary) sensors and redundant sensors for backup.
- The switching process is “ideal,” i.e., fault free.

Elements (Fig. 50.11) are designated in the following way:

- n is the number of the sensors of the main/redundant chain of the sensor section;
- m_{SGi} is a sensor in sensor group i of the main chain of the sensor section ($i = 1, \dots, n$);
- r_{SGi} is a sensor in sensor group i of the redundant chain of the sensor section ($i = 1, \dots, n$);
- m_{CG} is the main sensor of the communication section;
- r_{CG} is the redundant sensor of the communication section.

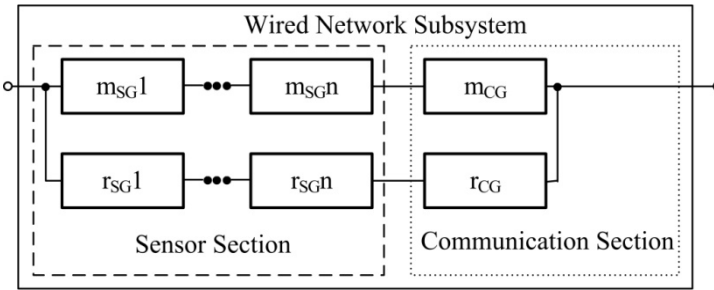


Fig. 50.11 – RBD for the wired network subsystem

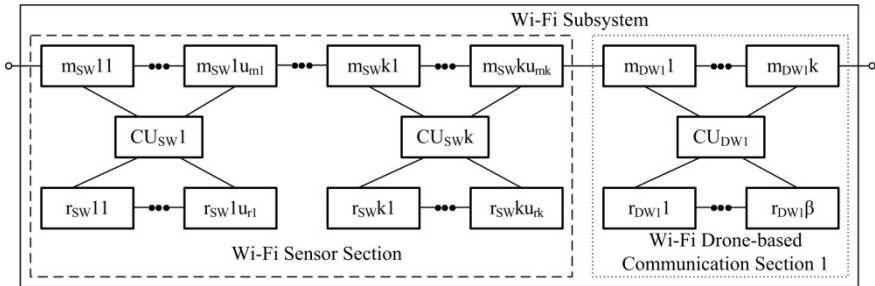


Fig. 50.12 – RBD for the Wi-Fi subsystem

Elements in Fig. 50.12 are designated in the following way:

- k is the number of groups of the Wi-Fi sensor section;
- $m_{SGi\eta}$ is a sensor η of the main chain of a group i of the Wi-Fi sensor section ($i = 1, \dots, k; \eta = 1, \dots, u_{mi}$, where u_{mi} is the number of such sensors);

- r_{SGij} is a sensor j of the redundant chain of a group i of the Wi-Fi sensor section ($i = 1, \dots, k; j = 1, \dots, u_{ri}$, where u_{ri} is the number of such sensors);
- CU_{SWi} is the switch of group i of the Wi-Fi sensor section ($i = 1, \dots, k$);
- m_{DW1i} is a drone i of the main chain of the Wi-Fi drone based communication section 1 ($i = 1, \dots, k$);
- r_{DW1b} is a drone b of the redundant chain of the Wi-Fi drone based communication section 1 ($b = 1, \dots, \beta$, where β is the number of such drones);
- CU_{DW1} is the switch of the Wi-Fi drone based communication section 1.

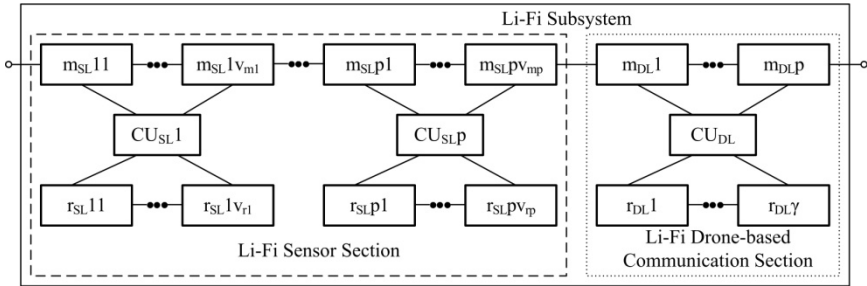


Fig. 50.13 – RBD for the Li-Fi subsystem

Elements in Fig. 50.13 are designated in the following way:

- p is the number of groups of the Li-Fi sensor section;
- $m_{DSi\eta}$ is a sensor η of the main chain of a group i of the Li-Fi sensor section ($i = 1, \dots, p; \eta = 1, \dots, v_{mi}$, where v_{mi} is the number of such sensors);
- r_{SLij} is a sensor j of the redundant chain of a group i of the Li-Fi sensor section ($i = 1, \dots, p; j = 1, \dots, v_{ri}$, where v_{ri} is the number of such sensors);
- CU_{SLi} is the switch of a group i of the Li-Fi sensor section ($i = 1, \dots, p$);
- m_{DLi} is a drone i of the main chain of the Li-Fi drone based communication section ($i = 1, \dots, p$);

- $r_{DL}b$ is a drone b of the redundant chain of the Li-Fi drone based communication section ($b = 1, \dots, \gamma$, where γ is the number of such drones);
- CU_{DL} is the switch of the Li-Fi drone based communication section.

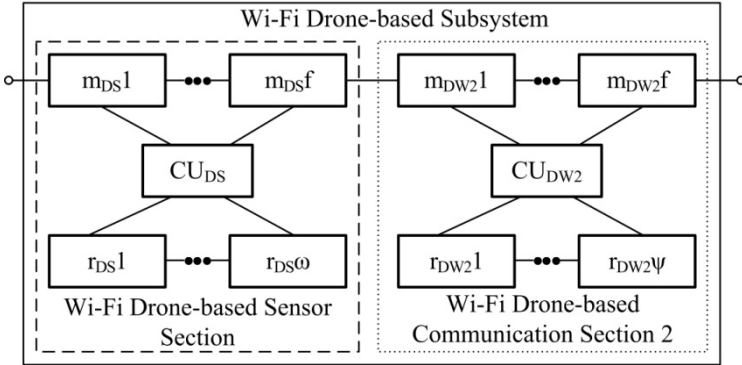


Fig. 50.14 – RBD for the Wi-Fi drone based subsystem

Elements in Fig. 50.14 are designated in the following way:

- $m_{DS}i$ is a drone i of the main chain of the Wi-Fi drone based sensor section ($i = 1, \dots, f$, where f is the number of such drones);
- $r_{DS}j$ is a drone j of the redundant chain of the Wi-Fi drone based sensor section ($i = 1, \dots, \omega$, where ω is the number of such drones);
- CU_{DS} is the switch of the Wi-Fi drone based sensor section.
- $m_{DW2}i$ is a drone i of the main chain of the Wi-Fi drone based communication section 2 ($i = 1, \dots, f$);
- $r_{DW2}b$ is a drone b of the redundant chain of the Wi-Fi drone based communication section 2 ($b = 1, \dots, \psi$, where ψ is the number of such drones);
- CU_{DW2} is the switch of the Wi-Fi drone based communication section 2.

Based on the above assumptions and the constructed RBD (see Figs. 5.11–5.14), the PFFO can be calculated for:

1) the wired network subsystem using Eq. (50.1) derived in accordance with the RBD shown in Fig. 50.11;

2) the Wi-Fi subsystem using Eq. (50.2) derived in accordance with the RBD shown in Fig. 50.12;

3) the Li-Fi subsystem using Eq. (50.3) derived in accordance with the RBD shown in Fig. 50.13;

4) the Wi-Fi drone based subsystem using Eq. (50.4) derived in accordance with the RBD shown in Figure 50.14.

$$P_{SubG} = 1 - \left(1 - p_{mCG} \prod_{i=1}^n p_{mSGi} \right) \left(1 - p_{rCG} \prod_{i=1}^n p_{rSGi} \right) \quad (50.1)$$

where P_{SubG} is the PFFO for the wired network subsystem, p_{mCG} is the PFFO for the main sensor of the wired network communication section, p_{rCG} is the PFFO for the redundant sensor of the wired network communication section, p_{mSGi} is the PFFO for a sensor i of the main chain of the wired network section, and p_{rSGi} is the PFFO for a sensor i of the redundant chain of the wired network section.

$$P_{SubW} = \prod_{i=1}^k \sum_{j=0}^{u_{ri}} C_{u_{ri}+u_{mi}}^j (1 - p_{SWi})^j p_{SWi}^{u_{ri}+u_{mi}-j} \times \sum_{b=0}^{\beta} C_{\beta+k}^b (1 - p_{DW1})^b p_{DW1}^{\beta+k-b} \quad (50.2)$$

where P_{SubW} is the PFFO for the Wi-Fi subsystem, p_{SWi} is the PFFO for each sensor of both the main and the redundant chain within its own group i , and p_{DW1} is the PFFO for each drone of both the main and the redundant chain within its own section.

$$P_{SubL} = \prod_{i=1}^p \sum_{j=0}^{v_{ri}} C_{v_{ri}+v_{mi}}^j (1 - p_{SLi})^j p_{SLi}^{v_{ri}+v_{mi}-j} \times \sum_{b=0}^{\gamma} C_{\gamma+p}^b (1 - p_{DL})^b p_{DL}^{\gamma+p-b} \quad (50.3)$$

where P_{SubL} is the PFFO for the Li-Fi subsystem, p_{SLi} is the PFFO for each sensor of both the main and the redundant chain within its own group i , and p_{DL} is the PFFO for each drone of both the main and the redundant chain within its own section.

$$P_{SubD} = \sum_{j=1}^{\omega} C_{\omega+f}^j (1 - p_{DS})^j p_{DS}^{\omega+f-j} \times \sum_{b=0}^{\psi} C_{\psi+f}^b (1 - p_{DW2})^b p_{DW2}^{\psi+f-b} \tag{50.4}$$

where P_{SubD} is the PFFO for the Wi-Fi drone based subsystem, p_{DS} is the PFFO for each sensor of both the main and the redundant chain within its own section, and p_{DW2} is the PFFO for each drone of both the main and the redundant chain within its own section.

5.3.2 System models

The proposed MPSAMS (see Fig. 50.9 and 50.10) can be modified under NPPs features. Thus, MPSAMS can be based on 2 (Figs. 50.15(a–c)), 3 (Figs. 50.16(a–c)), and 4 subsystems (Figs. 50.17(a–c)) without SubIoT, or 5 subsystems with SubIoT (Fig. 50.18).

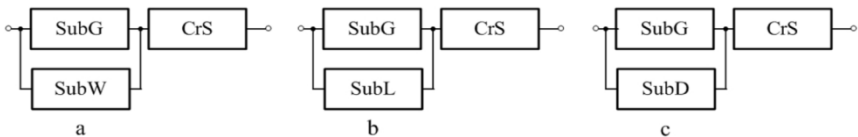


Fig. 50.15 – RBD for MPSAMS based on: (a) the wired network subsystem (SubG) and the Wi-Fi subsystem (SubW), (b) the wired network subsystem (SubG) and the Li-Fi subsystem (SubL), and (c) the wired network subsystem (SubG) and the Wi-Fi drone based subsystem (SubD)

Based on the above assumptions and the constructed RBD (see Figures 50.15–50.18), the PFFO for MPSAMS can be calculated according to one of the equations presented in Table 50.1.

50.3.3 Simulation

Figs. 50.19–50.21 are designed by simulation using Eqs. (50.1)–(50.4) and the equations from Table 9.1, and they illustrate the ways of increasing the MPSAMS reliability.

The first way is to increase the number of redundant elements (sensors or drones). For example, all plots (see Figs. 50.19–50.21) show that the PFFO for the MPSAMS will increase if the number of the redundant drones grows from 0 to 3.

The second way is to use more reliable elements for subsystems of MPSAMS. The depicted plots (see Fig. 50.20) show that the PFFO for the MPSAMS will increase if the PFFO for each of the redundant elements grows from 0.92 to 0.95.

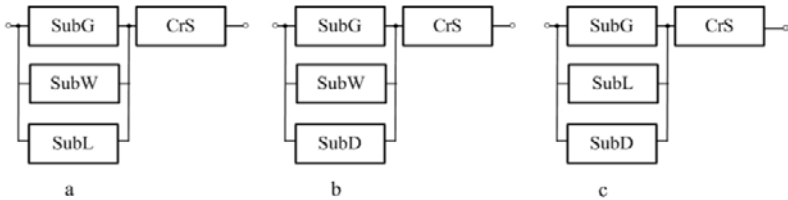


Fig. 50.16 – RBD for MPSAMS based on: (a) the wired network subsystem (SubG), the Wi-Fi subsystem (SubW), and the Li-Fi subsystem (SubL), (b) the wired network subsystem (SubG), the Wi-Fi subsystem (SubW), and the Wi-Fi drone based subsystem (SubD), and (c) the wired network subsystem (SubG), the Li-Fi subsystem (SubL), and the Wi-Fi drone based subsystem (SubD).

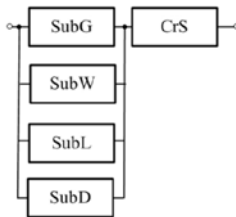


Fig. 50.17 – RBD for MPSAMS based on the wired network subsystem (SubG), the Wi-Fi subsystem (SubW), the Li-Fi subsystem (SubL) and the Wi-Fi drone based subsystem (SubD).

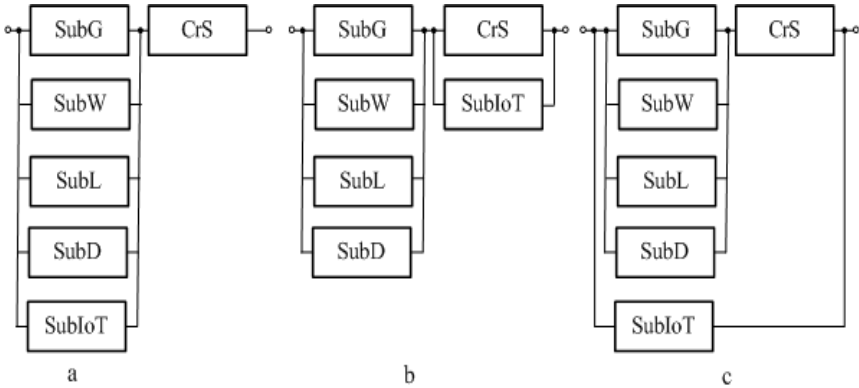


Fig. 50.18 – Various variants of RBD for MPSAMS based on the wired network subsystem (SubG), the Wi-Fi subsystem (SubW), the Li-Fi subsystem (SubL), the Wi-Fi drone based subsystem (SubD), and the IoT-based subsystem (SubIoT).

The third way is to increase the number of subsystems for MPSAMS. The MPSAMS based on SubG, SubW, SubL, and SubD (see Fig. 50.21) has the best PFFO among other structure modes.

Note that for the considered cases: the best PFFO for the MPSAMS is achieved when the number of the drones under redundancy is 9 and the number of redundant drones is 3 (see Figs. 50.19 and 50.20); the worst PFFO for the MPSAMS is achieved when the number of the drones under redundancy is 11 and the number of the redundant drones is 0 (see Figs. 50.19 and 50.20).

Table 50.1 – Equations for calculation of PFFO for various variants of MPSAMS in accordance with RBDs presented in Figures 50.15–50.18

Equation for calculation of PFFO	Figure with RBD based on which an equation is derived
$P_{S_{GW}} = [1 - (1 - P_{SubG})(1 - P_{SubW})]P_{CrS}$	Figure 50.15(a)
$P_{S_{GW}} = [1 - (1 - P_{SubG})(1 - P_{SubW})]P_{CrS}$	Figure 50.15(b)
$P_{S_{GD}} = [1 - (1 - P_{SubG})(1 - P_{SubD})]P_{CrS}$	Figure 50.15(c)
$P_{S_{GWL}} = [1 - (1 - P_{SubG})(1 - P_{SubW})(1 - P_{SubL})]P_{CrS}$	Figure 50.16(a)
$P_{S_{GWD}} = [1 - (1 - P_{SubG})(1 - P_{SubW})(1 - P_{SubD})]P_{CrS}$	Figure 50.16(b)
$P_{S_{GLD}} = [1 - (1 - P_{SubG})(1 - P_{SubL})(1 - P_{SubD})]P_{CrS}$	Figure 50.16(c)
$P_{S_{GWL D}} = [1 - (1 - P_{SubG})(1 - P_{SubW})(1 - P_{SubL})(1 - P_{SubD})]P_{CrS}$	Figure 50.17
$P_{S1_{GWL D \& IoT}} = 1 - (1 - P_{SubG})(1 - P_{SubW})(1 - P_{SubL}) \times (1 - P_{SubD})(1 - P_{SubIoT})P_{CrS}$	Figure 50.18(a)
$P_{S2_{GWL D \& IoT}} = [1 - (1 - P_{SubG})(1 - P_{SubW})(1 - P_{SubL})(1 - P_{SubD})] \times [1 - (1 - P_{SubIoT})(1 - P_{CrS})]$	Figure 50.18(b)
$P_{S3_{GWL D \& IoT}} = 1 - \{1 - [1 - (1 - P_{SubG})(1 - P_{SubW})(1 - P_{SubL}) \times (1 - P_{SubD})]P_{CrS}\} \times (1 - P_{SubIoT})$	Figure 50.18(c)

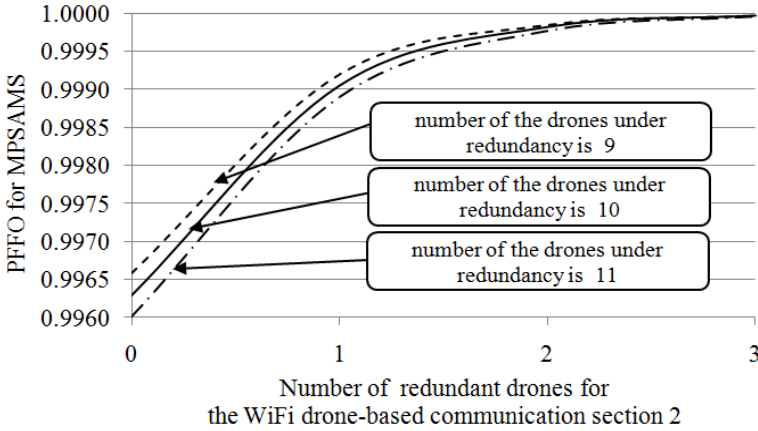


Fig. 50.19 – Dependence on PFFO for MPSAMS based on the wired network subsystem and the Wi-Fi subsystem on the number of the redundant drones for the Wi-Fi drone based communication section 2.

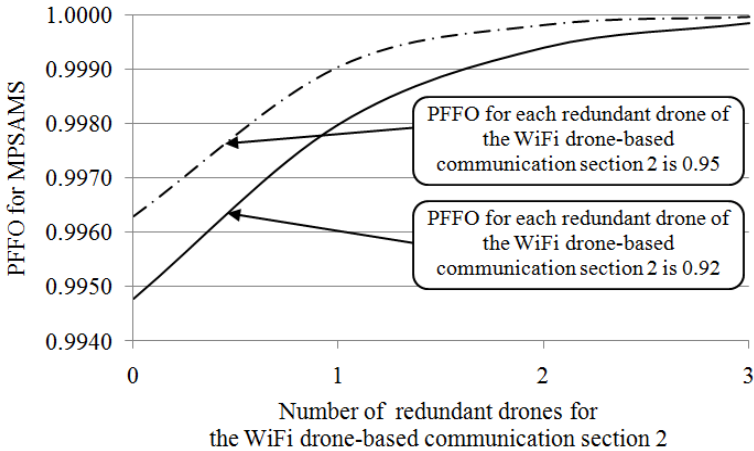


Fig. 50.20 – Dependence on PFFO for MPSAMS based on the wired network subsystem and the Wi-Fi subsystem on the number of redundant drones for the Wi-Fi drone based communication section 2 at different values of PFFO per each redundant drone.

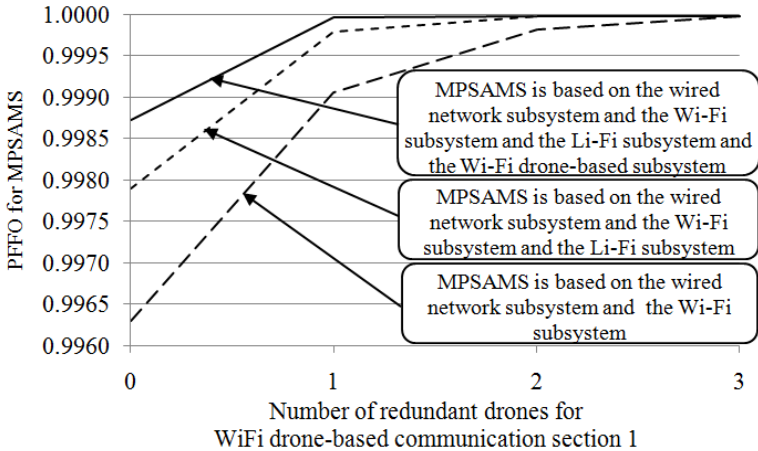


Fig. 50.21 – Dependence on PFFO for various variants of MPSAMS on the number of the redundant drones for the Wi-Fi drone based communication section 1

50.4 Work related analysis

The PAMS described in [12] assures functions of accident and post-accident monitoring at any, design-relevant, initial events, as well as beyond-design accidents (including those connected with severe damage of fuel) under conditions of a maximum design earthquake and full de-energization of a unit. The PAMS system is implemented as a two-level structure using two independent channels to measure, process and provide data.

The upper level of PAMS is implemented based on MSKU-4 industrial controllers and panel computers qualified according to application conditions. The lower level of PAMS is made of AKIP qualified for conditions of design and beyond-design accidents.

The ARSMS considered in [13] is intended to improve monitoring of NPP radiological parameters by computerizing their measurement, acquisition, processing, display, archiving and storage.

ARSMS provides automatic measurement of the following radiological and meteorological parameters: gamma dose rate; volumetric activity of aerosols and volumetric activity of radioactive

iodine in the air; volumetric activity of radioactive nuclides in water; wind velocity and direction; atmospheric pressure; relative air humidity; precipitations; radiation balance and total solar irradiance; atmospheric stability class.

Equipment of monitoring stations is located inside stationary container type stations equipped with intrusion and fire alarm systems, and also temperature control systems.

The main and topmost feature of the ERMS proposed by Eran Vax et al. [14] is the ability to monitor continuous gamma radiation fields through remote stations. In the event of emergency, transportable stations are rapidly deployed along the wind direction, in addition to the existing fixed positioned stations.

The goals of section are to develop the principles, the design of scalable IoD-based communications infrastructures, and the corresponding reliability models that can support a PAMS for severe accident surveillance of NPPs.

The following MSC and PhD programs have been analysed to develop lecture material for this module:

- EU Sesar program dedicated to study on drones development and application [22];
- Liverpool John Morris University LJMUs [23] and University of Manchester's [24] Drone Technology and Applications MSc programs on Unmanned Aerial Vehicles and their application;
- programs of 16 university of USA [25].

Conclusions and questions

The Fukushima Daiichi accident in March 2011 highlighted the need to re-examine criteria for instrumentation provided to monitor accident parameters in nuclear power plants. This re-evaluation was required to respond to lessons learned from accident experience and to extend the applicability of criteria to design extension conditions.

Accident monitoring instrumentation needs to provide the necessary information to support making operational decisions during implementation of emergency operating procedures and severe accident management guidelines.

Severe accident management guidelines are the guidelines used for severe accidents and are typically meant for use by the technical support centre staff or equivalent support or crisis teams.

Accident monitoring that supports mitigative accident management needs to provide the safety information required to appropriately respond to plant conditions as the accident progresses.

Radiation Monitoring Systems (RMSs) comprises three major groups: an Accident and Post-accident Monitoring System (PAMS), an Environmental Radiation Monitoring System (ERMS) (also known as an Area Radiation Monitoring System (ARMS) or an Automated Radiation Situation Monitoring System (ARSMS)) and a Universal Radiation Monitoring System (URMS) capable to perform functions both of a PAMS and an ERMS.

The use of diverse data transmitted from the measurement and control modules of the proposed MPSAMS as well as additional modules (sensors), which can be placed in areas not accessible by human operators, allows increasing trustworthiness of information about the reactor and the station area as whole.

The use of wireless connections with specified modules is a fail-safe mechanism to maintain critical operational monitoring for a severely damaged NPP wired network. It is understood that the deployment of wireless communication within an NPP is prohibited by current regulatory standard. However, in the event of a major nuclear accident, all strategic technologies must be made available at that critical time.

The MPSAMS can be used to mitigate the potential hazards arising from severe NPP accidents. The MPSAMS includes one wired network subsystem (traditional PAMS) and three wireless network subsystems that are more resilient to cope with wired communication failures.

To increase the MPSAMS' survivability, both sensor and communication sections of wireless network subsystems are equipped with backup batteries and multiple blocks of wireless communication modules as well as self-testing and self-diagnostic systems. To provide the increment of MPSAMS' reliability, the number of redundant elements (drones or sensors) of subsystems should be increased and more reliable subsystem components should be used.

In order to better understand and assimilate the educational material that is presented in this section, we invite you to answer the following questions:

1. What does accident monitoring instrumentation need for?
2. What are severe accident management guidelines used for?
3. What are plant status parameters to be monitored to support accident management and emergency response actions necessary for?
4. What are parameters to support mitigative accident management?
5. Name the set of new measurement variables based on the Fukushima Daiichi accident analysis.
6. Name the Set of Severe Accident Plant States.
7. Give severe accident classification examples?
8. What groups of systems belong to Radiation Monitoring Systems?
9. Characterize an Accident and Post-accident Monitoring System.
10. Characterize an Automated Radiation Situation Monitoring System (Environmental Radiation Monitoring System).
11. Characterize a Universal Radiation Monitoring System.
12. Explain principles of design of multi-version drone based systems for monitoring of NPP severe accidents.
13. Characterize the sensor and communication section of the multi-version drone based system for monitoring of NPP severe accidents.
14. Characterize functions of drones fleets of the multi-version drone based system for monitoring of NPP severe accidents.
15. Show how an Internet of Drones is used in the multi-version drone based system for monitoring of NPP severe accidents.
16. Characterize the crisis centre and the decision making system of the multi-version drone based system for monitoring of NPP severe accidents.
17. Characterize the reliability of IoD based systems for monitoring of NPP severe accidents.

References

1. American Nuclear Society, Criteria for Accident Monitoring Functions in Light-Water-Cooled Reactors, ANS Standard 4.5-1980, ANS, La Grange Park, IL (1980).
2. Nuclear Regulatory Commission, Instrumentation for Light-Water-Cooled Nuclear Power Plants to Assess Plant and Environs Conditions During and Following an Accident, Regulatory Guide 1.97, Rev. 2, US Govt Printing Office, Washington, DC (1983).
3. Institute Of Electrical And Electronics Engineers, IEEE Standard Criteria for Accident Monitoring Instrumentation for Nuclear Power Generating Stations, IEEE Standard 497-2010, IEEE, Piscataway, NJ (2010).
4. International Electrotechnical Commission, Nuclear Power Plants – Instrumentation and Control Important to Safety – Classification of Instrumentation and Control Functions, Standard 61226, IEC, Geneva (2009).
5. International electrotechnical commission, Nuclear Power Plants – Control Rooms – Design, Standard 60964, IEC, Geneva (2011).
6. Kerntechnischer Ausschuss, Accident Measuring Systems, Safety Standard 3502 (11/2012), KTA, Salzgitter (2012).
7. Electric Power Research Institute, Instrument Performance under Severe Accident Conditions: Ways to Acquire Information from Instrumentation Affected by an Accident, TR-102371, EPRI, Palo Alto, CA (1993).
8. Electric Power Research Institute, Assessment of Existing Plant Instrumentation for Severe Accident Management, TR-103412, EPRI, Palo Alto, CA (1993).
9. International Atomic Energy Agency, Safety of Nuclear Power Plants: Design, IAEA Safety Standards Series. No. SSR-2/1, IAEA, Vienna (2012).
10. International Atomic Energy Agency, Severe Accident Management Programmes for Nuclear Power Plants, IAEA Safety Standards Series. No. NS-G-2.15, IAEA, Vienna (2009).

11. International Atomic Energy Agency, Accident monitoring systems for nuclear power plants, IAEA Nuclear Energy Series No. NP-T-3.16, IAEA, Vienna (2015).

12. Accident and post-accident monitoring system (PAMS). (2016, Nov.). [Online]. Available: <http://imp.lg.ua/index.php/en/pams-2>.

13. Radiation Situation Monitoring System. (2018, Nov.). [Online]. Available: <http://www.xaec.org.ua/store/pages/eng/nucmon/latest>.

14. E. Vax, B. Sarusi, M. Sheinfeld, S. Levinson, I. Brandys, D. Sattinger, U. Wengrowicz, A. Tshuva, and Dan Tirosh. (2018, Nov.). Environmental Radiation Monitoring System. [Online]. Available: https://inis.iaea.org/collection/NCLCollectionStore/_Public/43/052/43052692.pdf

15. Automated system of radiation control for NPP ASRC-01. (2018, Nov.). [Online]. Available: <http://www.sniip.ru/en/nuclear/sistemyi-i-apparatura-radiaczionnogo-kontrolya-dlya-atomnoj-energetiki.html>.

16. R. Hiromoto, A. Sachenko, V. Kochan, V. Koval, V. Turchenko, O. Roshchupkin, and K. Kovalok, "Mobile Ad Hoc wireless network for pre- and post-emergency situations in nuclear power plant," in Proc. 2nd IEEE Int. Symp. on Wireless Systems within the Conf. on Intelligent Data Acquisition and Advanced Computing Systems, Offenburg, Germany, IDAACS-SWS 2014, P. 92–96.

17. V. Kharchenko, "Diversity for safety and security of embedded and cyber physical systems: fundamentals review and industrial cases," in *Proc. of the 15th Biennial Baltic Electronics Conf.*, Tallinn, Estonia, BEC 2016, P. 17–26.

18. A. Sachenko, V. Kochan, V. Kharchenko, M. Yastrebenetsky, H. Fesenko, and M. Yanovsky, "NPP post-accident monitoring system based on unmanned aircraft vehicle: Concept, design principles," *Nucl. and Radiation Safety J.*, vol.73,no.1, P. 24–29, Mar. 2017.

19. V. Kharchenko, A. Sachenko, V. Kochan, and H. Fesenko, "Reliability and survivability models of integrated drone based systems for post emergency monitoring of NPPs," in Proc. Int. Conf. on Inform. and Digital Technologies 2016, Rzeszow, Poland, IDT 2016, P. 127–132.

20.V. Kharchenko, H. Fesenko, A. Sachenko, R. Hiromoto, and V. Kochan, “Reliability issues for a multi-version post-severe NPP accident monitoring system,” in Proc. 9th IEEE Int. Conf. Intell. Data Acquisition and Advanced Computing Syst.: Technology and Applicat., IDAACS 2017, vol. 2, P. 942–946.

21. Nuclear Regulatory Commission, Functional Criteria for Emergency Response Facilities, Final Report, NUREG-0696, US Govt Printing Office, Washington, DC (1980).

22. https://www.sesarju.eu/sites/default/files/documents/reports/European_Drones_Outlook_Study_2016.pdf

23. <https://www.ljmu.ac.uk/study/courses/postgraduates/drone-technology-and-applications>

24. <https://www.mace.manchester.ac.uk/research/facilities/unmanned-aerial/>

25. <https://www.dronethusiast.com/top-universities-unmanned-aerial-system-programs/>

51. IOT-BASED PHYSICAL SECURITY SYSTEMS OF BUILDINGS AND CAMPUSES

Assoc. Prof., Dr. D. D. Uzun, PhD student Al-Khafaji Ahmed Waleed,
PhD student O.O. Solovyov, Dr. O. O. Illiashenko,
Prof., DrS V. S. Kharchenko (KhAI)

Contents

51.1 Physical security systems assessment and development tasks ..	715
51.1.1 Need to implement physical security systems	715
51.1.2 Tasks of physical security systems dependability assessment and assurance.....	716
51.2 IoT based physical security systems development	718
51.2.1 Principles of IoT based physical security systems development	718
51.2.2 IoT based physical security systems prototyping	721
51.3 Models of physical security systems risk analysis	723
51.3.1 Principles of IoT based physical security systems assessment	723
51.3.2 Models of physical security systems functions and components	724
51.3.3 Fault models of physical security system	727
51.3.4 Investigation and analysis of the occurrence of physical security systems failures	728
51.4 PSMECA based assessment of physical security systems	730
51.4.1. An example of PSMECA based assessment.....	730
51.4.2 Discussion of the PSMECA	731
51.5 Work related analysis	733
Conclusions and questions	733
References	734

Abbreviations

CCTV – Closed-Circuit Television

DES – Data Encryption Standard Lightweight algorithm

FMECA – Failure Mode, Effect and Criticality Analysis

ES – Environment system

IEC – International Electrotechnical Commission

ISA – International Society of Automation

ISMS – Information Security Management System

ISO – International Standardization Organization

MS – Metasystem

NIST – National Institute of Standards and Technologies

RFID – Radio Frequency IDentification

PSMECA – Physical security Failure Mode, Effect and Criticality Analysis

PSS – Physical security system

51.1 Physical security systems assessment and development tasks

51.1.1 Need to implement physical security systems

The modern qualitative and quantitative growth of the achievements of science and technology has served as the driving force for creating a multitude of scientific and practical developments. The importance of such developments is difficult to overestimate, because the average person is the carrier and / or implementer of many different ideas and technical solutions. In addition, it is necessary to take into account such aspects of socialization as culture and traditions, politics, religion, which often are catalysts to the acceleration of the diffusion of scientific and technical solutions and modern society.

Given that the objective existence of a set of positive scenarios for the application of science and technology achievements is undeniable, it is also necessary to take into account potential destructive actions and / or their scenarios. One of the systems, on which such destructive actions can be directed, is the physical security systems (PSS) of the sophisticated objects related to state buildings, buildings of infrastructure objects, buildings of educational units (universities, schools, etc.), buildings cultural fund buildings and so on.

Analysis of information from the world-known, generally accepted open sources [1-5] allows drawing a conclusion about a large number of terrorist acts on state, infrastructure facilities, objects of cult of cultural heritage in such countries as Iraq. The reasons for such attacks are obvious - inadequate security of objects of social significance.

The main points in the security of physical security of this kind of objects include 4 types of events: physical security (guards), frames - metal detectors, Closed-Circuit Television (CCTV), electronic access cards. However, the real problem is that the operators of the control room are exposed to the type of blackmail, intimidation, etc., as a result, they often become involuntary accomplices in crimes. Therefore, the problem arises of automating the functions of operators. On the other hand, there are multi-vector attacks, such as malicious disconnection of electricity, which disables video surveillance and access control systems or provocations to distract attention with the aim of enabling the penetration of intruders into the protected territory.

Another aspect that should be underlined is that the global physical security market size was valued at USD 133.94 billion in 2016, registering a compound annual growth rate of 9.1% over the forecast period [6].

Taking into account all of the above, the need of physical security to an environment aimed to mitigate or reduce terrorists acts, crime or vandalism through theft, burglaries and fire are anticipated to be the key trends driving the market and society.

51.1.2 Tasks of physical security systems dependability assessment and assurance

Analysis shown that authors do not provide a holistic approach of analysis of intrusion modes, their effects and further risk-assessment by ranging of its criticality. Threat assessment and response for intrusions applied to power substations is presented in [7]. The same researchers describe physical security monitoring system with the use of multi-agent system [8] authors which can be applied for CCTV. The process of designing, analysing, and selecting an exterior physical security system is studied in [9]. The importance of system vulnerability assessment as an outcome of analysis and evaluation is underlined in [10]. The importance of determination of vulnerabilities and threats is considered as one of the most critical considerations for physical systems in [11]. Although the assessment guide of physical security systems, developed by US Department of Energy [12] describes assessment methods and outlines their use, it contains only the overall picture without addressing the technologies for been used for providing security systems on the market.

There are various definitions and approaches to ensure dependability and resilience of complex systems. Some of them are reviewed in [13-15]. In the context of the research interest, the PSS of the RI object is, on the one hand, a subsystem of the RI, and on the other hand, it includes a deterministic (finite) set of subsystems (or components), which it consists of. Each subsystem (or component) can be represented structurally in the form of separate elements and connections among them.

The formulation of the task directly includes the research of the functioning of PSS. There are various formulations for the definition of PSS and approaches to ensure it [16-18]. In general, PSS can be

represented by an appropriate subsystem within the boundaries of the enterprise's integrated security system (facility or region).

The object of research and analysis is the PSS of the facility belonging to the Ministry of Education and Science of Iraq (as an infrastructure object of the region), and the territory of compact residence of students and employees.

In addition it is necessary to gather the following information:

- the types of failures which can occur in the system;
- the ways of distribution of the possible failures over the subsystems (components) and its elements;
- the likelihood of failures' occurrence;
- estimation of the risk of a successful attack on the protected object;
- the time needed to restore the normal functioning mode of the corrupted subsystem (or its component);
- the criticality of each specific type of attack, which can be a set (vector) of one and / or more failures (failure scenarios) provided their natural or artificial occurrence;
- determination of both sufficient and cost-effective countermeasures in order either to eliminate identified (or even possible in future) attacks, vulnerabilities and threats or make them difficult (or even impossible) to exploit by an attacker [19].

The actual decomposition of the real PSS of a specific infrastructure facility of the region can be described by the filling of the components and elements in accordance with the specifics of the technical implementation (see Figure 51.1). In the figure, for each element (subsystem), the proposed method of security analysis, which will be discussed in more detail later, is indicated.

After the designing of the structural-hierarchical scheme, it is necessary to research and analyse the behavior of the system and the individual elements and the interactions between them during the time.

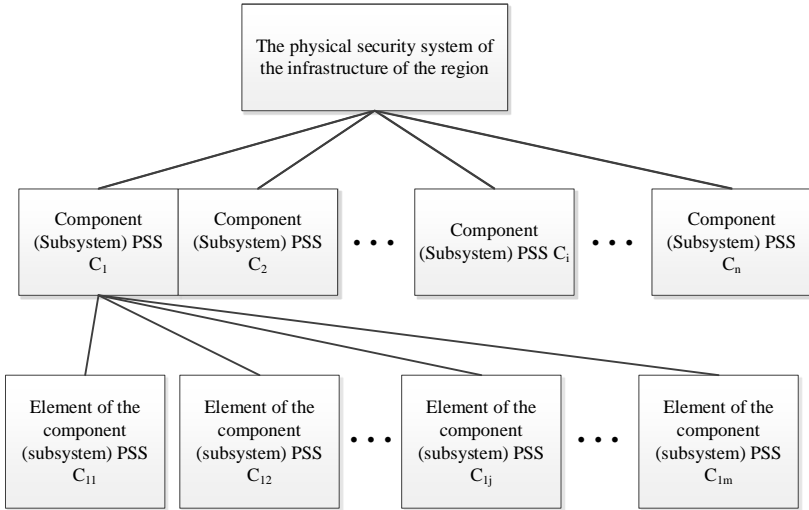


Fig. 51.1 - General view of the structural and hierarchical scheme of the physical security system

Thus, the objectives of the section are the following:

- analysis IoT-based PSS (subsection 51.2);
- development of the scheme of research and development of models and methods of risk analysis of PSS, model of functions and components of PSS, fault models of PSS;
- discussion of analysis results and of the occurrence of failures in PSS (section 51.3).

51.2 IoT based physical security systems development

51.2.1 Principles of IoT based physical security systems development

An example of the practical implementation of the structural hierarchical scheme for the PSS of the RI can be represented by a set of subsystems, e.g.: motion/intrusion detection subsystem and access control subsystem; 24/7 monitoring and signaling/alerting subsystems; CCTV subsystem; lighting subsystem; subsystem of communications and others.

The general view of the structural and hierarchical scheme of the PSS of the RI must be filled by the above subsystems (shown on Figure 51.2). Based on the example of the practical implementation of the structural hierarchical system for physical security of the RI facility, shown in Figure 2.1, we will consider modelling a prototype system using Raspberry Pi [20, 21] as the main module.

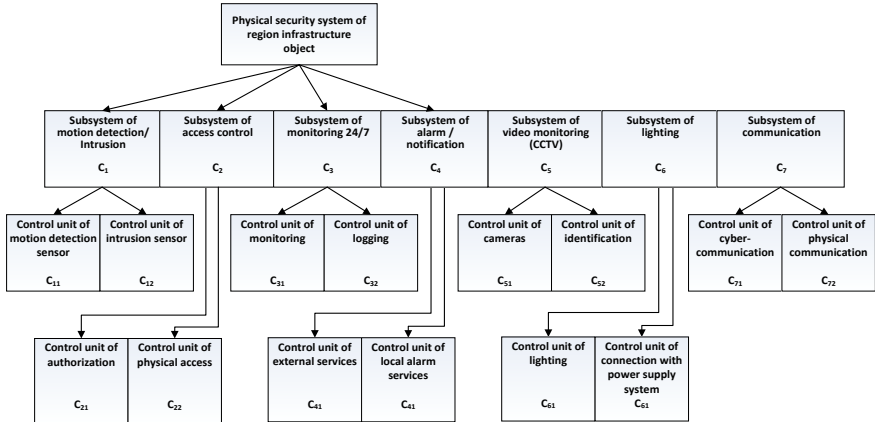


Fig. 51.2 - An example of practical implementation of the structural hierarchical scheme for the PSS of the RI facility

The Raspberry Pi microcomputer was chosen as the main control module due to the advantages in low power consumption, which allow creating an autonomous workstation for performing the tasks of automation. Due to the functional deployment using remote access and full-fledged graphic interfaces, this system is completely "friendly" for the operator and end user, which is not unimportant in the processing of information data [22].

Technical capabilities allow simulating the behavior of devices as connected directly through analog interfaces, and remotely via wireless systems. As the analogues of the microcomputer Raspberry Pi, the less expensive version which was studied is Banana Pi [23].

This is a hardware-software complex that allows performing operations like Raspberry Pi, but with some hardware deviations and reduced processing power.

More expensive analogue existed on the market which was reviewed during the research is CubieBoard4 [24].

Based on the device behavior pattern in the context of the common system, the purpose of the final product imposes a certain format of interaction between the modules.

The basic scheme of the prototype functioning of the "Motion Detection/Intrusion Detection" device combines a complex of hardware and software components that allow identifying the problem zones in the area of the PSS (see Figure 51.3).

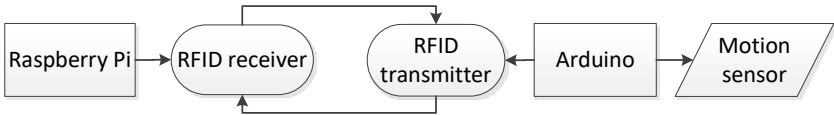


Fig. 51.3 - Functional diagram of the device "Motion detection / intrusion detection subsystems"

The "Motion Detection/Intrusion Detection " allows identifying problem zones in the area of the physical security of specific objects and taking measures to restructure security protocols including the development of a full complex of automated security system, which implies both an objective binding and global access to a single server, which is responsible for response in case of unauthorized access. Functionally, the prototype is made of a low-power Raspberry Pi microcomputer connected to the network of the inspected object and a set of external sensors combined via technology of Radio-frequency identification (RFID) using long-range identification capabilities.

This approach allows solving a wider range of problems at a distance of up to 50 meters. During the process of implementing the prototype, the data channel through RFID technology raises the current issue of security of transmitted signals, which, in case of interception and substitution, will allow an attacker to gain control both over the server side of the system and directly over the sensors. As a sample for a crypto-component, the DESL algorithm is taken as the basis, which is a modified version of the

DES algorithm for use in conditions of insufficient number of software and hardware resources [25].

Despite the shortcomings of DESL in the form of a small key size of 56 bits, this method will be hacked for several months, which is enough to test the necessary functions to automate the object within the prototype, with further replacement with more powerful security systems with a high level of cryptographic security. This approach allows one to check the basic functionality of the system and the possibility of unauthorized access, interception, substitution or jamming activities with the most rational resource consumption.

The capabilities of the prototype which is based on Raspberry Pi in connection with Arduino chips allow in the shortest possible time with less costs for components, energy resources and development to assemble a finished product aimed at the format of work at a certain position facility, check the relevance of the system from the point of view of safety, give a list of recommendations and procedures planned works to create a real fully functional sample based on more protected (expensive) software/hardware components.

51.2.2 IoT based physical security systems prototyping

For example was created hand-up prototype with common parts and user friendly devices. This project allows real-time implementation of completed functional prototypes of the Internet of things technology. As a hardware basis, the Raspberry Pi 3 microcomputer is used, which performs the functions of a basic hub and handler for connected devices. Due to the pre-installed wireless interfaces WiFi 802.11n and Bluetooth 4.1, Raspberry Pi has the ability to create a full-fledged cluster of sensors and devices.

The installation of the operating system is carried out on removable SD-card format media, thereby allowing the creation of specialized custom sets of systems. The microcomputer architecture allows you to create the necessary applications without using third-party hardware platforms. A wide selection of I / O ports allows you to connect both existing models of Internet-of-Thing hardware and software systems, and independently developed solutions. Using the prototyping system based on the Raspberry Pi allows you to quickly deploy an IoT project and test it with a real example.

The graphic presentation is shown in the picture 51.1.



Fig. 51.1. – IoT prototype KIT

For the description of attack scenarios (intrusion) or cascade failure of subsystems / elements, CASE-tool with the ability to describe the processes occurring in the system can be applied. To provide clarity, the scenario of power outage (accidental or intentional) in the interconnection of lighting and video surveillance subsystems, described in IDEF0 notation, is presented in Figure 51.4.

The next stage is to conduct the Failure, Modes, Effects, and Criticality Analysis for PSS (PSMECA) [26] which allows effectively solving the following problems:

- determination of possible types of failures of components (subsystems) of the system;
- analysis of the impact of these failures on the functioning of the system;
- establishing the countermeasures aka the possibilities (methods) of preventing failures and / or eliminating the effect of failures on the functioning of the system.

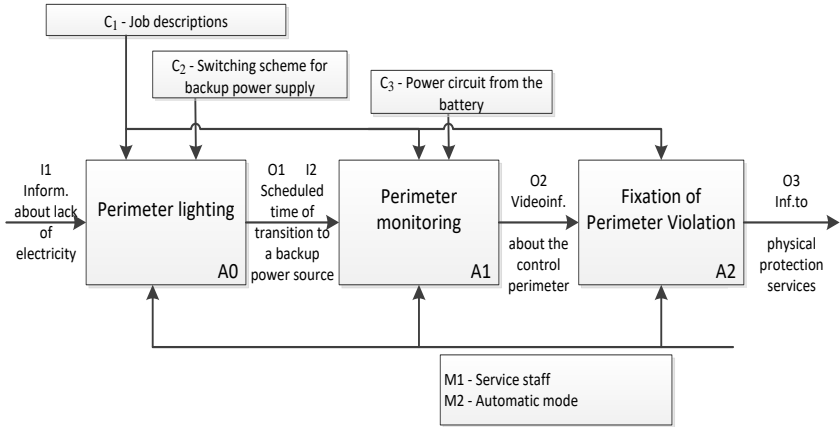


Fig. 51.4 - IDEF0 diagram of PSS functioning

51.3 Models of physical security systems risk analysis

51.3.1 Principles of IoT based physical security systems assessment

The process of research and development of models and methods for the risk analysis of physical security systems has been carrying out in the corresponding scheme shown in Figure 51.5, where HW – hardware, SW – software, HF – human factor, PIMECA – Physical Intrusion Modes, Effects and Criticality Analysis, IIMECA – Information Intrusion Modes, and Criticality Analysis.

PIMECA and IIMECA are both modifications of FMECA. More information about variations of FMECA-family analysis methods, which specifically concentrates on corruption of information security and cybersecurity in a form of intrusions in complex systems could be found in [19; 27-29]. The problem of choice of FMECA-family techniques and tools for safety analysis of critical systems is described in [30].

Objects under study represent as follows: components of the system, their interrelations and functions as well as environment, which also plays a significant role during evaluation as well as its defects and faults. Environment state include both normal state (when single and multiple fault can occur, but their criticality and the related risk can be easily mitigated and so doesn't harm the security properties) and aggressive

environment state (with indication of single and multiple attacks, which can harm the security properties of the object), assessment of risk and consequences includes the appropriate method of risk assessment and its practical issues.

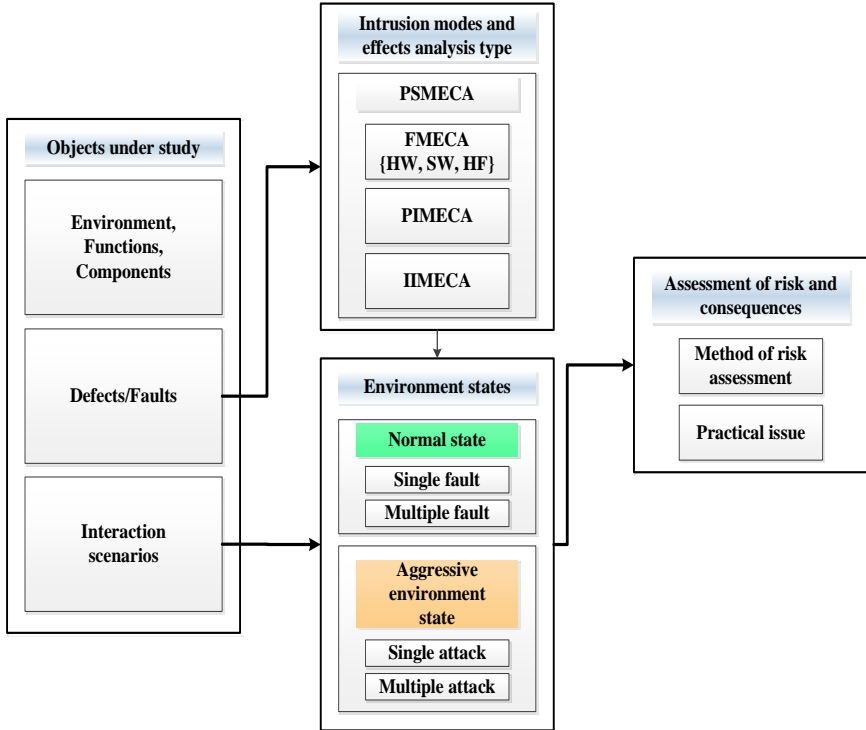


Fig. 51.5 - Scheme of research and development of models and methods of risk analysis of PSS

51.3.2 Models of physical security systems functions and components

This subsection contains formal description of the functions and components of PSS. PSS is a system of physical security, which is a part of the metasystem (MS), which in its turn includes the environment of the system (ES):

$$MS = \{PSS, ES\} \quad (51.1)$$

PSS is designed to perform the following functions:

$$SFSS = \{FVis, FVDet, Finf\}, \quad (51.2)$$

where *FVis*, *FVDet*, *Finf* are subsets of visualization, detection and information processing correspondingly.

PSS consists of a set of disjoint components:

$$SCPSS = CHF \cup CHW \cup CSW, \quad (51.3)$$

where *CHF* – multiple components (operators) which are difficult to formalize, *CHW* – multiple hardware components, and *CSW* – multiple software components. In order to reveal prime reasons of failure occurrence the intersection of hardware components and software components, human factor and hardware components, human factor and software components are defined as null:

$$CHF \cap CHW = \emptyset, CSW \cap CHF = \emptyset, CHW \cap CSW = \emptyset. \quad (51.4)$$

In its turn

$$CHW = CHWS \cup CHWH, CHWS \cap CHWH = \emptyset, \quad (51.5)$$

where *CHWS* – a subset of hardware (primary) components - media of software (storage devices, data stores), *CHWH* - a subset of hardware (secondary) components – video cameras, motion sensors, presence, etc.

In its turn, the dependency between system software and applications could be written as:

$$CSW = CSWS \cup CSWA, CSWS \cap CHWA = \emptyset, \quad (51.6)$$

where *CSWS* – a subset of system software (operating systems), *CSWA* is a subset of application software (specialized software).

The environment includes physical components (*EPS*) and information components or subsystems (*EIS*). *EPS* and *EIS* subsystems are divided into natural (passive) subsystems (*EPNS* and *EINS*) and artificial (active or aggressive with respect to the system) – *EPAS* and *EIAS*.

From one side, systems environment consists of its physical and information components

$$ES = \{EPS, EIS\} \quad (51.7)$$

From other side it could be represented in a form of its environment states – normal (*ENS*) or aggressive (*EAS*)

$$ES = \{ENS, EAS\} \quad (51.8)$$

In other words, the medium can described by the Cartesian product

$$ES = \{EPS, EIS\} \times \{ENS, EAS\} = \{EPNS, EINS, EPAS, EIAS\}. \quad (51.9)$$

There is a mapping Ω_{EC} of sets of subsystems of the environment of functions

$$SFPSS = \{FVis, FDet, FInf\} \quad (51.10)$$

on sets of components

$$SCPSS = CHF \cup CHW \cup CSW \quad (51.11)$$

which could be represented as

$$\Omega_{EC} : SFPSS \rightarrow SCPSS, \quad (51.12)$$

which is described by a Boolean matrix *BFC*, such that 0, if there is no influence (dependence); 1, if there is some influence; \emptyset , if the nature of the indicators is different.

There is a mapping Ω_{EF} of sets of subsystems of the environment of functions

$$SFPSS = \{FVis, FDet, FInf\} \quad (51.13)$$

on sets of components

$$SCPSS = CHF \cup CHW \cup CSW \quad (51.14)$$

which could be represented as

$$\Omega_{FC} : SFPSS \rightarrow SCPSS \quad , \quad (51.15)$$

which is described by a Boolean matrix BFC with the following values:

- 0 – in case if there is no influence (dependence);
- 1 – in case if there is influence;
- \emptyset – in case if the nature of the indicators is different.

51.3.3 Fault models of physical security system

In accordance with [1, 3] the faults are divided into four types:

- physical (*pf*),
- project (*df*),
- operator (*hf*),
- interaction (*if*).

Respectively, a number of faults of the *SDPSS* of the *PSS* system consist of disjoint sub-spaces.

$$SDPSS = SDpf \cup SDdf \cup SDhf \cup SDif, \quad (51.16)$$

and

$$SDpf \cap SDdf = \emptyset, SDdf \cap SDif = \emptyset, SDpf \cap SDif = \emptyset, \dots \quad (51.17)$$

The non-intersection of subsets of faults means that they concern different causes of their occurrence, but not consequences.

Given that

$$ES = \{EPS, EIS\}, \quad SDPSS = SDpf \cup SDdf \cup SDhf \cup SDif \cup SDiif. \quad (51.18)$$

Errors associated with the actions of the operator can also be divided into those that cause physical defects (*hpf*) or information violations (*hif*).

In this case

$$SDPSS = SDpf \cup SDdf \cup SDhpf \cup SDhif \cup SDipf \cup SDiif. \quad (51.19)$$

There is a mapping ΩDC of set of system faults *SDPSS* on the set of components *SCPSS*:

$$\Omega DC : SDPSS \rightarrow SCPSS, \quad (51.20)$$

which is described by a Boolean matrix *BDC*, such that 0, if there is no influence (dependence); 1, if there is some influence; \emptyset , if the nature of the indicators is different.

51.3.4 Investigation and analysis of the occurrence of physical security systems failures

At this stage, it is necessary to determine the uniqueness of the correspondence of the failures arising in the physical security system (in fact – violations in the implementation of the functions specified in the system design) and the components of this system (necessary to perform the functions).

Thus, taking into account the occurrence of failures of different nature (hardware, software, human factor ones), the sought-for match is represented as a projection of the hierarchical structure on the table of the basic structural elements of the physical security system.

The construction of the table is caused by the need of justification of formal confirmation (proof) of the reason for including different types of

components in the generated fault matrixes. PSMECA tables implies information from both FMECA and IMECA.

This construction grounds on formulas 51.1-51.20 from subsections 51.3.2 and 51.3.3 and allow to formalize different nature of failure occurrence. The implementation is presented below in Tables 51.1 and 51.2.

PSMECA								
FMECA					IMECA			
<i>pf</i>	<i>df</i>	<i>hf</i>		<i>if</i>				
		<i>hpf</i>	<i>hif</i>	<i>ipf</i>		<i>iif</i>		
				<i>ip(n)f</i>	<i>ip(a)f</i>	<i>ii(n)f</i>	<i>ii(a)f</i>	
HW	1	1	1	1	1	0	1	
SW	0	1	0	0	1	1	1	
OP	∅	∅	1	1	1	1	1	

Fig. 51.6 - The projection of the hierarchical structure of failures on the table of the main structural elements in the physical security system

Considering the dynamical nature of failures in the system of physical security the necessity of defining set of scenarios is existed. Set of scenarios (*SScen*) consists of different consequence of events, which drive to failure. So, taking into account the scenarios of dynamical occurrence of failures in the system of physical security under investigation:

$$SScen = \sum SSцени, i = 1, \dots, n , \tag{51.3.1.21}$$

taking into account the factor of time (*t*).

Thus, the developed formalization of the hierarchical structure of failures in connection with failure source nature will allow creating PSMECA tables based on set-theoretical model of the PSS components.

51.4 PSMECA based assessment of physical security systems

51.4.1. An example of PSMECA based assessment

An example of PSMECA tables for the case of CCTV subsystem functioning in normal operation mode. The process of creating PSMECA tables begins from developing the similar (basic or source) FMECA tables, which are modified according to developed set-theoretical model of the PSS components.

Main goal of such modification is to go deep into structure of analysed system failure sources to provide more strictly formalized approach, based on additional structure elements and levels of hierarchy, as shown in Figure 51.6.

Thus, for this example, first step will be developing the FMECA table of video surveillance subsystem. Table 51.1 depicts results of FMECA analysis, where: P – probability, S – severity, M – maintainability, C – Criticality.

Table 51.1. FMECA table of CCTV subsystem functioning in normal operation mode

Sub-system	HW/ SW	Failure mode	Failure cause	Failure effect	P	S	M	C
Motion/ intrusion detection sub- system	HW	Does not start	Installation error or emergency stop (interrupt)	Move- ment moni- ring within the controlled perimeter is disabled	L	H	L	H
		Improper functioning			M	M	M	M
	SW	Does not work	Staff error or design error		L	H	M	H
		No feedback			L	M	M	M
Access control sub- system	HW	Does not start	Installation error or emergency stop (interrupt)	Unauthori- zed access to the secured area can be granted	L	H	L	H
		Improper functioning			M	M	M	M
	SW	Improper functioning	Staff error or design error		L	M	M	M

Probability, severity and maintainability are ranged from low (L) through medium (M) to high (H) and the assessment is expert-based.

The resulted level of criticality (C) is indicated by the maximum range of probability, severity, and maintainability for the corresponding mode of failure.

Such fuzzy values (Low, Medium, High) are chosen just to demonstrate the opportunity of implementation of developed approach without unnecessary complication of calculations.

FMECA table for the case of CCTV subsystem functioning in normal operation mode should be modified into similar PSMECA table according to the developed set-theoretical model of the PSS components. The assessment of probability, severity and maintainability is also based on expert judgement.

The probability for PSMECA is established as:

- low (L),
- low to medium (L/M), which depends on aggressive environment conditions (e.g. in case of intensification of terrorist activities),
- medium (M) and high (H).

For severity and maintainability the same range (low, medium, high) as in in previous case is used.

Developed PSMECA table can be used for setting the more detailed causal relationship between subsystems, their failure types and PSS security risks.

Thus, based on the results of Table 51.2, obtained from Table 51.1, it is possible to determine the cause of the failure occurrence in the physical security system and the value of failure criticality more accurately.

54.4.2 Discussion of the PSMECA

The proposed technique for the PSS security assessment called Physical Security Modes and Effects Criticality Analysis (PSME(C)A) combines two well-known techniques taking into account PSS particularities [2]. First technique is Failure Modes, Effects and Criticality Analysis (FME(C)A) and the second one – Intrusion Modes, Effects and Criticality Analysis (IME(C)A).

Table 51.2. PSMECA table of CCTV subsystem functioning in normal operation mode

Sub system	Failure type			Failure mode	Failure cause	Failure effect	P	S	M	C	
Motion/intrusion detection subsystem	HW	pf		Does not start	Installation error or emergency stop (interrupt)	Movement monitoring within the controlled perimeter is disabled	L	H	L	H	
		df					L	H	L	H	
		hf	hpf				Improper functioning	M	H	L	H
			hif					M	M	M	M
		if	ipf	ip(n)f				L	L	L	L
	ip(a)f				L/M		L	M	M		
	iif		ii(a)f		L/M		H	H	H		
	SW	df		Does not work	Staff error or design error		L	H	M	H	
		hf	hif				No feedback	L	M	M	M
		if	ipf	ip(a)f				L	M	M	H
iif				ii(n)f			L	L	M	M	
			ii(a)f			L/M	H	H	H		
Access control subsystem	HW	pf		Does not start	Installation error or emergency stop (interrupt)	Unauthorized access to the secured area can be granted	L	H	L	H	
		df					L	H	L	H	
		hf	hpf				Improper functioning	M	H	L	H
			hif					M	M	M	M
		if	ipf	ip(n)f				L	L	L	L
	ip(a)f				L/M		L	M	M		
	iif		ii(a)f		L/M		H	H	H		
	SW	df		Improper functioning	Staff error or design error		L	H	M	H	
		hf	hif				L	M	M	M	
		if	ipf	ip(a)f				L/M	H	M	H
iif				ii(n)f			L	L	M	M	
			ii(a)f			L/M	H	H	H		

Features of PSME(C)A technique are the following:

- the technique is based on analysis of component and systems faults according with set SDPSS considering that SDipf and SDiif are decomposed on subsets faults caused by natural reasons (n) and aggressive environment (f), i.e. *ip(n)f* and *ip(a)f*, *ii(n)f* and *ii(a)f*. The figure 51.6 describes sets of the faults for different components; (hardware, software and human factor);
- the results of analysis are represented by a set of rows describing by a vector <component, type of faults, modes and effect of failure in point of view PSS security, probability *Prob*, severity *Sev* and complexity (time and costs) of up-state recovery *Crec*>.

$$\text{PSS security Risk} = \text{Prob} * \text{Sev} * \text{Crec} , \quad (51.5.1)$$

- taking into account the proposed PSS structures and platform hierarchical PSMECA, which consists of FMECA/IMECA (HF/IME(C)A) can be applied as shown in Tables 51.1, 51.2.

51.5 Work related analysis

This section is based on the results of analysis of curriculums and courses for MSc and PhD related to cyber security and safety assessment and assurance, development and implementation of PSSs and other monitoring systems in EU universities of ALIOT and SEREIN consortiums [31,32]. In particular there were analysed and used some courses developed in:

- Newcastle University [33],
- Coimbra University [34],
- KTH University [35]
- and others [36].

Besides, work related analysis of research projects and publications was carried on according with 51.1.1, 51.1.2 [6-25].

Conclusions and questions

The section describes principles of building physical security systems and features of development using IoT platform. Considering criticality of PSS the technique PSMECA for analysis of reliability and security is based on models of components, failures and effects of ones.

This technique is a modification of well-known FMECA procedure which is applied to analyse risks of component failures of safety critical systems Moreover, various IoT-based facilities for public use may be the object of using PSMECA analysis. An example of applying PSMECA for analysis of IoT based PSS for a university buildings and campus.

Thus, based on the research of the PSS the following results have been obtained:

- structural and functional decomposition of the physical security system of the RI was developed;

- engineering solutions for the implementation of the standard functions of the subsystems in the research object were proposed and some of the were reviewed in the paper;
- the set-theoretical models of the physical security system components, environment and faults, and general issues of PSMECA-based assessment have been analysed.

The section describes the context with a static system. Before conducting the assessing in dynamics, it is necessary to consider attack scenarios. In the case of a dynamic process, a posteriori analysis should be performed, i.e. if there is a specific event (failure mode), it is necessary to reassess the criticality of the effect of failure on the subsystem and on the system and conduct PSMECA once again.

The PSS should be analyzed periodically to ensure that the original protection objectives remain valid. Future research can be dedicated to developing scenarios of the physical and cyber-attacks including multi-step intrusions and multiple failures and considering these circumstances during PSMECA in dynamics.

In order to better understand the educational material that is presented in this section, we invite you to answer the following questions.

1. What are basic tasks of physical security systems?
2. Which are objectives of physical security systems assessment?
3. What is information needed to gather for the research of the functioning of PSS?
4. What are the principles of developing IoT-based PSS?
5. What are steps of IDEF0 diagram of PSS functioning?
6. What are tasks solving by PSMECA?
7. What are elements/stages of the risk analysis of PSS?
8. What is difference between PIMECA and IIMECA?
9. What are the main features of the PSME(C)A technique?
10. How many types of PSS faults should be analysed?
11. Describe the hierarchical structure of failures.
12. What elements does consist the PSMECA platform of?

References

1. 2010 Baghdad church massacre
https://en.m.wikipedia.org/wiki/2010_Baghdad_church_massacre

2. CNN, Deadly bombings worst Iraq attack in two years, <http://edition.cnn.com/2009/WORLD/meast/10/25/iraq.violence/index.html>
3. BBC news, Gunmen attack Iraqi central bank, <http://www.bbc.com/news/10304652>
4. The Guardian, Six bombs, 95 dead – carnage and despair return to Iraq, <https://www.theguardian.com/world/2009/aug/19/iraq-baghdad-bombings>
5. The New York Times, Suicide Bomber Kills Dozens in Attack on Iraqi Army Recruits, <https://mobile.nytimes.com/2010/08/18/world/middleeast/18iraq.html>
6. Grand View Research, ‘Physical Security Market Size, Share, & Trends Analysis Report By Component, By Hardware, By Services, By End-use (Energy, Utility, Retail, Commercial), And Segment Forecasts, 2018 – 2025’, 51 p. <https://www.grandviewresearch.com/industry-analysis/physical-security-market>
7. Jing Xie, Chen-Ching Liu, Marino Sforna, Martin Bilek, Radek Hamza, “Threat assessment and response for physical security of power substations”, Proceedings of Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), 2014 IEEE PES, 2014, October 12-15, Istanbul, pp. 1-6, DOI: 10.1109/ISGTEurope.2014.7028837
8. Jing Xie, Chen-Ching Liu, Marino Sforna, Martin Bilek, Radek Hamza, “Intelligent physical security monitoring system for power substations”, Proceedings of Intelligent System Application to Power Systems (ISAP), 2015 18th International Conference on, Porto DOI: 10.1109/ISAP.2015.7325524
9. Han Lin, David Burnett, Don Sheaffer, Eric Arnold, “Applying decision analysis process to exterior physical security system technology design and selection”, Proceedings of Security Technology, 2009. 43rd Annual 2009 International Carnahan Conference on, 5-8 Oct. 2009, Zurich, IEEE, pp. 312-312, DOI: 10.1109/CCST.2009.5335519
10. Siva RP, How to design effective physical security system, April 20, 2017, <https://www.linkedin.com/pulse/how-design-effective-physical-security-system-siva-rp-cpp-ppsp/>
11. Kline Technical Consulting, ‘The 7 Most Critical Considerations for Physical Security Systems’ Whitepaper [http://www.klinenm.com/uploads/common/The_7_Most_Critical_Considerations for Physical Security Systems.pdf](http://www.klinenm.com/uploads/common/The_7_Most_Critical_Considerations_for_Physical_Security_Systems.pdf)

12. Physical security systems. The assessment guide. US Department of Energy. Dec.2016

https://www.energy.gov/sites/prod/files/2017/02/f34/PhysicalSecuritySystemsAssessmentGuide_Dec2016.pdf

13.A. Avizienis, J.-C. Laprie, B. Randell, and C. Landwehr, “Basic concepts and taxonomy of dependable and secure computing”, IEEE Transactions on Dependable and Secure Computing, 1(1):11-33, Jan-March 2004.

14.M. Yastrebenetsky, V. Kharchenko (editors and authors), “Nuclear Power Plants Instrumentation and Control Systems for Safety and Security”. Hershey PA, USA: IGI Global, 2014, 470 p.

15.Qahtan, M. A.-S. Abdulmunem, and Kharchenko, V., (2016). “Availability and Security Assessment of Smart Building Automation Systems: Combining of Attack Tree Analysis and Markov Models” in Proceedings of Third International Conference on Mathematics and Computers in Sciences and in Industry, China, Greece, 302-307. DOI: 10.1109/MCSI.2016.062.

16.F. Charlie and M. Brayon, “Physical Protection Principles”, Nuclear Installation Dept. AELB. www.aelb.gov.my.

17.S. Harris, “Physical and Environmental Security. In CISSP Exam Guide”, USA McGraw-Hill, 6th ed., pp.427-502 2013.

18.J. Conrath, “Structural Design for Physical Security: State of the Practice [et al.]”, Task Committee, Structural Engineering Institute, ASCE Reston, 1999, 264 p.

19.Kharchenko, V. S, Illiashenko, O. A, et.al. (2014) “Security Informed Safety Assessment of NPP I&C Systems: GAP-IMECA Technique”, International Conference on Nuclear Engineering, Volume 3: Next Generation Reactors and Advanced Reactors; Nuclear Safety and Security, ASME, 22nd International Conference on Nuclear Engineering ICONE

20.S. Monk, “Programming the Raspberry Pi: Getting Started with Python”, McGraw Hill Professional, 2015, 192p.

21.J. Blum, “Exploring Arduino: Tools and Techniques for Engineering Wizardry”, Jonh Willey & Sons, 2013, 384p.

22.Raspberry Pi Official page, <https://www.raspberrypi.org/products/raspberry-pi-3-model-b/>

23.Banana Pi Official page, <http://www.banana-pi.org/>

24. Cubieboard Forum page, <http://cubieboard.org/model/cb4/>
25. Poschmann, A., Leander, G., Schramm, K., Paar, C., (2007) "New Light-Weight Crypto Algorithms for RFID", 2007 IEEE International Symposium on Circuits and Systems, New Orleans, LA, pp. 1843-1846.
26. Waleed, A. K. A., Kharchenko, V., Uzun, D., Solovyov, O., (2017) "IoT-based physical security systems: Structures and PSMECA analysis," 2017 9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Bucharest, 2017, pp. 870-873.
27. Gorbenko, A., Kharchenko, V., Tarasyuk, O., Furmanov, A. (2006) "F(I)MEA-technique of Web Services Analysis and Dependability Ensuring", Lecture Notes in Computer Science, vol. 4157, 2006, pp. 153-167.
28. Babeshko, E., Kharchenko, V., Gorbenko, A. (2008) "Applying F(I)MEA-technique for SCADA-based Industrial Control Systems Dependability Assessment and Ensuring". Third International Conference on Dependability of Computer Systems DEPCOS-RELCOMEX, 2008, pp. 309-315
29. Kharchenko, V., Illiashenko, O., Kovalenko, A., Sklyar, V., Boyarchuk, A., (2014) "Security Informed Safety Assessment of NPP I&C Systems: GAP-IMECA Technique", Proceedings of the 22nd International Conference on Nuclear Engineering ICONE, Prague, Czech Republic.
30. Illiashenko, O., Babeshko, E. (2012) "Choosing FMECA-based techniques and tools for safety analysis of critical systems" Information & Security: An International Journal, 2012, no. 28(2), pp. 275-285
31. Tempus SEREIN project official website <http://serein.eu.org/>
32. Erasmus+ ALIOT project official website <http://aliot.eu.org/>
33. <https://www.ncl.ac.uk/postgraduate/courses/degrees/computer-security-resilience-msc/>;
34. <https://apps.uc.pt/courses/en/course/7281>;
35. <https://www.kth.se/student/kurser/program/TSMKM/20122/arskurs2?l=en>
36. <https://www.findamasters.com/masters-degrees/?Keywords=physical+security>

PART XIV. IOT FOR INDUSTRIAL SYSTEMS

52. STRUCTURES, MODELS AND TECHNOLOGIES FOR DEVELOPMENT OF INDUSTRIAL IOT-BASED SYSTEMS

Prof., DrS Yu. P. Kondratenko, Assoc. Prof., Dr. O. V. Kozlov,
Senior Researcher O. V. Korobko, PhD Student O. S. Gerasin,
PhD Student A. M. Topalov (PMBSNU)

Contents

Abbreviations	739
52.1 General approach to structures and models building of IoT-based industrial systems	740
52.1.1 The current state of development and implementation of the IoT	740
52.1.2 The basic principles and levels of the IoT	742
52.1.3 Branched structures and models of industrial systems based on the IoT	745
52.2 IoT technologies for monitoring and control tasks implementation in industry	747
52.2.1 Wired and wireless technologies for IoT networks building..	747
52.2.2 Software components and protocols for IoT wired networks.	750
52.2.3 Software components and protocols for IoT wireless networks	752
52.3 Security problems in industrial IoT-based systems	756
52.3.1 Main types of attacks in the Internet.....	756
52.3.2 Recognized standards for data encryption in industrial networks based on IoT	758
52.3.3 Security policy of industrial systems based on IoT	760
52.4 Work related analysis	763
Conclusions and questions.....	766
References	768

Abbreviations

AES – Advanced Encryption Standard
ALG – Application Level Gateway
API – Application Programming Interface
BLE – Bluetooth Low Energy
CoAP – Constrained Application Protocol
CPU – Central Processing Unit
CSMA/CD – Carrier Sense Multiple Access with Collision Detection
DCE – Data Communications Equipment
DES – Data Encryption Standard
DoS – Denial of Service
DSSS – Direct-Sequence Spread Spectrum
DTE – Data Terminal Equipment
HTTP – HyperText Transfer Protocol
IETF – Internet Engineering Task Force
IIoT – Industrial Internet of Things
IoT – Internet of Things
M2M – Machine-to-Machine
MAC – Medium Access Control
MQTT – Message Queuing Telemetry Transport
OFDM – Orthogonal Frequency-Division Multiplexing
SCADA – Supervisory Control And Data Acquisition
WEP – Wired Equivalent Privacy
WLAN – Wireless Local Area Network
WPA – Wi-Fi Protected Access
WPAN – Wireless Personal Area Network

52.1 General approach to structures and models building of IoT-based industrial systems

52.1.1 The current state of development and implementation of the IoT

Basically the Internet of Things (IoT) is a network consisting of interrelated physical objects (“things”) or devices that have built-in sensors and software that allows you to transfer and exchange data between the physical world and computer systems by using standard communications protocols. In addition to sensors the network can have actuators embedded in physical objects and linked together with wired or wireless networks. These interrelated objects (“things”) have the ability of data reading and actuating according to the control signals, the functions of programming and identification, as well as allow excluding the need for human participation by using the intelligent interfaces [1]. The basis of IoT approach is a possibility of connection all kinds of objects (“things”) that people can use in everyday life, such as refrigerator, car, bicycle, washing machine, etc. All of these objects (“things”) should be equipped with built-in sensors that are able to process information coming from the environment, share it and perform different actions depending on the received information. The ideology of the IoT is aimed at increasing of economic efficiency by processes automation in various fields of activity and elimination the need for human participation in them.

According to statistics in 2014, Internet-connected devices were about 3.807 billion. In 2016 - 5.88 billion devices, which is already 30% more than in 2015, and by 2020, Gartner predicts that the number of things connected to the Internet will be increased up to 20.8 billion [2]. Some other analytical agencies have even more optimistic predictions that by 2020 the number of devices connected to the Internet will reach, or perhaps exceed, 50 billion. At the same time, revenue from the sale of equipment, software and hardware and services will amount to 1.9 trillion dollars. The world's largest IT companies have already started the race for leadership in this market.

Let's take a look at the main areas of IoT development.

Home automation. In this field the “Smart house” systems are used, that are the residential extension of building automation and

realize the control and automation of lighting, air conditioning, ventilation, heating and security. Such systems include different switches and sensors, washers, dryers, ovens, refrigerators and other home devices, that are connected to a central hub for remote monitoring and control. The user interface can be interacted with a wall-mounted terminal, tablet, laptop, mobile phone software or a web interface via internet cloud services. The most popular communications protocols for such systems are: Ethernet, RS-485, Bluetooth LE (BLE), ZigBee, Z-Wave and others [3-5].

Environmental monitoring automation. IoT applications for environmental monitoring use different sensors to aid in the field of environmental protection [3, 6, 7]. These IoT systems can implement monitoring of air and water quality as well as soil and atmospheric conditions. Also, the IoT applications for tsunami and earthquake early-warning systems can be used by emergency services to provide more effective aid. IoT devices in this application should be enough mobile because they cover a large geographic area.

City infrastructure automation. In this field the “Smart city” systems are used, that implement monitoring and controlling operations of urban and rural infrastructures like bridges, railway tracks, on- and offshore- wind-farms etc [3, 7]. The IoT infrastructure can be used for monitoring and control of any parameters of urban objects that can increase safety and compromise risk. For example, the IoT system for city automation can calculate and predict the energy balance point of the city for a certain period of time, automatically sending the control data to generators, power grids and smart household devices in order to maintain the required energy balance. Municipal companies can save large sums of money, while continuing to maintain the reliability and integrity of the power supply instead of buying new equipment.

Transport automation. The IoT can assist in monitoring, control, and information processing across various transportation systems [7, 8]. IoT systems can help to configure dynamically switching of traffic lights and adjustable exits from highways, thereby reducing congestion and improving traffic flow in real-time, rather than in predictive models. Application of the IoT extends to all aspects of transportation systems: smart parking, smart traffic control, vehicle control, fleet management and logistic, electronic toll collection systems, road assistance, etc.

Industrial automation. The application of the IoT in the manufacturing industry is called the Industrial Internet of Things (IIoT) [9, 10]. The IIoT will revolutionize manufacturing by enabling the acquisition and accessibility of far greater amounts of data, at far greater speeds, and far more efficiently than before. A number of innovative companies have started to implement the IIoT. The company "Inductive automation" developed the only IIoT platform "Ignition" with effective Message Queue Telemetry Transport (MQTT) data transfer protocol and full-featured Supervisory Control And Data Acquisition (SCADA) functionalities built right in. "Ignition's" cross-platform compatibility and flexible modular configurability make it the world's first truly universal industrial application platform. "Ignition" empowers you to connect IIoT data across your entire enterprise, launch clients to any device equipped with a web browser, rapidly develop automated systems without any limits.

The main complexity of the IoT approach application in the industry is that "things" in the industrial systems are complex technical objects, such as internal combustion engines, industrial robots, steam turbines, chemical reactors, cargo cranes, lathes, etc., that are involved in the performance of complex technological processes. For the productive carrying out of these technological processes it is necessary to implement monitoring and automatic control of their technical objects main process parameters via the internet with high quality indicators in the real time mode. Any technical malfunctions or errors, caused by the incorrect control, slowing down of the performance, loss of the Internet for some time, etc., can lead to a reduction of an economic efficiency or serious industrial accidents sometimes even with human victims.

Thus, the IIoT systems should include highly efficient software and hardware means for the implementation of specialized algorithms of monitoring and automatic control. Also, such systems should have an increased level of reliability, performance and information security.

52.1.2 The basic principles and levels of the IoT

The basic principles and levels of the IoT are formulated in the general scheme of the combination of physical and virtual things, which is presented in Fig. 52.1.

In turn, Fig. 52.1 shows that virtual things can exist without their physical incarnations, whereas physical objects / things necessarily correspond to at least one virtual object. The leading role is played by devices that can collect different information and distribute it over communication networks in various ways: via gateways and through the network; without gateways, but through the network; directly with each other. Recommendation Y.2060 describes a different combination of these types of connections. This indicates that the use of IoT provides a host of network technologies - global networks, local area networks, ad-hoc wireless networks and mesh networks. These communication networks transfer data collected by devices to the corresponding software applications, as well as transmit commands from software applications to devices.

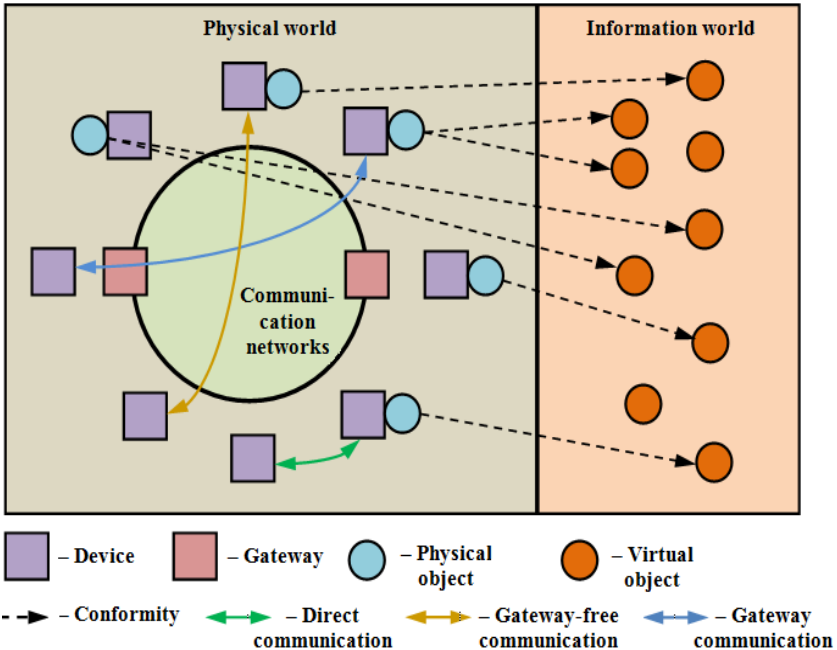


Fig. 52.1 – Scheme of reflection of physical and virtual things

It should be noted that things and their associated devices can have full control processors for processing data in the form of "system-on-

crystal", including its own operating system, sensor unit and communication unit.

It is considered that the IoT is based on three basic principles: 1) the widespread communication infrastructure; 2) the global identification of each object; 3) the ability of each object to send and receive data through a personal network or the Internet to which it is connected.

The most important differences of the Internet of things from the existing Internet of people are: the focus on things, and not on a person; considerably more connected objects; significantly smaller objects sizes and low data rates; the focus is on reading information, not on communications; the need to create a new infrastructure and alternative standards.

The IoT includes three main levels: components, structural units and system of systems. The basic features depend on the components. The structural blocks cover products technologies that arise as a result of the integration of new Internet components with traditional technology components. The system of systems describes unique ways of the possible integration and integration of structural units as well as the construction of their structures in various fields.

The components are designed for a specific application and therefore - for solving a specific task. Depending on this task, different sensors (light, movement, heat, etc.) are used to monitor parameters and actuating mechanisms (motors, damper, etc.) to control these parameters.

Structural blocks are common elements for many solutions, which are extremely important for successful work (I/O devices, control and processing devices). Structural blocks are the basis of many solutions and include communication modules, security and analytics, remote computing nodes and update modules. Other examples of structural blocks include the following: software, mobile devices, various security and privacy technologies, as communication and network technologies, home automation technologies (including monitoring and measurement of indicators) as well as Internet and network protocols (such as IPv6).

Structural blocks are used to create systems that are then merged into system of systems. For example, a car is a system consisting of numerous structural units and components. The system of street traffic systems allows the car and driver to interact with the street systems to

navigate routes and traffic. For car manufacturers, the context is shifted to consumer support systems. The collected information on safety, conditions and driving style as well as maintenance records are transferred to the customer support system of the manufacturer, creating a system of customer service. In both scenarios, the IoT solutions deal with the co-ordination and interaction of many smaller systems, each of which has its own level of autonomy, dependency and interaction.

52.1.3 Branched structures and models of industrial systems based on the IoT

Modern Internet technologies provide opportunities for developing complex data processing programs in monitoring and control systems. These systems have modular structures with robust and highly effective software and hardware as well as industrial communication interfaces for monitoring and automatic control in a safe and uninterrupted mode.

Industrial systems based on the IoT, as a rule, combine four stages of automated production: the presence of a technological process; collecting data from sensors; data analysis; taking measures to improve the quality of the technological process.

There are different types of connection of software and hardware for the construction of branched structures and models of industrial monitoring and control systems based on the IoT [11-17].

Device-to-device connection. A communication model device-to-device represents two or more devices connected and communicating with each other directly and not through an intermediate server. These devices communicate over different types of networks, including networks based on the IP protocol or the Internet. However, these devices often use protocols such as: WiFi, Bluetooth, Z-Wave or ZigBee - to establish direct connection from device to device [6].

These networks with device-to-device communications allow devices that support a specific protocol to communicate and exchange messages to perform their functions. This communication model is commonly used in simple automation systems that use small data packets to establish communication between low-level devices in the area of speed and security of data transmission. The devices themselves are equipped with built-in security mechanisms. IoT devices, such as:

bulbs, switches, thermostats and door locks, exchange small amounts of information in the automation system (for example, a message about the status of the door lock or the command of light inclusion).

Device-to-cloud connection. In the device-to-cloud communication model, the IoT connects to a cloud-based Internet service such as an application's rental service provider for data exchange and message traffic management. In this approach, existing communication mechanisms are often used, such as traditional Ethernet or Wi-Fi wired connections to establish a connection between the device and the IP network, which, in turn, connects to the cloud service. In this approach, the cloud connection allows the operator to receive remote access to the device through the web interface of a smartphone, industrial PC (Personal Computer), etc.

Device-to-gateway connection. In the case of a connection model between the device and the gateway, or, most often, in the device connection model to the Application Level Gateway (ALG), the IoT device connects via the ALG service as a channel for using the cloud service. Simply put, this means that the application software operates on a local gateway device that acts as an intermediary between the device and the cloud service, and also provides security and other functions such as data or protocol transformation.

Another variation of this model to connect the device to the gateway are devices that act as a hub in automation software applications. These devices are used as a local gateway between individual IoT devices and cloud services, but they can also fill in the gaps between the devices themselves. For example, the SmartThings Hub is a separate gateway device with Z-Wave and Zigbee transceivers installed to maintain communication with both types of devices. The hub connects to the SmartThings cloud service, which allows the user to access the devices through a specialized program and an Internet connection. This communication model is often used to integrate new smart devices into a traditional system with devices that initially can not interact with them. The disadvantage of this approach is that the need to develop a system and a gateway of application level increases the complexity and cost of the system as a whole.

Model of data sharing on the server. The model of data sharing on the server is consistent with the architecture that allows users to export and analyze data of intelligent objects from a cloud service in

conjunction with data from other sources. This architecture supports the desire of users to give third-party access to downloaded sensor data.

The data sharing model on the server provides a unified cloud service approach. Otherwise, you need regional application programming interfaces (APIs) to ensure the interoperability of cloud-based data from smart devices.

However, intermediate additional I/O (input/output) modules, controllers and other means for constructing large branch information-measuring and controlling systems of industrial purpose may also be used, regardless of the connection structure.

52.2 IoT technologies for monitoring and control tasks implementation in industry

52.2.1 Wired and wireless technologies for IoT networks building

The development and improvement of complex IoT networks with a variety of technological content is accompanied, above all, by the widespreading of wireless networks, the emergence of cloud computing, the development of inter-machine interaction technologies and the development of software-configuring networks, the start of active transition to IPv6 protocol.

Identification tools. The special equipment for information recording and processing as well as for actuators controlling is involved in any IoT system. Obviously, for the effective functioning of the IoT system it is necessary to ensure a high level of network service and consequently the unique identification of software and hardware elements of the system. The identification problems for connected devices depend on the number of concurrent connections to the Internet, which the given system can support, and on the quality of service, which can be guaranteed. Now the majority of Internet-connected devices use IPv4 protocol from the family of TCP/IP protocols, which is based on 32-bit addressing scheme and is limited to 2^{32} (4 294 967 296) unique addresses. Considering that predicted for the IoT possible number of connected units is 50-100 billion for optimal scalability it is required to move to IPv6 protocol from the family of TCP/IP protocol, which uses 128-bit addressing system capable of supporting up to 2^{128} addresses ($3,4 \cdot 10^{38}$ units).

Measuring instruments. By measurement means of the object measuring transducers are generally understood, that are designed to generate measurement data in a form, suitable for transmission, further transformation, processing and storage. The IoT technology uses a wide class of measurement tools, from the elementary sensors (temperature, rotation angle, etc.), consumption metering devices (smart meters) to complex integrated measurement systems. Also, all measuring devices are combined, as a rule, in the wired/wireless intelligent sensor networks, due to what is possible to build M2M interaction systems.

Data processing means. For the processing and storage of data, given from the sensors, it is advisable to use embedded software and hardware means in the form of small-sized computers (for example, Raspberry Pi, Intel Edison) with access to the Internet . Moreover, the final processing of the data and making an informed decision on the cloud service is performed with the use of Big Data technologies. The main difference between Big Data and "ordinary" data is that it is impossible to process these data with traditional database management systems and business intelligence solutions because of their large volume and diverse composition. Another important property of them is the accelerated accumulation of data and their continuous change. Such popular tasks as data reduction, obtained from different sources (Data Cleaning, Data Merging, De-duplication), require special analysis methods in case of inaccurate data, especially huge data. For the processing of measurement data today are available for free in the test mode such cloud services as: Azure, Freeboard, Grovestreams, Developer.ibm, Thingspeak, Thingworx and other.

Data transmission means. The range of possible data transmission technologies covers all possible means of wireless and wired networks. Among wired technologies of software and hardware components interaction the long-established industry network standards are used in the IoT, such as Profibus, Canbus, LON, Modbus, etc. It should be also noted, that for the software and hardware elements connection to the Internet the standard family of protocols TCP/IP is basically used in the IoT. Moreover, today for the networks service development in the IoT according to the standard IEEE 802.15.4 it is especially important to use the open 6LoWPAN protocol, standardized by Internet Engineering Task Force (IETF), that allows combining the intellectual sensors in the Internet with a low data rate.

For wireless transmission of data between the software and hardware elements of the IoT networks a particularly important role play such qualities as efficiency in conditions of low speeds, resilience, adaptability, the ability to self-organization. Therefore, the class of wireless personal area networks (WPAN) is actively used. Currently WPAN can be with a short range (up to 10 m) and with increased range (up to 100 m), which allows them to be located on the functional capabilities at the junction with the wireless local area networks (WLAN). WPAN can be created based on different technologies of the IEEE 802.15.4 standard: ZigBee, WirelessHart, MiWi, etc.

The industrial systems based on IoT use different network technologies [12-14]. Typically, computerized monitoring and control systems of the technological process consists of three levels: the first - the level of sensors and actuators, the second - the level of peripheral control devices, the third - the level of operators. At the first and second levels the industrial networks (Fieldbus) are used, which include Profibus, CANbus, Modbus and many others. At the third level Ethernet and TCP/IP protocol are the most widely used. Wireless technologies are increasingly and more widely used in measurement and control systems at different levels of the hierarchy. The most common wireless data transmission technologies in the production are: Bluetooth, Wi-Fi, WiMAX, GPRS.

The main advantage of a wired network is high speed and stable operation, and the main plus of a wireless network is mobility (lack of conductive connections). It should be noted that wireless technologies are actively developing and increasing the speed of data transmission and improving the stability of networks.

The disadvantages of wired networks are the following: high cost in building with a large number of devices (network elements); the complexity of system expansion, additional cost for expansion, especially when using the "star" topology; very poor mobility of network devices.

Among the disadvantages of wireless networks, one can note the following: low noise immunity; low communication reliability; low security level.

Regardless of wired or wireless networks the connection from device to the Internet is carried out by the basic data transfer protocols, among which are: Constrained Application Protocol (CoAP),

HyperText Transfer Protocol (HTTP), Message Queuing Telemetry Transport (MQTT) and others [6, 18-20].

HTTP is an application-level protocol, the messaging in which goes through the usual "request-response" scheme. HTTP uses the global uniform resource identifiers (URIs) to identify resources. Unlike many other protocols, HTTP does not save its status. According to this protocol, the client and server should not be aware of previous queries and replies.

MQTT is an exchange protocol that implements the publish/subscribe model. The MQTT protocol is located on top of the TCP/IP and works with the client/server model, where each device is a client and is connected to a server, which, in turn, is a broker. The MQTT protocol requires a mandatory presence of the broker, which manages the distribution of data to subscribers. All devices send data only to the broker and accept data only from him.

Consequently, the HTTP protocol uses a request/response model, which is currently the most common message exchange protocol. MQTT, in turn, uses a publish/subscribe pattern.

CoAP is a protocol developed by the IETF Internet Engineering Board. The protocol operates at the application level and is intended for data transmission over lines with limited throughput. The CoAP was developed on the basis of the HTTP protocol. Conceptually CoAP is compatible with HTTP except that it's designed for devices with constrained resources like sensors and microcontrollers that have restricted memory and bandwidth capabilities. It should be noted that unlike HTTP, CoAP has a compact binary format. While conceptually it might seem like a subset of HTTP, in reality the wire protocol is very different. CoAP is designed for constrained platforms where every bit and central processing unit (CPU) cycle matters.

52.2.2 Software components and protocols for IoT wired networks

In the wired networks of industrial systems based on IoT, the following standards are often used: EIA-RS-232; EIA-RS-422; EIA-RS-485; Hart; IEEE 802.3 - Ethernet; IEEE 802.5 - Token ring.

In accordance with these standards, industrial protocols and networks are being developed. The most commonly used

communication standards for measuring technologies are given in Table 52.1.

Interface RS-232, RS-485 and Modbus RTU network. RS 232 is the interface standard for data interchange between two devices via serial data transmission (asynchronous or synchronous communication), which is used in serial ports of computers and other devices. The RS-232 provides data and some special signals transfer between the terminal (Data Terminal Equipment, DTE) and the Data Communications Equipment (DCE) up to 15 meters at a maximum speed (20 kbps). The interface protocol provides two modes of data transmission (synchronous and asynchronous) as well as two methods of data management: hardware and software. Each mode can work with any control method.

Table 52.1 – Basic standards used in measuring technologies

Type	Title	Maximum distance	Maximum speed transmission
1	2	3	4
RS-232	Sequential interface	15 m	20 kbps (larger for short connections)
RS-423A	Sequential interface	1200 m	100 kbps for connections up to 30 m
RS-422A	Sequential interface	1200 m	10 Mbps
RS-485	Sequential interface	1200 m	10 Mbps
USB	Universal serial Bus	15 m	12 Mbps (480 Mbps for US 2.0)
IEEE-1394	Fire Wire	4.5 m (72 m between the most remote nodes)	400 Mbps (3.2 Gbps for IEEE-1394b)
EPP, ECP	Contronics	15 m	500 kbps
MXI-3	Multi-system Extension Interface	200 m for light guide, 10 m for copper wire	1,5 Gbps

RS 485 is the data transmission standard of two-wire, half-duplex multipoint serial communication channel. The data transmission is carried out using a differential method of signal transmission, when the voltage, corresponding to the level of the logic unit or zero, is measured as the potential difference between the two transmission lines: Data + i Data-.

RS-485 provides data transfer speeds up to 10 Mbps. The maximum range depends on the speed: at a speed of 10 Mbps, the maximum length of the line is 120 m, at a speed of 100 kbps - 1200 m. Moreover, one transmitter is designed for control of 32 standard receivers.

RS interfaces are most commonly used in industrial automation. They are used by industrial networks Modbus RTU, Profibus DP, ARCNET, BitBus, WorldFip, LON, Interbus and many non-standard networks.

The Modbus RTU network is currently well known, which is due, first of all, to the compatibility with a large number of equipment that has the Modbus RTU protocol. In addition, Modbus RTU has a high reliability of data transmission associated with the use of reliable error control method.

Ethernet and Modbus TSP/IP network. Currently Ethernet is the family of products for LANs that are compliant with IEEE 802.3. In industrial automation the most commonly used physical interfaces according to IEEE 802.3 are 10Base T and 100Base FX. 10Base T means the physical interface specification for 10 Mbps with the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) access method that uses two twisted pair wires. Ethernet allows to organize multi-master networks of different topologies.

Modbus TCP protocol (or Modbus TCP/IP) is used to connect devices to an Ethernet or Internet network. It uses the Modbus RTU frames and the TCP/IP family of protocols. That is, Ethernet TCP/IP is used for transporting a modified Modbus RTU frame.

52.2.3 Software components and protocols for IoT wireless networks

Wireless networks especially grow largely by adding vast amounts of small Internet of Things devices with minimum hardware, software

and intelligence, limiting their resilience to any imperfections in all their functions. Based on the research of the growing network complexity, caused by the Internet of Things, predictions of traffic and load models will have to guide further research on unfolding the predicted complexity to real networks, their standards and on-going implementations.

Wireless networks that are built with the use of radio waves have become the most widespread. These networks can be divided into local and global. In addition, increasingly introduced mobile networks (GSM/GPRS, 3G, 4G), that are actively developing. Comparison of speed and range of basic wireless networks is presented in Fig. 52.2.

Wi-Fi wireless data transmission technology. Wi-Fi is one of the most widely used wireless networking technologies and is based on the IEEE 802.11 standard. The IEEE 802.11 standard defines the protocols required for the organization of WLANs. The main of them are: the Medium Access Control (MAC) protocol and the physical signals transmission protocol PHY. As the main method of accessing the environment, the CSMA/CA mechanism is defined in standard 802.11.

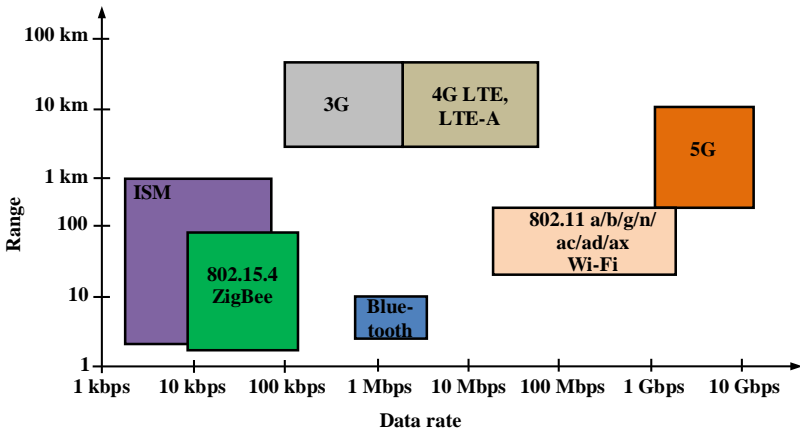


Fig. 52.2 – Graph of speed and range of main wireless networks in terms of direct visibility

The 802.11 standard exists in several basic forms. The original version of this standard is 802.11b. It operates in the 2.4-2.483 GHz unlicensed band. It uses the direct-sequence spread spectrum (DSSS) and is capable of data rates up to 11 Mbps in a range of up to 100 m. This frequency band is divided into 11 channels, each 22 MHz wide. Another popular version of the standard is 802.11g. It is a faster version of Wi-Fi that also operates in the 2.4-GHz band. It can achieve data rates as high as 54 Mbps up to 100 m. It uses Orthogonal Frequency-division Multiplexing (OFDM) with 52 subcarriers. Also there is a variant of the standard is 802.11n, which uses OFDM and MIMO (Multiple Input Multiple Output) to achieve even higher data rates up to approximately 600 Mbps. In addition a less popular version 802.11a exists, which uses the 5-GHz unlicensed band. It also uses OFDM and can achieve data rates up to 54 Mbps. Even newer and faster versions are available. 802.11ac uses the 5 GHz band and can produce data speeds up to several Gbps under the most favorable conditions. It uses wider 80 and 160 MHz bands and higher-level 256-QAM (Quadrature Amplitude Modulation) as well as increased MIMO configurations.

Bluetooth wireless data transmission technology. Bluetooth technology is based on the IEEE 802.15.1 standard and is used in compact communication systems between small personal computers, mobile phones and other devices. It is a low-speed data transmission method. Bluetooth operates in the same 2.4-2.483 GHz unlicensed spectrum as a Wi-Fi. It uses a technique known as frequency-hopping spread spectrum (FHSS), where the data is divided into chunks and transmitted via a carrier that hops from one random frequency to another. Data is transmitted at a 1-Mbps rate using FSK (Frequency Shift Keying). An enhanced data rate form of Bluetooth is also available to transmit at higher speeds up to 3 Mbps. The range is 10–50 m depending on the environment. The standard is managed by the Bluetooth Special Interest Group.

More recent versions of Bluetooth use a different form of FHSS and are designed to operate on less power. The Bluetooth Low Energy (BLE) is available in several forms for data rates of 1 or 2 Mbps. BLE nodes can operate for years from a single button cell because of the very low current drain. A newer version of BLE called Bluetooth 5 uses different modulation and coding schemes to achieve data rates to 2 Mbps over a longer range up to 50 m or more.

ZigBee wireless data transmission technology. ZigBee is another short-range PAN (Personal Area Network) technology with the IEEE designation 802.15.4. It uses low power, so the range is typically 100 m or less, basically depending on the antennas and the physical environment where it is used. ZigBee also operates in that unlicensed spectrum from 2.4 to 2.483 GHz.

The IEEE 802.15.4 standard defines the basic radio technology. It uses DSSS and a version of QPSK (Quadrature Phase Shift Keying) that gives a data rate of 250 kbps. The frequency spectrum is divided into 16 1-MHz channels. A major feature of the ZigBee technology is its ability to perform mesh networks. While a typical ZigBee radio node may only have a range of 30 m or less, the range can be extended by simply transmitting data from one node to another in a mesh network that may cover hundreds of meters or in some cases even miles. Mesh networks have many different paths for data and, therefore, are extremely reliable.

Global Mobile Wireless Networks GSM, GPRS, 3G, 4G. GSM technology (from the name of Special Mobile Group, later renamed Global System for Mobile Communications) - global digital standard for mobile communications with channel division by TDMA (Time Division Multiple Access) principle and a high degree of security through public key encryption. Communication is realized on two main frequencies 900 and 1800 MHz. The maximum radiated power of mobile phones of the standard GSM-1800 - 1W, for comparison in GSM-900 - 2W. For data transfer there are technologies of CSD (Circuit Switched Data), GPRS (General Packet Radio Service) and EDGE GPRS. With their help the following speeds in data transmission can be achieved: CSD - 9.6 kbps; GPRS - 53.6 kbps; EDGE - up to 384 kbps.

GPRS is an add-on to GSM packet data transfer technology. It has data transmission speeds up to 171.2 kbps. More modern than GSM and GPRS technologies is UMTS (Universal Mobile Telecommunications System, 3G, 4G). Using the development of W-CDMA (Code Division Multiple Access), UMTS supports the speed of data transfer at the theoretical level up to 21 Mbps (HSPA +).

52.3 Security problems in industrial IoT-based systems

52.3.1 Main types of attacks in the Internet

The concept of functional safety means that the system correctly and fully implements those and only those goals that correspond to the intentions of its owner, and functions in accordance with existing requirements. The concept of proper information security concerns the safety of the process of technical information processing and is the property of a functionally secure system. Such a system should prevent unauthorized access to data and prevent their loss in the event of a malfunction [21].

Information security is the state of the security of systems of data processing and storage in which the confidentiality, availability and integrity of the information is ensured, or a set of measures aimed at ensuring the protection of information from unauthorized access, use, disclosure, destruction, modification, inspection, verification, recording or destruction. There are different types of attack classification. For example, division into active and passive, external and internal, intentional and unintentional, etc.

Mailbombing. The oldest type of attacks. Significantly increases the traffic and the number of messages sent, which generates a failure in the work of the service. This causes paralysis of not only mail but also the work of the mail server itself. The effectiveness of such attacks today is considered zero, because now the provider has the ability to set traffic restrictions from one sender.

Buffer overflow. The principle of this type of attacks is software errors, in which memory is in breach of its borders. This, in turn, forces to complete the process crashing, or run an arbitrary binary code that uses the current account. If the account is administrator, then these actions allow you to get full access to the system.

Viruses, trojans, post worms, sniffer. This type of attacks combines various third-party programs. The purpose and principle of such a program can be extremely different, so it makes no sense to dwell in detail on each of them. All these programs combine the fact that their main goal is access and "infection" of the system.

Network intelligence. This type of attacks itself does not involve any destructive action. Intelligence means only collecting information by an intruder - external or internal scan of the network without authorization in it - port scanning, DNS request, computer security check and system validation. Usually intelligence is conducted before a serious targeted attack.

Sniffing packages. The principle of operation is based on the features of the network card. Packages received by the system are sent to processing, where special applications interact with them. As a result, the attacker gets access not only to information about the structure of the computer system, but also to directly transmitted information - passwords, messages and other files.

IP-spoofing. The type of attacks on local networks when an attacker computer uses an IP address that is part of this local network. Attack is possible if the security system requires identification of the IP address type, excluding additional conditions.

Man-in-the-middle. An intruder intercepts a communication channel between two applications, which results in access to all information that goes through this channel. The purpose of the attack is not only theft, but also falsification of information.

Denial of Service (DoS). An attack that has the purpose of forcing the server to not respond to queries. This type of attack does not imply directly obtaining some secret information, but is used to paralyze the work of targeted services.

The remote industrial location of the sensors and their automatic operation increases their vulnerability to third-party intrusions and attacks. It is easy enough to intrude into a wireless connection to intercept packets transmitted by the sensor. For example, the biggest threat is the threat of a denial-of-service attack, the purpose of which is to disrupt the correct functioning of the sensor network. This can be achieved by various methods, for example, by feeding a powerful signal that prevents sensors from exchanging information ("white noise" or "jamming attack"). There are various ways to protect systems from intruders, but for many of them you need high requirements for hardware resources, which is difficult to achieve due to limitations on many sensor requirements. Consequently, sensory wireless networks require new solutions in the field of data protection, providence of

identification, creation of complex keys among legitimate users of the networks.

Unauthorized access. It is also possible to monitor applications running on the network and effortlessly, if appropriate precautions are not taken, to access the wireless network being out of the placement where it operates. For example, someone sitting nearby in a parked car can connect to one of the base stations located in the building. The adequate protection is not provided, the person will be able to access data transmitted over the wireless network. Usually the main reason for such problems is the use of the base station configuration, which is set by default and does not provide the required level of protection, which causes unimpeded access to network computers.

52.3.2 Recognized standards for data encryption in industrial networks based on IoT

An encryption device using an pseudorandom numbers sensor is most often used in the software implementation of the cryptographic data protection system. This is due to the fact that on the one hand, it is quite simple for programming, and on the other hand, it allows to create algorithms with very high cryptostability. In addition, the efficiency of this encryption tool is high enough. In the industry, systems based on the encryption means using a pseudorandom numbers sensor, can encrypt several hundreds of kilobytes of data per second. Taking into account the experience of the developers of the encryption algorithms and the means of their implementation [21-24], we note that each new algorithm of data encryption before its application should be a subject of comprehensive mathematical, statistical and cryptographic analysis. Let us consider the most common data encryption standards.

One of the most common cryptographic standards for encryption of data used in USA is Data Encryption Standard (DES). The DES standard is used by federal departments and agencies to protect all sufficiently important data in computers (except for some data whose security means are determined by special acts). It is used by many non-state institutions, including most banks and money-handling services. The main advantage of DES is that it is standard. According to the US National Bureau of Standards, the algorithm has the following properties: high level of data protection against decryption and possible

modification of data; simplicity and understanding; a high degree of complexity, which makes its disclosure more expensive than the profit received; economic in realization and effective in speed.

The specified properties of DES favorably distinguish it from the encryption tool using a pseudorandom numbers sensor. However, DES also has a number of shortcomings.

The most significant disadvantage of DES, that experts consider, is the size of the key, which is considered too small. To decrypt information by means of key selection it is enough to execute 2^{56} decryption operations (that is, only about $7 \cdot 10^{16}$ operations). Therefore, the direct development of DES is currently the Triple DES (3DES) algorithm. In 3DES, encryption / decryption is performed by running the DES algorithm threefold.

RSA Cryptographic Algorithm. RSA (abbreviation of the names Rivest, Shamir and Adleman) is an open-source cryptographic algorithm based on the computational complexity of the factorization of large integers. The algorithm is used in a large number of cryptographic applications, including PGP, S/MIME, TLS/SSL, IPSEC/IKE and others [11]. It is very promising because encryption of information does not require the transfer of the key to other users. It advantageously distinguishes it from all of the above cryptographic data protection means.

Among the advantages of the RSA tool a very high cryptostability should be considered as well as quite simple software and hardware implementation. However, as in the previous standard, the use of this tool for cryptographic data protection requires a high level of development of computer technology.

It should be noted separately that in the modern access points of wireless networks the following methods of data encryption are also used:

– WEP (Wired Equivalent Privacy) is a wireless network protection standard based on the streaming coding method using the RC4 algorithm (using a common secret key). There are variants of encryption with a length of the key of 64, 128 and 256 bits. The use of WEP for network protection can not be considered enough a reliable way to guarantee security. The problem is to realize the choice of the

initialization vector used as a pseudorandom sequence for data encryption;

- WPA (Wi-Fi Protected Access) is one of the security standards used to protect wireless networks. Created to replace the outdated WEP protocol. Based on TKIP (Temporary Key Integrity Protocol), which effectively addresses the problem that is at the core of the vulnerability of the WEP standard - the reuse of encryption keys;

- AES (Advanced Encryption Standard) is the standard of symmetric block encryption (block length is 128 bits), 128-bit keys are supported, but can be maintained also longer ones - 192-bit and 256-bit.

52.3.3 Security policy of industrial systems based on IoT

Policy of the information security (IS) of any organization - a set of requirements, rules, restrictions, recommendations that regulate the organization of information activities in the organization and aimed at achieving and maintaining the state of its IS [22, 23].

Currently, there are two trends in industrial control systems: the gradual transition of control means to Ethernet standard and TCP/IP protocols, and the emergence of specific industrial malware that attack specific types of industrial control systems. This trend in the industry has seriously affected the interconnection of processes within the control systems in the direction of their complications. Construction of networks of automatic control system of technological processes (ACSTP) according to the principle of office networks has led to the migration of the vulnerabilities of the latter into the industrial IT-loop. The PLC and other field-level controls, together with an Ethernet connection, have become open to new sources of threats that their developers did not expect. As a result, the number of failures and downtime due to harmful software and cyber attacks has increased seriously.

Here are 11 steps you need to go for protection against these threats. These steps are taken from NIST (National Institute of Standards and Technology), ISA 99 (Industry Standard Architecture) and other industrial cybersecurity standards integrated into one international standard IEC 62443 (International Electrotechnical Commission).

Step 1. Creating a security policy. First, you must ensure the existence of security policies for system control. If it is not available for the system, it can be borrowed from the organizational policy of the IT department of the enterprise.

Step 2. Installing of network security perimeters. This step involves setting up network security perimeters to restrict access points where third-party software can enter the control system.

Firewalls are used to segment the IIoT system itself and isolate it from other external networks. You need to be sure that all traffic from and to the IIoT system is encrypted and passes through at least one firewall. As part of the IIoT system, firewalls should also be used to protect controllers, industrial wireless networks and network equipment from the category of systems for controlling functionally hazardous objects from workstations. When firewalls and switches are already installed, they need to be serviced throughout the life cycle of the system to maintain their efficiency.

Step 3. Protection of workstations. The given step provides protection for workstations of IIoT system in a way to complicate the path of penetration of malware to the system. Workstations should be limited to engineering functions and all programs, services and ports that are not needed to perform these functions should be removed or disabled to prevent the use of known or not yet known vulnerabilities. Additionally, an industry-specific anti-virus software must be installed to detect and remove known malware before it infects the workstation.

Step 4. Management of user accounts. The given step is completely associated with the users accounts. Users should only provide the privileges that they need, their passwords must be long enough and use combinations of at least three of four elements: uppercase and lowercase letters, numbers, and special characters.

Step 5. Software update. The idea underlying this step is the timely installation of patches and updates related to the security of both the operating system and the entire software of the control system. These fixes allow you to get rid of the vulnerabilities that can be used to infect the software.

Step 6. Software backup and recovery. The given step involves implementing a software backup and recovery plan. All backups should be located on a separate carrier from the workstation, which should be kept in a separate room not connected with the premises of the

workshop or department where the workstation is installed. An effective plan allows you to restore the configuration of the infected system and its software to a stable (non-infected) state.

Step 7. Monitoring and risk assessment. The given step involves the system monitoring for suspicious activity and risk assessment. Security software monitoring packages check log files of workstations, firewalls, switches and other devices on the availability of third-party software. Some software products monitor network traffic, as well as the use of processor and RAM in search of anomalies. Risk assessment should be carried out at the design stage, before commissioning and during the entire period of operation of the system, to ensure that changes in the control system do not lead to a decrease in its safety level.

Step 8. Revision of all used software. It is necessary to conduct a thorough revision of all software used at the workstations to detect uncertified software. If such programs are available, they should be removed as soon as possible from computers and replaced with certified analogues. After this procedure, a new, full-scale validation of the IIoT system should be conducted in order to ensure that the system does not have malicious "bookmarks" from the actions of the removed software.

Step 9. Use of industrial controllers and network devices. The PLC (Programmed Logical Controller) with redundancy of control networks should be used, that is, PLC with two network modules: basic Industrial Ethernet or standard Ethernet, backup - serial interface or standard fieldbus. The switches with port access control protocol 802.1x (authentication protocol of network stations) should be used in industrial Ethernet networks. For critical infrastructure objects, it is recommended to use PLCs with built-in access control protocol for ports 802.1x and/or the built-in AES symmetric block encryption protocol.

Step 10. Zoning (segmentation) of the industrial network. Zoning (segmentation) of the industrial network is a mandatory requirement for the implementation of new control systems of technological processes and the modernization of existing ones. Without fulfillment the requirements of network zoning, the IIoT system can not be accepted for use. Tracking and analyzing of traffic that passes through dedicated

channels helps to prevent DoS attacks and distributing malware, protect adjacent areas, integrity and privacy of traffic.

Step 11. IIoT using. Applicable IIoT technologies at each implementation level should fulfill the following requirements:

- use built-in security (cardOS smart cards based solution);
- use secure communications (hardware protection modules and creation of secure identifiers);
- use identification information management for related objects (trusted infrastructure);
- if possible, not to use for critical production of devices with ZigBee protocol (when using equipment for creating radio interference and 2.4 GHz oscillation process control system loses connection with sensors or misinterprets the signals received from them);
- use https protocol everywhere instead of http. In this case, be sure to use additional antivirus protection of the content;
- use support for two-factor authorization;
- use only server authentication, not authentication on the device;
- use exceptionally safe cloud environments. Digital certificates guarantee full protection when exchanging information through the integration of software with authentication services, the impossibility of denial of authorship and the preservation of confidentiality.

52.4 Work related analysis

The issues discussed above can be supplemented by an analysis of the existing works of European partner universities of the ALIOT project on the topic of the section [25]. Structures, models and technologies for development of industrial IoT-based systems are considered in different university-partners, besides *Leeds Beckett University*, *Consiglio Nazionale delle Recerche - Istituto di Scienza e Technologie dell' Informazione "A.Faedo" (ISTI-CNR)*, *Royal Institute of Technology (KTH)* and *Newcastle University*. So, let's consider the following projects.

The main goal of the proposed in [3] project is to harness the emerging IoT technology to empower elderly population to self-manage their own health and stay active, healthy, and independent as long as possible within a smart and secured living environment. The

developed innovative cloud-based integrated open-sourced IoT ecosystem will provide a one-stop shop for integrated smart IoT-enabled services to support older people who live alone at home (or care homes). The system uses designed an integrated IoT gateway for well-being wearable and home automation system sensors with varying communication protocols.

Another focused on health IoT application developed in [4] exploits heartbeat rate and wrists acceleration data, gathered via smartwatch, in order to identify subject's sleep behavioral pattern. In [5] authors present a practical and scalable solution that aims to achieve the Internet of Things paradigm in complex contexts, such as the home automation market, in which problems are caused by the presence of proprietary and closed systems with no compatibility with Internet protocols. In turn, in the work [6] IoT technology is expected to offer promising solutions for food supply chain and in-home healthcare, which may significantly contribute to human health. An author has investigated the technologies and architectures of the IoT for these two applications as so-called Food-IoT and Health-IoT respectively. A series of research problems about the WSN (Wireless Sensor Network) architectures, device architectures and system integration architectures are resolved. Correspondingly, the WAN-SAN (Wide Area Network - Storage Area Network) coherent architecture of WSN, the RTOS-based (Real-Time Operating System) and multiprocessor friendly stack architecture, the content-extraction based data compression algorithm, and the I2Pack (intelligent and interactive packaging) solution are proposed and demonstrated.

The IoT has become a promising technology for addressing societal challenges by connecting smart devices and leveraging Big Data analytics to create smart cities worldwide [7]. At the same time IoT for smart cities needs to guarantee the accessibility of open data and cloud services to allow industries and citizens to develop new services and applications. So, the authors provide a case study of the GreenIoT platform in Uppsala, Sweden, to demonstrate the idea of interoperability and open data for smart cities. Moreover, the platform, dubbed as a "Mobile ISP" – mISP (Internet Service Provider) is a natural extension on the established wireless ISP concept with a practical bent towards wire-free deployment and gateway connectivity [8]. It justifies a split microarchitecture approach and depicts further

usage schemas for the device afforded by virtue of the extensibility it offers.

Well-known micro-controllers such as Arduino are widely used by all kinds of makers worldwide. In the paper [16] authors propose Arduino application for the IoT realization. They present the Arduino Service Interface Programming (ASIP) model, that addresses the issues above by (1) providing a "Service" abstraction to easily add new capabilities to micro-controllers, and (2) providing support for networked boards using a range of strategies, including socket connections, bridging devices, MQTT-based publish-subscribe messaging, discovery services, etc. Also, an open-source implementation of the code running on Arduino boards and client libraries in Java, Python, Racket and Erlang are provided.

Simple Network Management Protocol (SNMP) is an application-layer protocol that is used to monitor IP based devices. Also it can monitor and manage IP based devices without impacting their performance. SNMP is also used in a cloud computing environment to monitor and control virtual machines. The paper [18] discusses the deployment SNMP for monitoring and controlling Type 1 hypervisor (in a cloud environment), what complements presented branched structures and models of industrial systems based on the IoT.

A mobile ad hoc network (MANET) is a self-configuring wireless network in which each node could act as a router, as well as a data source or sink [17]. Its application areas include battlefields and vehicular and disaster areas.

Security problems in industrial IoT-based systems are shown in [22], where resource starvation DoS attacks are considered. This paper introduces an approach to proactively detect such a DoS attack in its early development stages and therefore avoid damage using the set of data in the Management Information Base retrieved by the SNMP. By detecting in the early development stages, it is possible to avoid service interruption, system availability problems and other related effects, such as system and bandwidth performance degradation caused by legitimate operations.

As another example, the functionality-based application confinement (FBAC) access control model presented in [23]. FBAC is an application-oriented access control model, intended to restrict processes to the behaviour that is authorised by end users,

administrators, and processes, in order to limit the damage that can be caused by malicious code, due to software vulnerabilities or malware. FBAC is unique in its ability to limit applications to finely grained access control rules based on high-level easy-to-understand reusable policy abstractions.

In [19] authors suppose that the sensed data tends to new trend of research i.e. big data with considering the number of sources and types of data from smart sources. Accordingly, security will be a fundamental enabling factor of most IoT applications and big data, mechanisms must also be designed to protect communications enabled by such technologies. The authors analyse existing protocols and mechanisms to secure the IoT and big data, as well as security threats in the domain.

The paper [24] presents the results of a pilot study of proposed by authors environment based on oVirt that enables students to gain hands-on experience with security tools in rich and complex learning scenarios. Opportunities for improvements are identified, and it is concluded that oVirt is a feasible platform on which to build a lab environment for teaching computer security.

Conclusions and questions

Structures, models and technologies for development of industrial and home use IoT-based systems are given in the chapter. Main trends and peculiarities in industrial IoT-based systems are selected from big variety of IoT applications. In particular, the automation is presented as the most effective mean in production, transportation, city infrastructure, ecology and health care. Besides, software components and protocols of wired and wireless technologies for IoT networks building are considered. Also, security problems in industrial IoT-based systems are analysed: main types of attacks in the Internet, data encryption standards and security policy of industrial systems based on IoT. The chapter includes technologies and projects, developed in partner universities of ALIOT program.

In this section, the materials for module ITMM6.1 of Industrial training course “IoT for industrial systems” are presented. They can be used for preparation to lectures and self-learning.

In order to better understand and assimilate the educational material that is presented in this section, we invite you to answer the following questions.

1. Choose the correct definition of the IoT system:
 - a) a systematized set of means of gathering information about a controlled object and means of influencing its behavior, intended to achieve certain goals;
 - b) a network consisting of interrelated physical objects or devices that have built-in sensors and software that allows you to transfer and exchange data between the physical world and computer systems by using standard communications protocols;
 - c) a control system that uses computers, networked data communications and graphical user interfaces as well as other peripheral devices for high-level process supervisory management.
2. The “Smart house” systems are used for:
 - a) health monitoring automation; b) city infrastructure automation; c) home automation.
3. What is one of the basic IoT principles?
 - a) the global identification of each object of the network; b) the presence of a wired internet connection; c) the presence of powerful computing devices.
4. The main three levels of IoT are:
 - a) level of sensors, level of peripheral control devices and level of man-machine interface; b) components, structural units and system of systems.
5. The SmartThings hub is used in the IoT industrial systems with a connection structure:
 - a) “device-to-device”; b) “device-to-cloud”; c) “device-to-gateway”.
6. The connection structure “data sharing on the server” is used for:
 - a) providing third-party access to downloaded sensor data; b) providing direct connection of several IoT devices; c) providing remote access for operator to downloaded sensor data.
7. The IPv6 protocol from the family of TCP/IP protocols uses:
 - a) 32-bit addressing system; b) 64-bit addressing system; c) 128-bit addressing system.

8. One of the main disadvantages of wireless networks is:
a) high cost in creating a large number of devices; b) low mobility of network devices; c) low noise immunity.
9. What maximum distance of the signal transmission has an interface RS-232?
a) 15 m; b) 150 m; c) 1200 m.
10. What maximum data transfer rate has an interface RS-485 at a distance of 120 m?
a) 1 Mbps; b) 5 Mbps; c) 10 Mbps.
11. Which network refers to the global mobile wireless networks?
a) ZigBee; b) GPRS; c) Bluetooth.
12. What is the frequency range of the Wi-Fi network?
a) 600-860 MHz; b) 1.2-2.4 GHz; c) 2.4-2.483 GHz.
13. What type of Internet attacks include sniffers?
a) active; b) passive.
14. What type of attacks has the purpose of forcing the server to not respond to queries?
a) IP-spoofing; b) Man-in-the-middle; c) Denial of Service.
15. Which of the following advantages does not apply to the data encryption standard DES?
a) high level of data protection against decryption and possible modification of data; b) large enough key size; c) economic in realization and effective in speed.
16. What is the maximum length of the encryption block for the standard AES?
a) 64 bits; b) 128 bits; c) 256 bits.
17. Firewalls are used in the IIoT systems:
a) to collect data from the sensors of the IIoT system; b) to segment the IIoT system itself and isolate it from external networks; c) for analysis of current parameters of IIoT system actuators.
18. What type of authentication is appropriate to use in the IIoT systems to improve their security level?
a) authentication on device; b) server authentication.

References

1. R. H. Weber and R. Weber, *Internet of Things*. Berlin, Heidelberg: Springer-Verlag, 2010.

2. U. Egham, "Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016", *Gartner.com*, 2018. [Online]. Available: <https://www.gartner.com/en/newsroom/press-releases/2017-02-07-gartner-says-8-billion-connected-things-will-be-in-use-in-2017-up-31-percent-from-2016>. [Accessed: 30- Aug- 2018].

3. A. Kor, C. Pattinson, M. Yanovsky, and V. Kharchenko, "IoT-Enabled Smart Living," in *Technology for Smart Futures*, M. Dastbaz, H. Arabnia, and B. Akhgar, Eds., 2017, pp. 3-28.

4. A. Alfeo, P. Barsocchi, M. Cimino, D. La Rosa, F. Palumbo, and G. Vaglini, "Sleep behavior assessment via smartwatch and stigmatic receptive fields," in *Personal and Ubiquitous Computing*, vol. 22, no. 2, 2017, pp. 227-243.

5. V. Miori and D. Russo, "Home automation devices belong to the IoT world," in *ERCIM news*, vol. 101, 2015, pp. 22-23.

6. Z. Pang, *Technologies and Architectures of the Internet-of-Things (IoT) for Health and Well-being*. KTH – Royal Institute of Technology, 2013.

7. B. Ahlgren, M. Hidell, and E. Ngai, "Internet of Things for Smart Cities: Interoperability and Open Data," in *IEEE Internet Computing*, vol. 20, no. 6, 2016, pp. 52-56.

8. C. Pattinson, A. Cor, and R. Braddock, "Community Wide Area Network and Mobile ISP," in *Green Information Technology: A Sustainable Approach*, M. Dastbaz, C. Pattinson, and B. Akhgar, Eds., 2015, pp. 3-28.

9. O. Vermesan and P. Friess, *Digitising the Industry - Internet of Things Connecting the Physical, Digital and Virtual Worlds*. NY: River Publishers, 2016.

10. S. Jeschke, C. Brecher, H. Song, and D. Rawat, *Industrial Internet of Things*. Switzerland: Springer International Publishing, 2017.

11. D. Uckelmann, M. Harrison, and F. Michahelles, *Architecting the Internet of Things*. Berlin, Heidelberg: Springer-Verlag, 2011.

12. Y. Kondratenko, O. Kozlov, O. Gerasin, A. Topalov, and O. Korobko, "Automation of Control Processes in Specialized Pyrolysis Complexes Based on Web SCADA Systems," *9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, pp. 107-112, September 2017.

13. Y. Kondratenko, O. Korobko, O. Kozlov, O. Gerasin, and A. Topalov, "PLC Based System for Remote Liquids Level Control with Radar Sensor," *IEEE 8th International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, pp. 47-52, September 2015.

14. Y. Kondratenko, O. Korobko, and O. Kozlov, "PLC-Based Systems for Data Acquisition and Supervisory Control of Environment-Friendly Energy-Saving Technologies," in *Green IT Engineering: Concepts, Models, Complex Systems Architectures, Studies in Systems, Decision and Control*, vol. 74, V. Kharchenko, Y. Kondratenko, and J. Kacprzyk, Eds., 2016, pp. 247-267.

15. Y. Kondratenko, O. Kozlov, O. Korobko, and A. Topalov, "Internet of Things Approach for Automation of the Complex Industrial Systems," *13th International Conference on Information and Communication Technologies in Education, Research, and Industrial Applications. Integration, Harmonization and Knowledge Transfer, ICTERI'2017, CEUR-WS*, pp. 3-18, May 2017.

16. G. Barbon, M. Margolis, F. Palumbo, F. Raimondi, and N. Weldin, "Taking Arduino to the Internet of Things: The ASIP programming model," in *Computer Communications*, vol. 89-90, 2016, pp. 128-140.

17. A. Pullin, C. Pattinson, and A. Kor, "Building Realistic Mobility Models for Mobile Ad Hoc Networks," in *Informatics*, vol. 5, no. 22, 2018, pp. 1-52.

18. A. Iqbal, C. Pattinson, and A. Kor, "Introducing controlling features in cloud environment by using SNMP," in *Green IT Engineering: Concepts, Models, Complex Systems Architectures. Studies in Systems, Decision and Control*, vol. 74, V. Kharchenko, Y. Kondratenko, and J. Kacprzyk, Eds., 2018, pp. 147-160.

19. D. Puthal, R. Ranjan, S. Nepal, and J. Chen, "IoT and Big Data: an architecture with data flow and security issues," in *Cloud Infrastructures, Services, and IoT Systems for Smart Cities. IISSC 2017, CN4IoT 2017. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, vol. 189, A. Longo et al., Eds., 2018, pp. 243-252.

20. R. Minerva, A. Biru, and D. Rotondi, *Towards a definition of the Internet of Things (IoT)*. Telecom Italia S.p.A., 2015.

21. E. Delgado, *The Internet of Things: Emergence, Perspectives, Privacy and Security Issues*. New York: Nova Science Publishers, 2015.

22. C. Pattinson and K. Hajdarevic, "Timing considerations in detecting resource starvation attacks using statistical profiles," in *International Journal of Electronic Security and Digital Forensics*, vol. 1, no. 2, 2007, pp. 194-205.

23. Z. Schreuders, C. Payne, and T. McGill, "The functionality-based application confinement model," in *International Journal of Information Security*, vol. 12, no. 5, 2013, pp. 393-422.

24. Z. Schreuders, E. Butterfield, and P. Staniforth, "An open cloud-based virtual lab environment for computer security education: A pilot study evaluation of oVirt," *The first UK Workshop on Cybersecurity Training & Education (Vibrant Workshop 2015)*, pp. 5-6, June 2015.

25. V. Kharchenko, D. Maevsky, E. Maevskaya, C. Phillips, and L. Vystorobska, "Employers' requirements-oriented assessment of IoT curriculum: The projects CABRIOLET and ALIOT," *9th International Conference on Dependable Systems, Services and Technologies (DESSERT 2018)*, pp. 677-681, May 2018.

53. ADVANCED TECHNIQUES AND MEANS FOR DESIGN, MODERNIZATION AND IMPLEMENTATION OF INDUSTRIAL IOT-BASED SYSTEMS

Prof., DrS. Yu. P. Kondratenko, Assoc. Prof., Dr. O. V. Kozlov, Senior Researcher O. V. Korobko, PhD Student O. S. Gerasin, PhD Student A. M. Topalov (PMBSNU)

Contents

Abbreviations	773
53.1 Design and implementation of IoT-based control and monitoring systems for floating docks	774
53.1.1 Introduction in control and monitoring systems for floating docks	774
53.1.2 IoT-based control and monitoring system of a floating dock for low-tonnage vessels.....	776
53.1.3 Hardware and software means for implementation of IoT-based control and monitoring systems for floating docks	778
53.2 Design and implementation of IoT-based control and monitoring systems in robotics	781
53.2.1 Main principles and tasks of robots control and monitoring systems development.....	781
53.2.2 IoT-based control and monitoring system of mobile robots able to move on inclined and vertical surfaces.....	784
53.2.3 Hardware and software means for implementation of IoT-based control and monitoring systems for industrial and specialized robots ...	787
53.3 Approaches to modernization of complex objects in different industrial systems based on IoT.....	789
53.3.1 Modernization conceptions in different industrial systems	789
53.3.2 IoT-based modernization of computer control and monitoring system of specialized pyrolysis complex.....	792
53.3.3 The IoT-based modernization of slippage registration system of industrial robot's adaptive gripper.....	796
53.4 Work related analysis	798
Conclusions and questions.....	800
References	803

Abbreviations

CF – Clamping Force

DAM – Data Acquisition Module

DOM – Discrete Output Module

FS – Ferromagnetic Surface

IIoT – Industrial Internet of Things

IoT – Internet of Things

MPW – Municipal Polymer Waste

MR – Mobile Robot

PLC – Programmable Logic Controller

PUE – Power Usage Effectiveness

SCADA – Supervisory Control And Data Acquisition

SDS – Slip Displacement Sensor

SPC – Specialized Pyrolysis Complexes

53.1 Design and implementation of IoT based control and monitoring systems for floating docks

53.1.1 Introduction in control and monitoring systems for floating docks

Fast quantitative growth of the world fleet puts the task of intensifying the use of ship lifting facilities [1]. Floating docks, despite the complex structure and high operational cost, is one of the main tools for repair, pull, lift and disposal of vehicles.

As floating structures dock must have buoyancy, stability, unsinkability, strength, ability to change its waterline (draft), but as a stacker pad - provide manufacturing location for a vessel which comes to the dock, access to his body for inspection and repairs.

The floating dock faces equilibrium problems in the course of the maintenance. As a rule, the own weight of the vessel is transmitted through keel blocks to the deck of a pontoon, so inclinations and violations of strength of floating dock can happen. Calculations of ballasting of dock are carried out before docking of the vessel for elimination of critical deformation and undesirable inclinations of floating dock. First of all, these calculations define selection of ballast in pontoons of floating dock, and the purpose of calculations - receiving such distribution of ballast in case of which a list and trim dock are equal to zero, also the bending system “ship/dock” moment will be less than admissible for this floating dock. It must be kept in mind that in case of a large load capacity of dock the curving moments, list and trim angles of the floating dock can be completely removed by load balancing on the each pontoon at the expense of ballast.

For effective functioning floating dock has the following systems: ballast, vacuum, ventilation and other systems that ensure the operation of the actuating mechanisms and the floating dock as a whole [1].

From the given above systems, that are parts of the floating dock, the ballast system is the most important for the performance of the docking operations, since ballast tanks filling and emptying leads to the floating dock draft changing, which is the main controlled parameter at the floating dock docking operations conducting.

The ballast system is designed for the providing of the floating dock submerging and surfacing on a certain set value of its draft by filling or emptying of the ballast tanks with ballast water during docking operations. It includes ballast pumps, filling and emptying pipelines, and valves (discrete and linear valves or flow regulators).

Providing of ballast water pumping by all available pumps for control of the floating dock draft current value during docking operations is the basic operational requirement for the ballast system. The breakage of even one pump at floating dock surfacing can make its lift dangerous or even impossible. In this regard, at least two pumps must be set even in the small floating docks, and the ballast system should ensure their interchangeability. The possibility of simple and rapid enabling or disabling of certain pumps and, as a consequence, the possibility of ballast water pumping from any ballast tank of the floating dock allows to implement submerging and surfacing on the required value of its draft, providing a safe staging or withdrawal of vessels from the floating dock.

Ensuring the operational control of all parameters accurately and timely control of actuators floating dock during the performance of operations immersion and emersion of the ship is a complex technical task that requires attentiveness marginal team dock for a long time. Any "human" errors or outdated equipment can lead to increased time raising or lowering vessels, according to a decrease in economic efficiency of the dock, and possibly to emergencies both the dock and for himself vehicles. And in practice of floating docks operating can cause serious accidents and emergencies, flooding the dock, broken towers, corrugated appearance on the towers and dents on the stocks-deck floating dock, emergency heel of ships when submerged dock for their output, and others.

The rapid development of computer technology contributes to the creation of effective industrial IoT-based control and monitoring systems for floating dock [2, 3]. Usage of industrial IoT-based system enables the operator to automate the control processes of floating docks parameters, enable or disable mechanisms and devices, open or close valves on pipelines, monitor any parameters of floating docks with a specially equipped consoles or centralized supervisory control.

In addition, for floating docks parameters monitoring and control from the shore wireless technologies can be used. The combination of industrial IoT-based control and monitoring systems for floating dock with wireless technologies as well as the Internet allows to create industrial IoT-based systems [2-6]. However, at this stage of industrial IoT-based systems based on IIoT not yet reached the level of wide industrial application because there are difficulties with the protection of information transmitted. In addition, the implementation of control functions through unprotected channels contradicts to the security concerns of any process. In this regard, most of the Web interfaces are used as remote clients to control and collect data.

Thus, the problem of development and implementation of industrial IoT-based control and monitoring systems for floating dock is quite relevant. Today there is a focus on the module-structure-control-systems with variable configuration for use in different types of floating docks. Also safety and reliability requirements are enhanced to the monitoring and control systems of floating objects.

The use of new digital control systems based on the developing principles of distributed control systems using the SCADA software and wireless technologies will solve a number of problems described and to develop universal industrial IoT-based control and monitoring system for floating dock with rapidly changing configuration.

The next section considers development and research of docking operations control system based on IIoT of the floating dock for low-tonnage vessels (yachts, tugs, etc.).

53.1.2 IoT-based control and monitoring system of a floating dock for low-tonnage vessels

The authors developed a special multifunctional industrial IoT-based control and monitoring system for floating dock based on the remote monitoring and control principles using multiprocessor devices and SCADA software [7, 8]. The given system is designed for implementation of the main docking operations, monitoring and control of current values of the draft, list and trim angles, hogging and sagging, input and output valves states, as well as liquid level, temperature and volume in ballast tanks of floating docks for low-

tonnage vessels. This system is built on a modular (variable-configuration) structure and has a separate distinct system of remote monitoring using cloud-based technology.

The proposed generalized industrial IoT-based control and monitoring system for floating dock based on IoT approach has two levels of monitoring and automatic control: local level and remote level. Local level, in turn, is divided into three hierarchical levels of monitoring and control: level of sensors and actuators, controller level, operator level. Remote level is based on cloud technologies.

The level of sensors and actuators consists of sensors and actuators of the ballast complex and the floating dock hull. Each tank of the floating dock is equipped with the pressure sensor, three temperature sensors, one discrete level sensor (or float level switch), hydrostatic pressure sensor and the valve.

Level sensors and temperature sensors are used to obtain information of current level and water temperature in ballast tanks. A discrete level sensor is required for fixing a certain level value. The pressure sensor serves to determine the presence of excess pressure inside the tanks.

In addition, the left and right towers of the floating dock are equipped with hydrostatic pressure sensors. These sensors are used for indirect measurements of the list and trim angles of the floating dock, which are evenly spaced (three sensors along the starboard and the port side of the floating dock outside as nearer as possible to its bottom). The first and the fifth hydrostatic pressure sensors are set at the extreme points of the port side of the dock, the second and the sixth hydrostatic pressure sensors - at the extreme starboard points, the third hydrostatic pressure sensor - in the middle between the first and fifth hydrostatic pressure sensors on the port side, and the fourth hydrostatic pressure sensor - in the middle between second and sixth hydrostatic pressure sensors on the starboard.

The controller level contains various hardware and software means for information processing. Output signals from sensors are transmitted to the data acquisition module (DAM), which transforms analog signals to the corresponding digits that are transmitted to the Programmable Logic Controller (PLC). The PLC contains a program unit for calculating the dataset parameters, a program unit for liquid volume

calculation, and a program control unit for valves. All of them are implemented using specialized SCADA TRACE MODE software. The information about current parameters of the floating dock is transmitted to the operator level using a specialized human-machine interface of personal computer (PC).

The human-machine interface allows operator, to control pumps, pipeline valves for filling and emptying the ballast tanks by controlling the flow. Control signals arriving from the operator screen are processed in the program control unit for valves and sent to the discrete output module (DOM). In turn, DOM implements the distribution of discrete signals to actuators.

Remote level used to monitoring of parameters and is required for use with a floating dock to land office without the possibility of control of actuators as opposed to local control. This level extends this system capabilities to industrial IoT-based system namely Web SCADA system, and refers to the implementation of human-machine interface based on web-technologies. This allows monitoring and control of industrial IoT-based systems through a standard browser, acting in this case as a smart client. The architecture of these systems includes Web server and client terminals - PCs, tablets or mobile phones with a Web browser. Connecting customers to Web server via Internet / Intranet allows them to interact with task automation as applied with a simple Web or WAP page.

53.1.3 Hardware and software means for implementation of IoT-based control and monitoring systems for floating docks

For the hardware and software implementation of the above-mentioned system of measuring and controlling the parameters of the floating dock, the authors used various digital devices. Implementation of the industrial IoT-based control and monitoring system for floating dock is presented in the Fig. 53.1.

ICP DAS I-7018P modules are used as thermocouple data acquisition modules. In turn, ICP DAS I7017C with current input are used to collect information from hydrostatic pressure sensors. The ICP DAS I-7051 module with 16 inputs is used as a data acquisition module for discrete input signals (pump signals, valve position). In addition, the

ICP DAS I-7061 module with 12 power relay outputs is used to control actuators (pumps, valves).

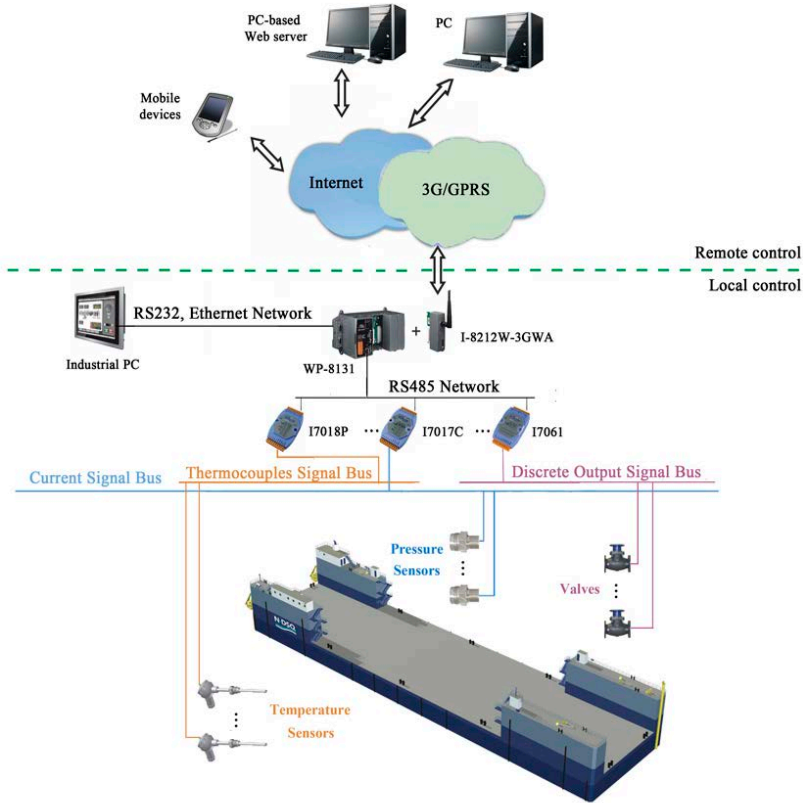


Fig. 53.1 – Functional structure of the IoT-based control and monitoring system for the floating dock

The ICP DAS WP-8131 PLC is used in the current control and measurement system as the main executive module. The main features of the PLC are: CPU PXA270 or Comparable (32-bit, 520 MGz), RW Memory SDRAM 128 Mb, Zeropower SRAM 512 kb, Flash-memory

128 Mb, and support for 16 GB microSD memory cards. The PLC includes VGA, Ethernet, USB 1.1, RS232, RS485 and RS 482 interfaces.

Industrial IoT-based control and monitoring system for floating dock is additionally equipped with an ICP DAS I7520 Interface Converter module, which performs the functions of converting RS485 bus signals to the RS232 interface. Accordingly, for the successful operation of the system, the host computer must be equipped with a COM port.

The software for monitoring and control of the floating dock parameters uses the SCADA package TRACE MODE 6 [8, 9]. The human-machine interface of this system is implemented using the tools provided in the basic version of the SCADA system TRACE MODE 6 (Fig. 53.2).

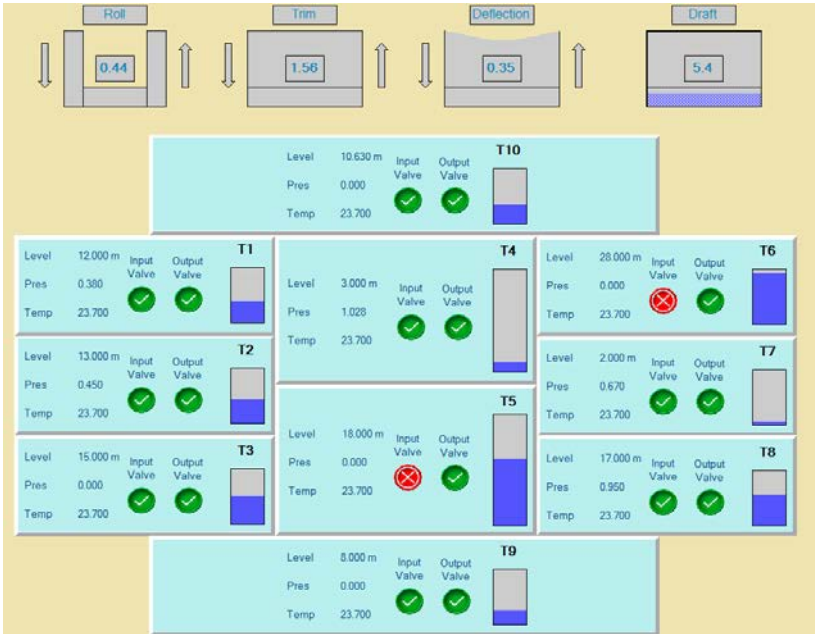


Fig. 53.2 – Human-machine interface of the industrial IoT-based control and monitoring system for floating dock

PLC is also connected with industrial and dual-band 3G WCDMA with 4 ranges GSM/GPRS module I-8212W-3GWA, which enables the creation of wireless communication to the Internet for remote monitoring and control options of floating dock.

In the developed industrial IoT-based control and monitoring system for floating dock the monitoring and automatic control operations in the remote level are implemented by means of the web servers, remote computers, tablets and different types of mobile devices. In this case, PLC with the help of wireless mobile network 3G or 4G connection and family of protocols TCP/IP exchange data via the Internet with specialized web server that is placed on a ship's enterprise land office. The main web server, in turn, receives the floating dock data process parameters and provides Web access to the other users (remote computers, tablets, mobile devices).

For remote monitoring of floating dock parameters used a special software module TRACE MODE Data Center [9]. The TRACE MODE Data Center provides remote web based and wireless access to real-time information using web-browser via Internet/Intranet or wireless networks (GSM, GPRS, Wi-Fi, Bluetooth). This new web server enables you to access real time data from any PC ship repair company, running operating system (Windows, Linux, Unix, QNX, Mac OS, etc.), and even from any PC connected to Internet anywhere in the world.

53.2 Design and implementation of IoT-based control and monitoring systems in robotics

53.2.1 Main principles and tasks of robots control and monitoring systems development

Improvement of labor productivity with reduction in the risks to human life, health and environment when performing various operations in extreme conditions and inaccessible areas is presently an urgent issue resulting from the intensive industrial development in many countries of the world [9]. There are various ways to solve this problem, and one of them is the use of advanced high-technology

equipment with programmable control, flexible production modules, and robotic technological complexes [9].

Creation of such robots and robotic complexes is necessitated by emerging extreme situations, increased requirements for the implementation of technological operations, and the conditions dangerous or difficult for a person to perform these actions [10]. Extreme conditions and environments may be characterized with an increased radioactivity, high temperatures, gas contamination, etc. Thereat, mobile robots (MR) are of the greatest interest, so let us consider main principles and tasks of robots control and monitoring systems development.

First of all, basic principles of robot`s construction must be predefined. At the same time robot`s construction is chosen according to their purpose, distinguishing industrial, transport, household, toy, research, agricultural, construction, medical, rescue, security, and military robots [10]. From the viewpoint of mobility, extendable functionality, and a wide scope of application, mobile robots are the most attractive. Among them, ground (wheeled, tracked, walking), air, planetary, marine (surface and underwater) are distinguished [10]. Such a classification is due to the fact that the MRs have to operate under different conditions.

MRs may be equipped with one or several technological manipulators depending on the technological task to be executed. The terminal member of the onboard manipulator can have the form of diagnostic equipment, sensors, physical quantity converters, technological tools or equipment [10]. By the way, an MR can be presented as a set of three major subsystems: a transport subsystem, a specialized subsystem and a control subsystem (Fig. 53.3) [10].

The transport subsystem (Fig. 53.3) is a platform intended for the delivery of specialized and technological equipment to the work site. The transport platform consists of an undercarriage, a main body, and a power plant. As a rule, the control system is installed inside the main body. Depending on the type of the operational environment, the MR may have a tracked, wheeled, wheel-tracked, semi-tracked, walking or wheel-walking under-carriage a water jet or gas jet propulsor. The appearance of the ground MR is primarily determined by the type and

design of the propulsor used to convert the force derived from the engine into the traction effort that drives the transport platform.

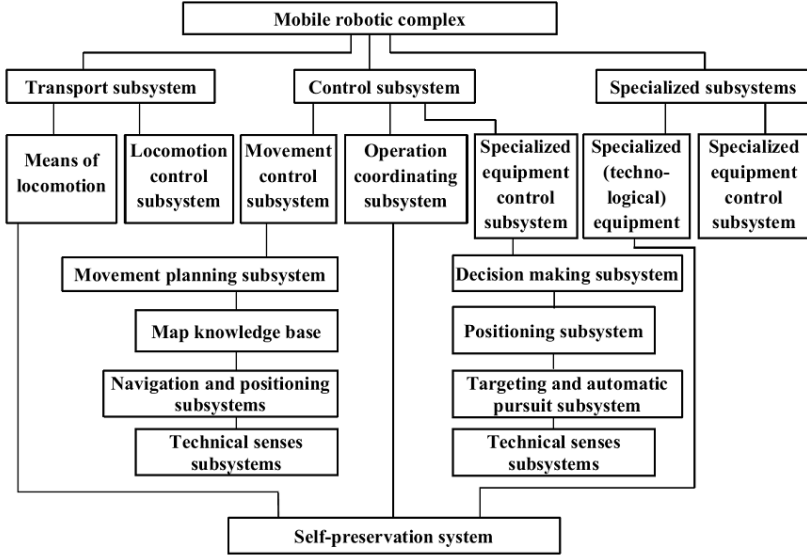


Fig. 53.3 – Generalized structure of a mobile robotic complex

Under the conditions where the speed of a wheeled or tracked robot is lower than the speed of a walking one, it is advisable to use the latter (for example, in a mountainous terrain or the site of destruction). When designing conventional vehicles, the propulsion parameters are optimized for the most typical operational conditions and surfaces. However, such optimization for a mobile robot is a very complex problem due to the uncertainty of the operational conditions. This is why the MR propulsors are currently constructed adaptable to the operating surface [10].

The specialized subsystems are directly designed for the execution of specific works. They comprise the required set of technological equipment, which is determined by the type of the problem being solved and the purpose of the MR.

The control subsystem provides control of the movement and operation of the technological equipment, as well as adaptive control of the undercarriage and power plant with account for interaction of the transport subsystem with the environment.

Control of robotic objects and systems employs the same principles as those used for other equipment. At that, programmed and remoted types of control have become the most widespread options [9, 10]. They enable the MR to tackle the following tasks: crossing and bypassing obstacles, moving along a given trajectory with account for the surface's inclination, keeping to a specified position, taking the required starting position, etc.

It should be noted that special features of the control object (the MR) require specific problems to be solved, which makes adaptive and intelligent systems the most attractive ones [10]. Adaptive and intelligent control provides for execution of the following tasks: processing of sensory information; formation of models of the environment; decision making and planning of further actions; movement control; creation of an intelligent human-robot interface. However, such control methods are not quite common due to the complexity of development of the systems. In addition, scientific publications hardly cover the general operational principles of control systems for various mobile robots.

53.2.2 IoT-based control and monitoring system of mobile robots able to move on inclined and vertical surfaces

Mobile robots have recently acquired widespread application related to exploration and research in various fields and in the places where using human labor is dangerous or inappropriate. Of great interest is the use of robots able to move along vertical surfaces for operation on building facades, ships, tanks, bridge supports. To move along external surfaces of buildings and facilities, mobile robots can be equipped with various types of clamping devices: mechanical, magnetic, adhesive, pneumatic, vacuum, and magnetically operated ones. The problem of processing large external and internal surfaces of various types of industrial facilities is of a great economic importance to all the developed countries of the world [10]. A large number of

technological operations are commonly performed on metal ferromagnetic surfaces (FSs): elements of various facilities, structures of hulls, tanks, pipelines, etc. Therefore, MRs with magnetically-operated movers and clamping devices are most appropriate in this case. According to constructions and peculiarities of different MRs for moving and performing technological operations on working FSs, let us regard the generalized robotic complex capable to move on large ferromagnetic surfaces as a multi-coordinate control and monitoring object. Then, there can be formulated the following major tasks for its monitoring and automatic control: monitoring and automatic control of the vector of the MR spatial motion parameters; monitoring and automatic control of the clamping force (CF) value created by the MR clamping magnets; monitoring and automatic control of the vector of the operating parameters of the technical equipment of the MR propulsor; monitoring and automatic control of the vector of the operating parameters of the technical equipment of the MR clamping device.

Therefore, it is recommended to use the specialized IoT-based system in order to implement the above-mentioned formalized tasks of automatic control and monitoring of the MR moving and performing given technological operations on large inclined FSs. Its multi-level branched structure is displayed in Fig. 53.4, where the following notations are adopted: GES – group of environment sensors; GAS – group of additional sensors; FS – force sensor; AS – angle sensor; DS – displacement sensor; CD1, CD2 – the first and the second clamping devices; P1, P2 – the first and the second propulsors; MCU – movement control unit; CFCU – clamping force control unit; PPCU – positioning program control unit; TCU – trajectory control unit; HMI/MMI – human-machine/man-machine interface; \mathbf{G}_{MR} – the influence of the MR on the working environment; \mathbf{G}_{WE} – the influence of the working environment on the MR; \mathbf{P}_{WE} – main parameters of the working environment; \mathbf{P}_{MR} – main parameters of the MR; F_{MR} – the MR's clamping force acting on the FS; φ_{MR} – the MR's angle of rotation; S_{MR} – the MR's linear displacement; F_{CD1} – the clamping force of the MR's first clamping device; F_{CD2} – the clamping force of the MR's second clamping device; S_{P1} – linear movement of the MR's first propulsor; S_{P2} – linear movement of the MR's second propulsor; \mathbf{U}_{PWE} –

the GES output signals corresponding to the main parameters of the working environment;

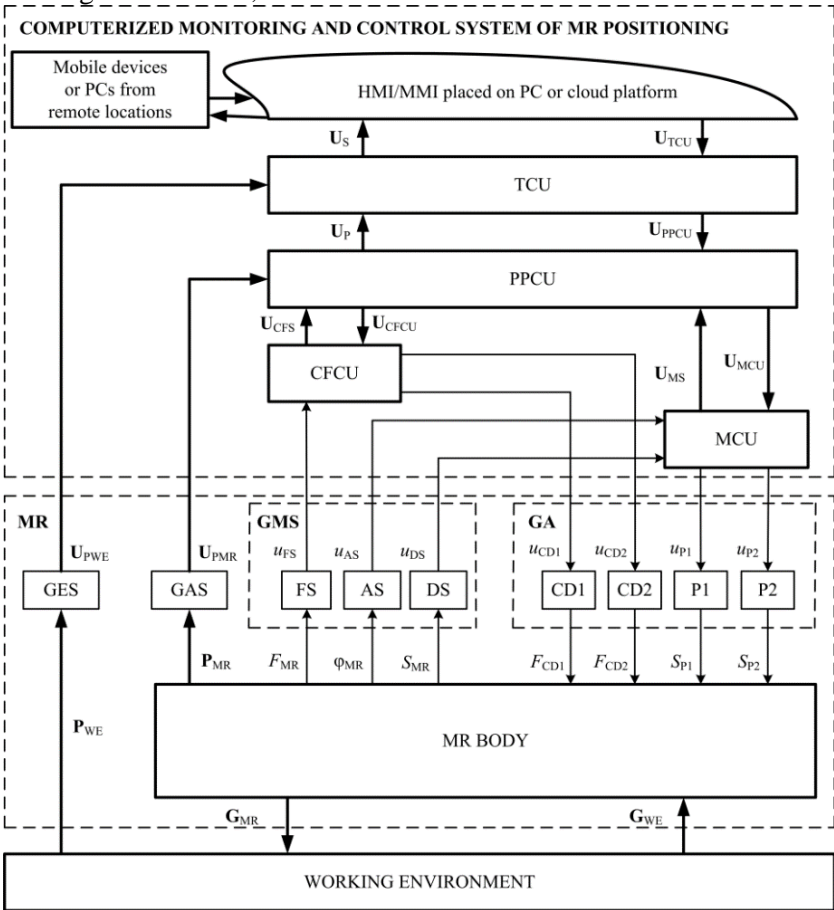


Fig. 53.4 – Functional structure of the IoT-based system of monitoring and control of MR positioning

U_{PMR} – the GAS output signals corresponding to the main parameters of the MR; u_{FS} – the output signal of the sensor of the MR’s clamping force acting on the FS; u_{AS} – the output signal of the sensor of the MR’s angle of rotation; u_{DS} – the output signal of the sensor of the MR’s

linear displacement; u_{CD1} – the control signal of the MR's first clamping device; u_{CD2} – the control signal of the MR's second clamping device; u_{P1} – the control signal of the MR's first propulsor; u_{P2} – the control signal of the MR's second propulsor; U_{CFS} – the output signals of the clamping force sensor; U_{CFCU} – the control signals for the MR's clamping force control unit; U_{MS} – the output signals of the MR's movement sensors (angle sensor and linear displacement sensor); U_{MCU} – the control signals for the MR's movement control unit; U_P – the output signals of the MR's main operating parameters; U_{PPCU} – the control signals for the positioning programming control unit; U_S – the output signals of the sensors of the MR's main operating parameters considering the state of the working environment; U_{TCU} – the control signals for the trajectory control unit.

The current values of the clamping force formed by CD1 and CD2, the angle of rotation and the displacement of the MR are measured using appropriate sensors. The obtained measurements are used for correction of control impacts on the MR's propulsors and clamping devices. Besides, the system performs measurement of additional MR parameters, such as: the current in the drive motor windings (for P1 and P2), the amplitude of the robot's main body vibration, the quality indicators of the operations performed by the robot.

53.2.3 Hardware and software means for implementation of IoT-based control and monitoring systems for industrial and specialized robots

Nowadays, the industrial and specialized robots have to use the advanced monitoring and control systems (typically with a hierarchical branched structure) based on data, received during the execution of the current technological processes in real time mode [11] for the effective operation with high energy and economic indicators. Automated posts of operator, process controllers, industrial computers, programmers, as well as facilities for industrial networks implementation, are the main components of such systems.

The measurements performed on the MR's operating parameters and the working environment are taken into account in the corresponding units of the functional structure (Fig. 53.4). In this case, the most important ones are displayed through the HMI/MMI on the

computer screen of the operator. The HMI/MMI additionally contains means for visualization of the MR's operating parameters in the form of tables and charts. Also, the HMI/MMI has the ability to record the measurement history to the database for further processing, modification of control algorithms, etc [11].

Furthermore, the system allows for automatic data sending in case of emergency to all the users of the enterprise network. Also, it has an advanced, highly integrated programming environment that is sufficiently flexible and easy to extend, as well as flexible network designs and possibility of connection to the online expert system for more detailed data analysis. There are ready-to-use instruments based on cloud services: Google Cloud Platform, Amazon EC2 and other online platforms. Some working tools may be presented in the cloud service. In other case a developer have to develop needed instruments itself or using tools like Hadoop. Hadoop is a project of the Apache Software Foundation, a freely distributed set of utilities, libraries and a framework for developing and executing distributed programs running on clusters of hundreds and thousands of nodes.

For hardware implementation of the above system for monitoring and automatic control of the MR's main working parameters, is proposed using modern gauges and transducers. Ready-to-use solutions based on PLCs, microcontroller developers' boards, input/output (I/O) modules allow accelerating the designing process and reducing the number of errors at testing procedures. Usually, such devices have standardized current, voltage and discrete inputs and outputs and are used as data acquisition modules for the analog and discrete input signals or for actuating automatic control mechanisms. Also, they may provide USB to RS-232/422/485 converting and vice versa for the module connection to PC at testing and debugging of the whole system [11].

Accordingly, we suggest installing a TCU (Fig. 53.4) on PC, a PPCU on PLC, and also CFCU and MCU based on microcontroller or I/O modules in the current system whether experimental setup development. As the main operating unit, the PLC has a high-capacity processor and includes VGA, Ethernet, USB 1.1, RS232, RS485 and RS482 interfaces for communication with PC and I/O modules. The respective data acquisition modules then convert the analog signals u_{FS} ,

u_{AS} , u_{DS} into proper digital ones, which are transmitted to the PLC via RS485 bus with DCON protocol [12]. The PLC has specialized software to process the data obtained from the sensors. For example, Micro TRACE MODE 6 is a good solution for different types of widespread PLCs [11]. So, the information on the current values of the clamping force acting on the FS, the MR's angle of rotation and linear displacement are displayed on the screen of the operator's PC with the help of a specialized HMI. All the control algorithms of the system under development may be implemented using the SCADA TRACE MODE 6 software [11].

53.3 Approaches to modernization of complex objects in different industrial systems based on IoT

53.3.1 Modernization conceptions in different industrial systems

Consequently, the introduction of IIoT technologies in modern automation systems enables the creation of a highly effective system for monitoring and managing technological processes that will work through the Internet. Today, IIoT is considered by global manufacturers of industrial IoT-based systems as the implementation of monitoring and management systems in a cloud server with the display of real-time imitator based on web technologies. In this case, industrial IoT-based system monitoring and control are implemented through a usual browser acting as a thin client. Customers can connect to the IIoT server by Internet/Intranet and interact with applied automation tasks through Web or WAP pages [6].

In particular, SIEMENS developed the WebNavigator package for the WinCC SCADA system, another example is the Adastra company that developed the Trace Mode Data Center web server for the SCADA system Trace node 6. All of these solutions provide access to the project for remote clients. Thin client technology allows you to view and make adjustments to operational and archival information from any remote workplace through any browser.

Thus, the industrial IoT-based systems should include highly efficient software and hardware means for the implementation of specialized algorithms of monitoring and automatic control. In addition,

such systems should have an increased level of reliability, performance and information security [7, 8].

For IIoT projects, as a new direction for the development of industrial IoT-based system, the most common conceptual and architectural solutions are currently defined. To assess the different IIoT projects in the near future, the standardization is actively rooted in order to form a unified and consistent regulatory normative base for the practical implementation of IIoT.

The main trends in the development of IIoT technology and their implementation problems are shown in Table 53.1.

Table 53.1 – Features of IIoT implementation at enterprises

Directions for the development of IIoT technology	Problems of implementation in industry
Development of computerized control systems	The need to adopt common standards
The emergence of powerful and autonomous automation devices	Incompatibility of a number of electronic components
Development of wired and wireless technologies	Construction of complex hybrid networks (complicated topology of networks)
Increasing the number of devices connected to the global network Internet	Slow transition to the protocol IPv6
Development of cryptography and methods of information protection	The problem of data protection and technological process safety
The need to preserve the environment and reduce energy costs	Problems of using alternative energy sources at certain enterprises
Technical solutions for automated production companies	Relatively high cost of implementation

The basic diagram of the generalized modernized system for monitoring and control of the parameters for complex technological objects and processes based on IoT approach is presented in Fig. 53.5, where the following notations are accepted: PC – personal computer;

PLC – programmable logic controller; FPGA – field-programmable gate array; SBC – single-board computer; SDAM – sensors data acquisition module; AOM – analog output module; S – sensor; AM – actuating mechanism; u_1, u_2, u_{n-1}, u_n – control signals of actuating mechanisms; y_1, y_2, y_{n-1}, y_n – output variables values of actuating mechanisms; x_1, x_2, x_{n-1}, x_n – technical object process parameters; $u_{S1}, u_{S2}, u_{Sn-1}, u_{Sn}$ – sensors output signals.

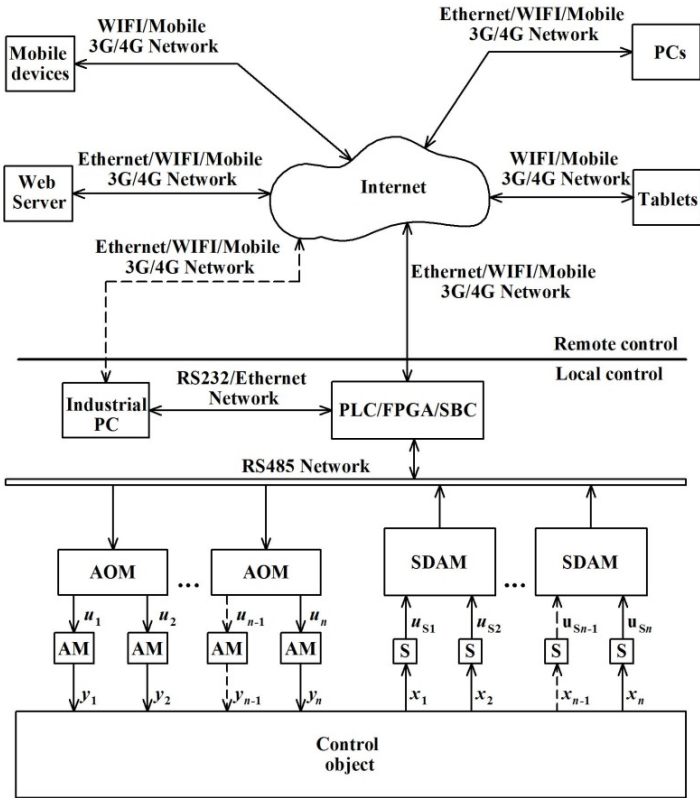


Fig. 53.5 – Basic diagram of the generalized industrial IoT-based system for complex industrial objects and processes based on IoT approach

The proposed generalized industrial system for complex technological objects and processes based on IoT approach [6] has two

levels of monitoring and automatic control: local level and remote level. Local level, in turn, is divided into three hierarchical levels of monitoring and control:

1) lower level – the level of the sensors and actuating mechanisms of the technical object, that is involved in the performance of a certain technological process;

2) average level – the level of the peripheral monitoring and control devices (includes modules for data acquisition and analog output as well as PLC/FPGA/SBC);

3) upper level – the level of HMI (includes industrial PC).

The monitoring and automatic control operations in the remote level are implemented by means of powerful web servers, remote computers, tablets and different types of mobile devices. In this case PLC/FPGA/SBC or industrial PC with the help of wired (Ethernet) or wireless (WiFi, mobile network 3G, 4G and others) connection technologies and family of protocols TCP/IP exchange data via the Internet with specialized web server that is placed on a powerful computer.

Specialized web server, in turn, receives data process parameters and provides Web access to other users (remote computers, tablets, mobile devices). Moreover using the web server the access to the technological process data can be given from any PC of the enterprise industrial IoT-based system, that is running under any operating system (Windows, Linux, Mac OS, etc.), and if desired, from any PC in the world connected to the Internet.

In turn, the specialized HMI in the form of a control panel of the technological process is installed on the server and on the all computers of the enterprise industrial IoT-based system, where it is necessary, with all available functions of monitoring and control.

53.3.2 IoT-based modernization of computer control and monitoring system of specialized pyrolysis complex

A new highly effective industrial IoT-based control and monitoring system developed by the authors for the specialized pyrolysis complexes (SPC), that are used for municipal polymeric waste thermal utilization [11], has also modular structure and implement monitoring and automatic control of main technological

process parameters in the local and remote levels using efficient data processing, analysis and storage instruments. The given system provides performance of the following tasks: monitoring, visualization and automatic control of the pyrolysis complex main operating parameters at the local level and at the remote level via the internet in real time mode; visual display of information about the state of the SPC main components with clear indication of current states and emergencies; the ability of integration into existing large-scaled industrial IoT-based control and monitoring systems of specialized pyrolysis complex of municipal polymer waste (MPW) utilization industrial plants, enterprises or factories; automatic data sending to all the operators of the enterprise in emergency cases.

The functional structure of the proposed by the authors highly effective industrial IoT-based control and monitoring system of specialized pyrolysis complex is shown in Fig. 53.6. The proposed structure (Fig. 53.6) of the computerized system based on IoT is built taking into account the necessity of the simultaneous measurement of various physical quantities, functioning in real-time mode and also the need to build a modular system that has the ability of integration into existing large-scaled industrial IoT-based control and monitoring systems of specialized pyrolysis complex.

The measuring equipment of the industrial IoT-based control and monitoring system of specialized pyrolysis complex is as follows: pressure sensors PD100 type, thermo-couples of the K- and L-types, inductive sensors of the SN04-N and PIP-8-3 types.

According to Fig. 53.6, main actuating mechanisms of SPC include: the hydraulic drive piston for MPW loading into the reactor, water cooling pumps, fuel pumps, normally closed Jaksa D224 valves, fans for cooling and flue gases blowing, AC gear motors as a part of MPW unloading unit. Mentioned actuating mechanisms are powered from the AC mains using contactors PML 1160M type.

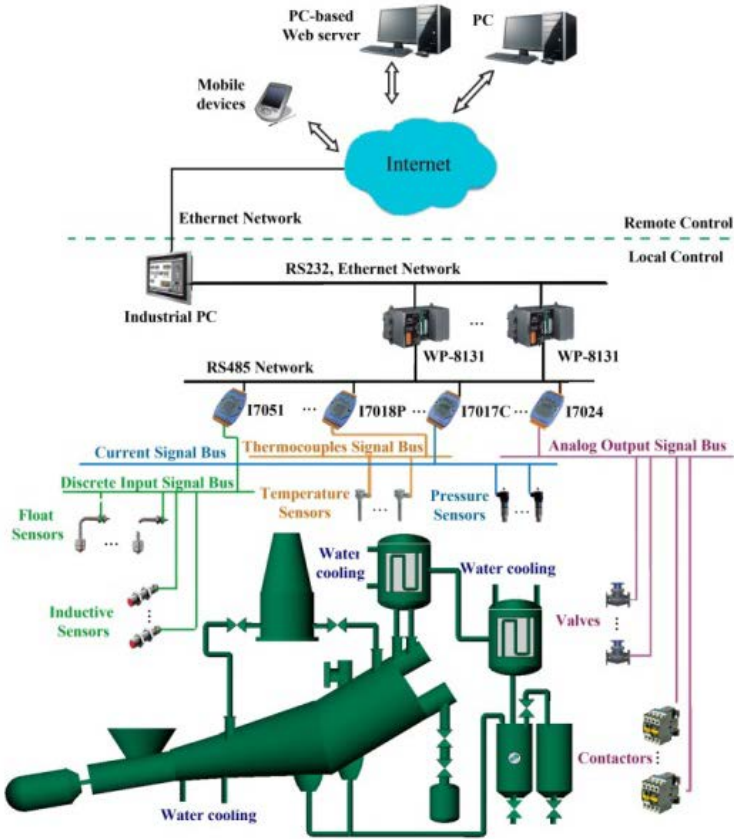


Fig. 53.6 – Functional structure of industrial IoT-based control and monitoring system of specialized pyrolysis complex

As the software facilities of the developed industrial IoT-based control and monitoring system of specialized pyrolysis complex for the MPW thermal processing the TRACE MODE 6 is also used [11]. which belongs to the class of integrated systems that provide maximum comfort to designers and users. Taking into account the main tasks of the given system the authors developed the specialized HMI with the help of TRACE MODE 6, main screen of which is presented in Fig. 53.7.

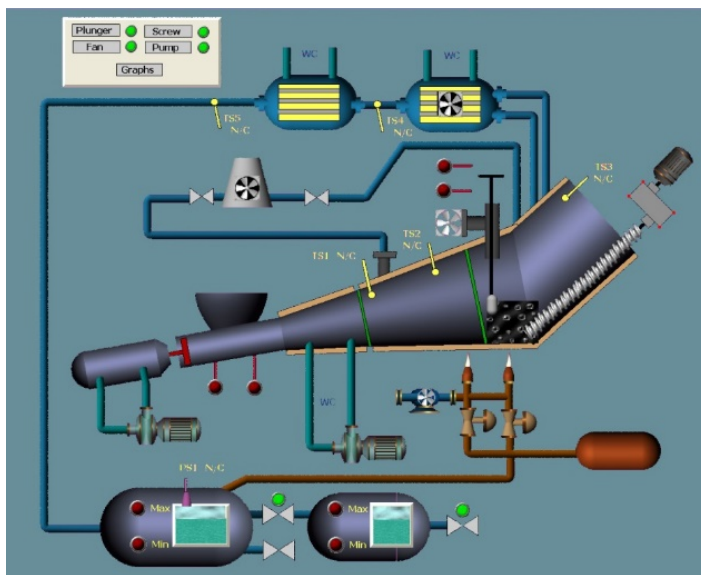


Fig. 53.7 – Human-machine interface of industrial IoT-based control and monitoring system of specialized pyrolysis complex

Designed HMI has a multi-window interface. Main screen (Fig. 53.7) provides the visualization of the main indicators of the industrial IoT-based control and monitoring system of specialized pyrolysis complex process parameters on the operator control display and also grants an ability to set needed ranges of the parameters.

As a web server for remote control of SPC processes is used TRACE MODE Data Center. The main objective of this software product is to provide users with the ability to control the process through a web browser using Internet / Intranet networks or wirelessly (GPRS, Wi-Fi, Bluetooth, etc.). This new web server enables you to access real time data from any computer using different operating systems (Windows, Linux, Mac OS, etc.).

TRACE MODE Data Center has a security system integrated into the TRACE MODE 6 security system.

Therefore, only authorized users can access the web server data. The rights of various users are flexibly configured and administered in

real time. To insure more safety TRACE MODE Data Center supports reliable encrypted VPN connection from external PCs connected to Internet.

53.3.3 The IoT-based modernization of slippage registration system of industrial robot’s adaptive gripper

^A significant number of robotic systems belongs to a control objects class, conditions of their functioning are randomly changed. This is especially true that adaptive robot grippers operating in the dynamic environment, where manipulated objects often accidentally get into a robot work area. The objects may differ in the parameters (mass, geometrical dimensions, material, surface roughness, etc.), which can change during the execution of robot manipulation operations [13].

For the successful solving of the problem robotic system must be able to recognize objects using their own tactile sensory systems. The robotics slip displacement sensors (SDSs) are installed in gripping devices and used to create the clamping force corresponding to the object’s parameters which is especially important during manipulation of fragile objects [13]. The mandatory requirements for the gripping devices include reliable capturing and object holding, stable positioning and inadmissibility of the object damage or destruction.

So, as an example let’s consider a manipulator like presented in Fig. 53.8 [14].

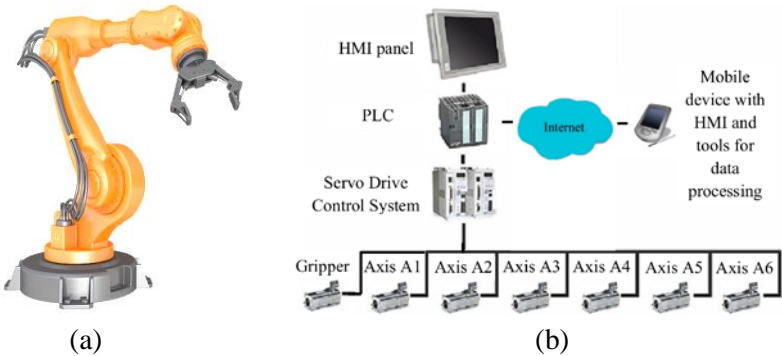


Fig. 53.8 – Robot manipulator: appearance (a) and structure of its control system (b)

This solution is a comprehensive automation system that includes hardware and software. At the lower level, LENZE servo drives are used, the system is controlled by the VIPA programmable logic controller, and the human-machine interface is implemented on the basis of an ESA industrial computer with a pre-installed SCADA zenon visualization system [14]. For the one shown in Fig. 53.8, a, the robot offers two basic vectors of modernization: the use of industrial IoT tools and the development of its sensing system. The first direction of modernization is due to the fact that the basic structure of the manipulator control system (Figure 53.8, b) does not contain the means to control the robot remotely [15, 16]. Then, it is advisable to expand the functionality of such a robot by using existing or creating new IIoT tools. Then, the modernized structure of the robot control system (Figure 53.8, b) will allow remote monitoring and control of the main parameters using IIoT means. According to the second direction, the robot manipulator can be equipped with an adaptive gripper with a sensing system based on a slip sensor [16]. The design of the upgraded sensor with multi-component registration element based on the conductive rubber and the functional structure of the slip detection system for it is shown in Fig. 53.9, (a) and (b), respectively.

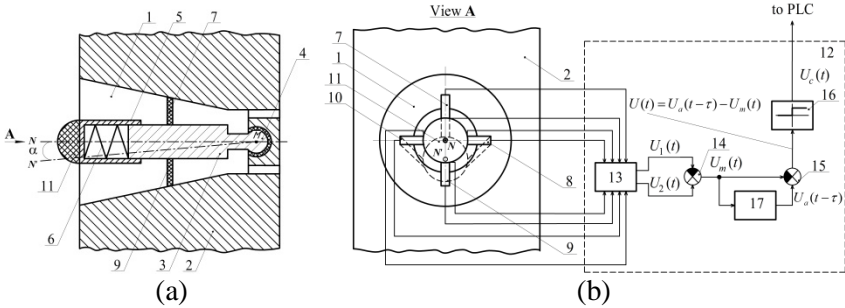


Fig. 53.9 – SDS with electro-conductive plates: mechanical (a) and electronic (b) components: 1 – conical groove; 2 – adaptive robot gripper sponge; 3 – rod, 4 – spherical hinge; 5 – tip; 6 – spring; 7,8,9,10 – plates made of conductive rubber; 11 – tip working surface; 12 – clamping force correction block; 13 – multi measurement unit; 14 – the first adder; 15 – the second adder; 16 – threshold element; 17 – delay element

For the stabilization of the rod position in the SDS four identical plates made of conductive rubber are used (Fig. 53.9, b). These plates are used as registering elements that change their electrical resistance due to deformation. The plates made of conductive rubber were connected as symmetrical Uitonson bridge circuit to compensate the individual components and complete error exclusion constant component of the voltage measuring [14].

Measuring bridge voltage $U_m(t)$ can be represented as a voltage difference $U_m(t) = U_1(t) - U_2(t)$, it depends on the supply voltage and resistors which correspond to individual electrical resistance components of the multicomponent registration element (Fig. 53.9, b). Output threshold element voltage $U_a(t - \tau)$ reiterates the value of the input voltage with delay in a certain period of time τ , which corresponds to the delay between adaptive robot trial motions. Herewith the second adder output signal $U(t)$ is formed which corresponds to the difference between the output signals of the first adder before $U_a(t - \tau)$ and after $U_{out}(t)$ trial motion. The output signal of the second adder, when slippage takes place, gets only positive values $U(t) > 0$ and comes to the threshold element input, ideal static characteristic of which consists of two branches: $U_c(t) = 1$ if $U(t) > 0$ and $U_c(t) = 0$ if $U(t) \leq 0$.

New sensor features expand its application field for slip signals' registration, particularly for operations with different type's objects, including brittle, and for various industrial manufacturing operations in aggressive environments. Simultaneously, IoT-based control system of the manipulator expands functional properties, control abilities and flexibility of object's processing.

53.4 Work related analysis

The presented issues can be supplemented by epy analysis of the existing projects of European partner universities of the ALIOT project on the topic of the given section [17]. Advanced techniques and means for design, modernization and implementation of industrial IoT-based systems are considered in different university-partners, among them *University of Coimbra and Newcastle University, Leeds Beckett University, Consiglio Nazionale delle Recerche - Istituto di Scienza e*

Technologie dell' Informazione "A.Faedo" (ISTI-CNR). So, let's consider the following works.

In [18] authors developed an integrated open-sourced IoT ecosystem that encompasses the entire data life cycle which involves the following processes: data acquisition and data transportation; data integration, processing, manipulation, and computation; visualization; data intelligence and exploitation; data sharing; and data storage. This innovative cloud-based IoT ecosystem will provide a one-stop shop for integrated smart IoT-enabled services to support older people.

A rapidly emerging trend in the IoT landscape is the uptake of large-scale datacenters moving storage and data processing to providers located far away from the end-users or locally deployed servers. The article [19] proposes a belief rule based expert system to predict datacenter PUE (Power Usage Effectiveness) under uncertainty. The system has been evaluated using real-world data from a data center in the UK. The results would help planning construction of new datacenters and the redesign of existing datacenters making them more power efficient leading to a more sustainable computing environment.

In the another side, with the advent of the IoT many applications emerged that are not suitable for well-known paradigms like the Cloud, requiring its extension to provide more features to final users. Thus, the Fog rises as an extension to the Cloud able to provide mobility support, geographical distribution, and lower latency, by moving the services closer to the users, to the edge of the network. So, the paper [20] presents a simple scheduling algorithm for Fog federative environments that organizes Fog instances into divisions for task assignment (this approach could be particularly beneficial for critical time applications, commonly located at the Fog).

Considering a particular enterprise as an end-user in IIoT systems development a good proposal is presented in [21]. Their special issue gathers together contributions related to end-user development for Internet of Things applications. They present not only innovative directions for the programmatic control of these environments, but also attempt to deepen understanding into who end-user developers may be and their changing relationship to the artefacts they create. I turn, in [22] authors discuss the issues raised by the Internet of Things for end user development of interactive applications, and how they can be

addressed. They design space, which identifies the main features that should be addressed to support IoT applications using EUD approaches.

The Internet of Robotic Things is an emerging vision that brings together pervasive sensors and objects with robotic and autonomous systems [15]. The survey [15] examines how the merger of robotic and Internet of Things technologies will advance the abilities of both the current IoT and the current robotic systems, thus enabling the creation of new, potentially disruptive services.

Very important problem related to the robots' localization systems development is considered in [23]. The diversity and heterogeneity of applications, scenarios, sensor and user requirements, make it difficult to create uniform solutions. The authors introduce the general lines of the EvAAL benchmarking framework, which is aimed at a fair comparison of indoor positioning systems through a challenging competition under complex, realistic conditions. Another one [24] focused on the concepts that underlie automation technologies, robotics technologies and the developments, which in the near future, thanks to the application of the paradigm of Ambient Intelligence and the IoT, will be available and usable by all people. The advanced research activities of Research Laboratory in Domotics of the CNR, which is sensitive to make it easier and dignified life for the chronically ill, are described.

Robotic coordination problem is also discussed in paper [25]. The authors show how the concept of virtual pheromones in swarm robotics can be implemented in Jason, a Java-based interpreter for an extended version of AgentSpeak, providing a high-level modelling and execution environment for multi-agent systems. The authors also exploit MQTT, a messaging infrastructure for the IoT. This allows the implementation of stigmergic algorithms in a high-level declarative language, building on top of low-level infrastructures typically used only for controlling sensors and actuators.

Conclusions and questions

Advanced techniques and means for design, modernization and implementation of industrial IoT-based systems are given in the chapter. There is description of IoT-based control and monitoring systems for floating docks as well as design and implementation of IoT-

based control and monitoring systems in robotics in the chapter. Hardware and software means for implementation of mentioned above IoT-based control and monitoring systems is presented in details. Also, approaches to modernization of complex objects in different industrial systems based on IoT are considered for specialized pyrolysis complex and industrial robot's adaptive gripper. Additionally, the chapter includes technologies and projects, developed in partner universities of ALIOT program.

The materials for module ITMM6.2 of Industrial training course "IoT for industrial systems" are presented in this section. They can be used for preparation to lectures and self-learning.

In order to better understand and assimilate the educational material that is presented in this section, we invite you to answer the following questions.

1. Which feature does not apply to the floating dock?
 - a) buoyancy; b) stability, c) ability to change its waterline (draft); d) high speed.
2. What basic system allows the floating dock to change the draft?
 - a) fire safety system; b) ballast system; c) mooring system.
3. What types of sensors are used by the IoT-based control and monitoring system of the floating dock for low-tonnage vessels?
 - a) pressure sensors, temperature sensors and level sensors; b) pressure sensors, speed sensors and acceleration sensors; c) pressure sensors, speed sensors and force sensors.
4. The controller level of the floating dock IoT-based control and monitoring system consists of:
 - a) sensors and actuators;
 - b) various hardware and software means for information processing;
 - c) human-machine interface.
5. Which modules are used as the thermocouple data acquisition modules of the floating dock IoT-based control and monitoring system?
 - a) I7017C; b) I-7061; c) I-7018P.
6. The TRACE MODE Data Center of the floating dock IoT-based control and monitoring system provides:

a) remote web based and wireless access to real-time information using web-browser via Internet/Intranet or wireless networks; b) local access to sensors information; c) opportunity of actuators control.

7. Locomotion control subsystem is a part of:

a) transport subsystem of the mobile robotic complex; b) control subsystem of the mobile robotic complex; c) specialized subsystem of the mobile robotic complex.

8. What types of control systems are the most effective for mobile robots?

a) program; b) adaptive and intelligent; c) tracking.

9. What types of clamping devices are the most appropriate for mobile robots moving on metal ferromagnetic surfaces?

a) mechanical; b) adhesive; c) magnetic; d) pneumatic; e) vacuum.

10. What is the main purpose of the movement control unit of the IoT-based system of monitoring and control of MR positioning?

a) control of the robot clamping devices; b) control of the robot propulsors; c) control of the robot operating instruments.

11. It is expedient to install trajectory control unit of the mobile robot IoT-based monitoring and control on:

a) PC; b) PLC; c) output modules.

12. The DCON protocol is used in the mobile robot IoT-based monitoring and control for data transmission:

a) from sensors to data acquisition modules; b) from PC to the mobile devices; c) from data acquisition modules to PLC.

13. The development of wired and wireless technologies has the following problems of implementation in industry:

a) problems of using alternative energy sources at certain enterprises; b) construction of complex hybrid networks (complicated topology of networks); c) slow transition to the protocol IPv6.

14. The average level of generalized industrial system for complex technological objects and processes based on IoT approach is:

a) the level of the sensors and actuating mechanisms; b) the level of the peripheral monitoring and control devices; c) the level of HMI.

15. What kind of thermo-couples are used in the industrial IoT-based control and monitoring system of specialized pyrolysis complex?

a) K- and L-types; b) M- and E-types; c) B- and T-types.

16. The HMI main screen of the industrial IoT-based control and monitoring system of specialized pyrolysis complex provides:

a) only visualization of the main indicators of the pyrolysis complex; b) only ability to set needed ranges of the parameters of the pyrolysis complex; c) both visualization of the main indicators and ability to set needed ranges of the parameters of the pyrolysis complex;

17. The gripping devices of the robotic systems create the clamping force corresponding to the object's parameters with the help of:

a) strain gauges; b) slip displacement sensors; c) accelerometers.

18. The registering elements of the IoT-based control system of the robot manipulator are made of?

a) bimetallic plates; b) metallic plates; c) conductive rubber.

References

1. O. Rashkovsky, V. Prudivus, O. Schedrolosev, and O. Nodes, *Basics of Floating Docks Design*. Nikolaev: RAL-printing, 2011. (in Ukrainian)
2. S. Jeschke, C. Brecher, H. Song, and D. Rawat, *Industrial Internet of Things*. Switzerland: Springer International Publishing, 2017.
3. O. Vermesan and P. Friess, *Digitising the Industry - Internet of Things Connecting the Physical, Digital and Virtual Worlds*. NY: River Publishers, 2016.
4. A. Topalov, O. Kozlov, and Y. Kondratenko, "Control Processes of Floating Docks Based on SCADA Systems with Wireless Data Transmission," *Perspective Technologies and Methods in MEMS Design (MEMSTECH 2016)*, pp. 57-61, April 2016.
5. G. Yang, H. Liang, and C. Wu, "Deflection and inclination measuring system for floating dock based on wireless networks," in *Ocean Engineering*, vol. 69, 2013, pp. 1-8.
6. Y. Kondratenko, O. Kozlov, O. Korobko, and A. Topalov, "Internet of Things Approach for Automation of the Complex Industrial Systems," *13th International Conference on Information and Communication Technologies in Education, Research, and Industrial Applications. Integration, Harmonization and Knowledge Transfer, ICTERI'2017, CEUR-WS*, pp. 3-18, May 2017.
7. I. Efimov and D. Soluyanov, *SCADA-system Trace Mode*. Ulyanovsk: UIGTU, 2010. (in Russian).
8. V. Bukreeva and A. Tskhe, *Fundamentals of Tool-System Development of SCADA Trace Mode*, Tomsk: TPU, 2004 (in Russian).

9. T. Braunl, *Embedded robotics. Mobile robot design and applications with embedded systems*, 3rd ed. Berlin Heidelberg: Springer-Verlag, 2008.

10. O. Kozlov, O. Gerasin, and G. Kondratenko, "Complex of tasks of monitoring and automatic control of mobile robots for vertical movement," in *SHIPBUILDING & MARINE INFRASTRUCTURE*, vol. 2, no. 8, 2017, pp. 77-87.

11. Y. Kondratenko, O. Kozlov, O. Gerasin, A. Topalov, and O. Korobko, "Automation of Control Processes in Specialized Pyrolysis Complexes Based on Web SCADA Systems," *9th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS)*, pp. 107-112, September 2017.

12. V. Denisenko, *Computer control of technological process, experiment, equipment*. Moscow: Goryachaya liniya - Telekom, 2009. (in Russian)

13. Y. Kondratenko, O. Gerasin, and A. Topalov, "A simulation model for robot's slip displacement sensors," in *International Journal of Computing*, vol. 15, no. 4, 2016, pp. 224-236.

14. SV ALTERA, "Realization of complex control system for industrial robot manipulator", *Svaltera.ua*, 2018. [Online]. Available: <http://www.svaltera.ua/solutions/typical/mashinostroenie/8762.php>. [Accessed: 20-Sep-2018].

15. P. Simoens, M. Dragone, and A. Saffiotti, "The Internet of Robotic Things: A review of concept, added value and applications," in *International Journal of Advanced Robotic Systems*, vol. 15, no. 1, 2018, pp. 1-11.

16. O. Gerasin, Y. Kondratenko, and A. Topalov, "Dependable Robot's Slip Displacement Sensors Based on Capacitive Registration Elements," *The 9th IEEE International Conference on Dependable Systems, Services and Technologies (DESSERT'2018)*, pp. 378-383, May 2018.

17. V. Kharchenko, D. Maevsky, E. Maevskaya, C. Phillips, and L. Vystorobska, "Employers' requirements-oriented assessment of IoT curriculum: The projects CABRIOLET and ALIOT," *9th International Conference on Dependable Systems, Services and Technologies (DESSERT 2018)*, pp. 677-681, May 2018.

18. A. Kor, C. Pattinson, M. Yanovsky, and V. Kharchenko, "IoT-Enabled Smart Living," in *Technology for Smart Futures*, M. Dastbaz, H. Arabnia, and B. Akhgar, Eds., 2018, pp. 3-28.

19. M. S. Hossain, S. Rahaman, A. Kor, K. Andersson, and C. Pattinson, "A Belief Rule Based Expert System for Datacenter PUE Prediction under Uncertainty," in *IEEE Transactions on Sustainable Computing*, vol. 2, no. 2, 2017, pp. 140-153.

20. D. Abreu, K. Velasquez, M. Assis, L. Bittencourt, M. Curado, E. Monteiro, and E. Madeira, "A Rank Scheduling Mechanism for Fog Environments", *IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)*, pp. 363-369, August 2018.

21. P. Markopoulos, J. Nichols, F. Paternò, and V. Pipek, "Editorial: End-user development for the internet of things," in *ACM Transactions on Computer-Human Interaction*, vol. 24, no. 2, 2017, pp. 1-3.

22. F. Paternò and C. Santoro, "A design space for end user development in the time of the internet of things," in *New Perspectives in End-User Development*, F. Paternò and V. Wulf, Eds. Berlin: Springer, 2017, pp. 43-59.

23. F. Potortì, S. Park, A. J. Ruiz, P. Barsocchi, M. Girolami, A. Crivello, S. Lee, J. Lim, J. Torres-Sospedra, F. Seco, R. Montoliu, G. Mendoza-Silva, M. P. Rubio, C. Losada-Gutiérrez, F. Espinosa, and J. Macias-Guarasa, "Comparing the Performance of Indoor Localization Systems through the EvAAL Framework," in *Sensors*, vol. 17, no. 10, 2017, pp. 23-27.

24. D. Russo, "Domotics and Robotics," in *Dolentium hominum*, vol. 84, 2014, pp. 137-144.

25. M. Bottone, F. Palumbo, G. Primiero, F. Raimondi, and R. Stocker, "Implementing virtual pheromones in BDI robots using MQTT and Jason," *5th IEEE International Conference on Cloud Networking*, pp. 196-199, October 2016.

54. APPLICATION OF IOT TECHNOLOGIES IN ENTERPRISE MANAGEMENT AND ENGINEERING

Dr. A.O. Oliinyk, Prof., DrS S.O. Subbotin, Assoc. Prof., Dr.
D.V. Pavlenko, PhD student S.D. Leoshchenko (ZNTU)

Contents

54.1 Application of IoT technologies in the processes of high-tech enterprise management. Smart logistics, material resource and service maintenance management.....	808
54.1.1 Methodologies of enterprise management.....	809
54.1.2 Smart logistics	810
54.1.3 Material resource management.....	810
54.2 Intelligent information technologies and mathematical support of IoT in mechanical engineering	811
54.2.1 Information technologies for designing in mechanical engineering. Determination of the optimal combination of geometric parameters of product components.....	811
54.2.2 Statistical analysis of factors affecting the endurance of product components.....	812
54.2.3 Evaluation of the influence of production modes of parts on the quality parameters of nonrigid products.....	814
54.2.4 Intelligent control in the Internet of Things with the example of the hardening process of gas turbine air-engine details.....	816
54.3 Application of IoT technologies for diagnostics, monitoring and prediction of complex technical system state	818
54.3.1 Expert evaluation of state of products based on fuzzy sets and IoT methods.....	819
54.3.2 Selection of geometric parameters and synthesis of the model of the compressor frequency response.....	820
54.3.3 Methods and IoT technologies for the synthesis of recognition models.....	826
54.3.4 Intelligent data processing in the IoT with the example of a gas turbine air-engine testing.....	828
54.4 Work related analysis	829
Conclusion and questions	830
References	831

Abbreviations

ACF – autocorrelation function
CCF – cross-correlation function
EY – Ernst & Young
IoT – Internet of Things
IIoT – industrial IoT
PSD – power spectral density

54.1 Application of IoT technologies in the processes of high-tech enterprise management. Smart logistics, material resource and service maintenance management

Today the industry of different countries goes through a process of digital transformation. A necessary condition is the introduction into production of a single information space in which enterprise management systems and industrial equipment can exchange data in a timely manner. According to experts, projects in the field of digitalization of production are already 10-100 times cheaper than five to ten years ago. There is an exponential decline in the value of the means of production with the digital component. Thanks to the emerging ecosystem, the IoT platform will be able to connect any partner companies that are ready to provide their capacity to fulfill the order, as well as customers who in real time will be able to choose where and how much to order the goods. According to Cisco, in the world today is becoming increasingly widespread sale of IoT-products and services in the field of IoT. In other words, consumers are increasingly paying for the life of the equipment or its resource [1, 2].

The study of ways to use the IoT will help global organizations to prevent incidents and improve the safety of employees, according to IBM [3]. Data collected from sensors are combined with innovative cognitive capabilities and indicators from other external sources.

Analysis of global practices of IoT implementation shows that the main areas of application of solutions are production, characterized by the presence of one or more of the following conditions:

- production of a wide range of products, the using of a large list of components;
- necessity of improve the quality of production and reduce the degree of marriage;
- necessity of ensure efficient service of previously delivered products;
- necessity of reduce production operating costs;
- significant energy intensity of production;
- complex production environment;
- necessity for rapid troubleshooting of process equipment to reduce unplanned production stops;

- necessity of ensure high productivity of personnel;
- necessity of ensure the safety of personnel;
- necessity for system integration of a wide range.

54.1.1 Methodologies of enterprise management

IoT provides for the inclusion of people, sensors, machines and devices in a single automatic network without manual intervention. It is often perceived as an efficiency tool used in the production and logistics environment to monitor equipment and monitor deliveries. Kevin Cornelius, head of mobility services at Ernst & Young (EY) [4], suggested that this could be just as useful in managing people. This can help HR functions use more intelligent systems for operations and innovation management in training, training and staff development.

Processed data received from sensor systems are provided to all departments of the production. This helps to establish interaction between employees of different departments and make informed decisions.

The information obtained can be used to prevent unplanned downtime, equipment failures, reduce unscheduled maintenance and supply chain management failures, thereby enabling the enterprise to operate more efficiently. When processing a huge array of unstructured data coming from sensors, their filtering and adequate interpretation becomes a priority. Therefore, of particular importance is the presentation of information in a user-friendly form. For this purpose, advanced analytical platforms are used to collect, store and analyze data on technological processes and events, working in real time.

IoT allows creating productions that are more economical, flexible and efficient than existing ones [5]. IP-enabled wireless devices, including smartphones, tablets, and sensors, are already being used extensively in production. The existing wired sensor networks will be expanded and supplemented with wireless networks in the coming years, which will significantly expand the areas of application of monitoring and control systems in enterprises. The next stage of optimization of production processes will be characterized by an increasingly dense convergence of the best information and operational technologies.

54.1.2 Smart logistics

The introduction of IoT technologies in the field of logistics allows optimizing the entire system, including warehouse operations, transportation and delivery. IoT provides an opportunity to improve process efficiency, safety and quality of service. Analytics can be used for the entire value chain, so everyone benefits from the introduction of new technologies: logistics, their partners and end users [6].

IoT technology allows:

- monitor all processes in real time;
- identify people's productivity and make adjustments as you work to improve it;
- automate the process and reduce the amount of manual work;
- optimize the process of joint activities of workers, systems and assets;
- implement a more effective and innovative data-driven approach;
- improve service quality and minimize risks in case of unforeseen circumstances.

Special sensors allow monitoring of production assets within the supply chain. They collect large amounts of data, which are subsequently processed by the system.

At the moment, the most favorable circumstances for the transformation of the logistics industry due to the IoT are formed: the rapid development of the mobile application market, the introduction of user devices into the corporate IT system, the emergence of 5G networks, the development of effective solutions for working with Big Data, etc [7]. In addition, today customers increasingly require innovative approaches, which also contributes to the faster process of deployment of IoT technologies in logistics.

54.1.3 Material resource management

Integration of control systems connected to the Internet can optimize general energy and resource consumption. It is expected that IoT devices will be integrated into all kinds of power-consuming devices [8]. IoT devices will be able to communicate with the power

supplier to effectively balance power generation. Such devices also provide users with the ability to remotely control or centrally manage their devices via the cloud interface and enable advanced features such as scheduling (e.g. remote switching on or off heating systems, controlling furnaces, machines, changing lighting, etc.).

Therefore, IoT is relevant to the Smart Grid since it provides systems to collect and process information about energy and power in automatic mode with the aim to improve the efficiency, reliability, cost effectiveness and sustainability of the production and distribution of electricity and production resources. Using advanced measurement infrastructure devices connected to the Internet backbone, electrical utilities can not only collect data from end users, but also manage other distribution devices such as transformers and reclosers.

54.2 Intelligent information technologies and mathematical support of IoT in mechanical engineering

The main benefit of digitalization and implementation of IoT for mechanical engineering is a unique opportunity to boost the competitiveness of its products relative to the major players. This possibility lies in the fact that even the world's leading manufacturers of engineering products are still in the initial stage of transition to the creation of Industry 4.0 generation products.

If acting quickly, then having the advantages of starting from a low base of production capacity efficiency (the ability to quickly increase it by about four times), based on the availability of a sufficient number of qualified personnel in the field of IT and engineering, proximity to the local consumer and the willingness to develop products, it gave time to occupy a niche in the emerging market of mechanical engineering products of generation 4.0, at least on the local, among the first [9].

54.2.1 Information technologies for designing in mechanical engineering. Determination of the optimal combination of geometric parameters of product components

Automation and IT-technologies are necessary at the stage of design and production, too, as at the stage of realization of finished

products. The opportunities offered by the use of information technology in the design of engineering are simply grandiose. Development and optimization of specialized software allowing in 3D format to see any detail, the unit, not just in the picture, but also in action, opens simply unfathomable horizons for the designers. Things that used to take years of hard work and calculations is now available in a few minutes.

The use of automation processes in production is no less effective, since the control over the production and assembly of various components ensures the production of higher quality products, as well as a significant reduction in the amount of manual labor involved in the enterprise. The issue of reducing the share of manual labor in modern enterprises is extremely acute in recent years.

54.2.2 Statistical analysis of factors affecting the endurance of product components

The tasks of statistical analysis of processes include the definition of some statistical characteristics of processes, such as correlation characteristics, power spectral density (PSD), etc [10].

The previous section has already defined the PSD of a random process based on the established connection of the PSD with the Fourier image. However, Signal Processing Toolbox has a special procedure called “psd” that allows you to immediately find the signal PSD. Appeal to it has the form: “[S,f] = psd(x, nfft, Fmax)”, where x is the vector of the given process values, $nfft$ is the number of elements of the vectors, which are processed by the procedure $nfft$, $F_{max} = 1/T_s$ is the value of the sampling the signal, S is a vector of values of the PSD signal, f is the vector of frequency values that correspond to the values of PSD. In the General case, the length of the latter two vectors is $nfft/2$ [11].

Here is an example of applying the psd procedure to find the PSD of the previous random process:

```
[C,f]=psd(y1,dovg,Fmax);
stem(f(1:200),C(1:200)),grid,
set(gca,'FontName','Arial Cyr','FontSize',16)
title('Power spectral density');
```

```
xlabel('Frequency (Hz)');
```

The result demonstrated at the fig. 54.1.

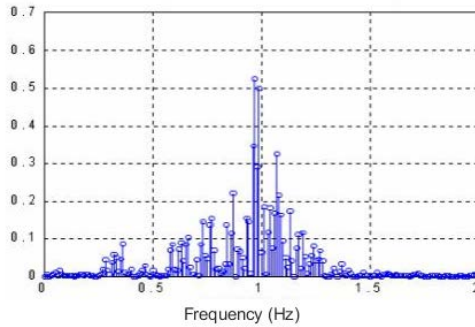


Fig. 54.1 – Result of psd

If the same procedure is called without specifying the output values, the result of its execution will be the output of the PSD graph from the frequency. That demonstrated at fig. 54.2.

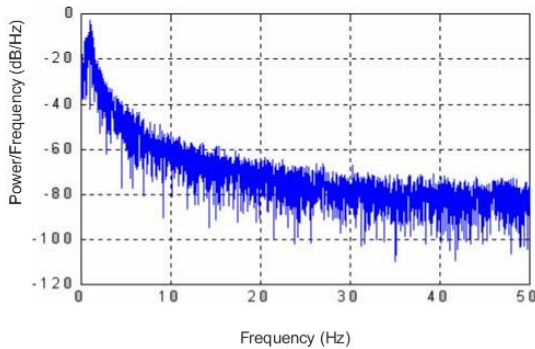


Fig. 54.2 – Result of psd

The `xcorr` function group computes an estimate of the cross-correlation function (CCF) of two discrete-time sequences. Inversion $c=xcorr(x,y)$ computes and outputs the vector c of length $2N-1$ of the values CCF of vector x and the vector y of length N . Inversion $c=xcorr(x)$ computes the autocorrelation function (ACF) of the sequence given in the vector x .

Let try example. Two sensors at different locations measure vibrations caused by a car as it crosses a bridge. Load the signals and the sample rate, $F_s=11025\text{Hz}$. Create time vectors and plot the signals. The signal from Sensor 2 arrives at an earlier time than the signal from Sensor 1.

```
load sensorData
t1 = (0:length(s1)-1)/Fs;
t2 = (0:length(s2)-1)/Fs;

subplot(2,1,1)
plot(t1,s1)
title('s_1')
subplot(2,1,2)
plot(t2,s2)
title('s_2')
xlabel('Time (s)')
```

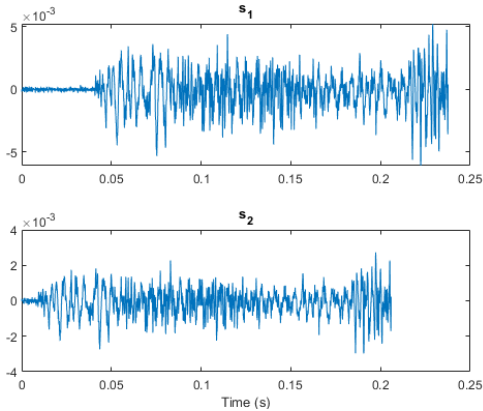


Fig. 54.3 – Plot the cross-correlation

54.2.3 Evaluation of the influence of production modes of parts on the quality parameters of nonrigid products

One of the parameters that ensure high quality and reliability of products is the accuracy of their manufacture. The accuracy of

manufacturing parts is the degree of compliance of the parameters of the part to the parameters that are set by the designer in the working drawing. Compliance with the actual and specified parts designer is determined by the roughness and physical and mechanical properties (material, heat treatment).

Accuracy characterizes along with the geometric parameters of the product and the uniformity of quality indicators such as power, performance, efficiency, etc. More accurately manufactured devices have a narrow field of variation of these indicators and higher performance. The accuracy of manufacturing parts depends on the complex processes used in this production. Every technological process of manufacturing parts inevitably makes certain errors, so it is almost impossible to get an absolutely accurate part. Improving the accuracy of manufacturing primary blanks can reduce machining allowances, which determines the structure of the processing process, reduces its cost and the amount of assembling work. Part of the dimensions of the part must be made with guaranteed accuracy (within the specified clearances) and the remaining dimensions are performed without drawing limits deviations. In the manufacture of such parts on the free dimensions set technological clearances. The accuracy of the size is determined by the accuracy of the cutting tool on the size (setting), the length of the passes and the size of the tool (dimensional or profile). The accuracy of the mutual arrangement of the surfaces is determined by various factors of the process. When processing a part in multiple operations, the accuracy of the relative positioning of the surfaces depends on the errors in the installation of the part in different operations. When processing parts of complex shapes can simultaneously process all the surfaces of one shaped tool, in this case, the accuracy of the relative position of the surfaces is determined by the accuracy of the tool. The accuracy of the part shape is important for mating surfaces. Therefore, in the manufacture of precise parts, the permissible deviation of the shape is set within a stricter range than the accuracy of the size. The accuracy of the surface shape is usually higher than the accuracy of the relative position of the surfaces, and this accuracy is higher than the accuracy of the dimensions that bind the surfaces.

The accuracy of manufacturing parts depends on the complex processes used in this production. Every technological process of manufacturing parts inevitably makes certain errors, so it is almost

impossible to get an absolutely accurate part. Improving the accuracy of manufacturing primary blanks can reduce machining allowances, which determines the structure of the technological process, reduces its cost and the amount of assembling work.

The following factors affect processing accuracy:

- inaccuracy and deterioration of the machine;
- inaccuracy and deterioration of fixtures and tools;
- error in the installation of parts on the machine;
- temperature deformation;
- residual stresses of the workpiece;
- copying errors of previous processing;
- inaccuracy of means and methods of measurement.

54.2.4 Intelligent control in the IoT with the example of the hardening process of gas turbine air-engine details

The company "Motor Sich" hardened steel balls in ultrasonic field over 275 titles of parts of complex design are compressor blades and the turbine drives the compressor and turbine, flowpath surface centrifugal and axial monowheels, gears, spline shafts and the surface [12].



Fig. 54.4 – Fragments of the shaft of the compressor before and after treatment in the fluidized abrasive (1 - after turning; 2-after PSA)

The main technological features of hardening gas turbine air-engine details balls in the ultrasonic field are:

- as working bodies used steel balls of stainless steel with a diameter of 0.4-3.0 mm;
- loading balls to harden the blades airfoil is in the range (200-1000 g), and the consolidation of their shanks (30-60 g); the time of hardening the blades airfoil is (4-10 min), and shanks: 20-45 with;
- number of simultaneously hardened blades (10-60 pieces);
- the amount of wetting liquid in the working volume is within 4-10 ml;
- the oscillation frequency of the transducer is 16-22 kHz, and the oscillation amplitude of the emitting surface is 10-25 microns.

The ultrasonic hardening unit and the compressor drum are shown in Fig. 54.5.

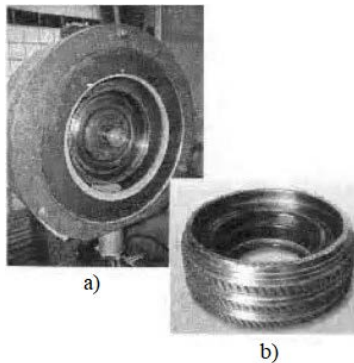


Fig. 54.5 – Installation (a) for ultrasonic hardening and compressor drum (b)

In the process of ultrasonic hardening in the surface layer of the bearing surfaces of parts formed residual compression stress, the maximum of which is at a depth of 20-40 microns.

The main feature of the surface profilogram after ultrasonic hardening, in comparison with their previous grinding, is an increase in the radius of the cavities of micro-roughness, which leads to a decrease in the value of the technological stress concentration.

The depth of the plastically deformed layer varies between 15-35 microns.

The microhardness of the surface layer increases after ultrasonic hardening. The endurance limit after ultrasonic hardening of parts is increased by 23-40 %.

To control such precise and delicate processes, a number of sensor systems are needed that can monitor quality and filter out defects. It should be noted that the storage of such data requires huge resources. On the other hand, processing of such big data arrays also requires significant computing resources. In this case, it becomes necessary to use cloud technologies. However, technologies that enable real-time monitoring of complex processes can significantly improve production quality.

54.3 Application of IoT technologies for diagnostics, monitoring and prediction of complex technical system state

In terms of monitoring the state of complex technical systems, it is advisable to use new technologies based on the work of mathematical algorithms with large information flows and databases. In some cases, there is a need to monitor the status of complex technical systems, followed by the safety and systematization of measurements, which reduces the cost of maintenance of systems.

When monitoring the status of complex technical systems using IoT, the following features should be noted [13]:

- continuous monitoring and real-time data collection
- combining and comparing data from different sources: sensors, infrastructure, applications;
- obtaining and processing not only unstructured data, but also integration with classical databases;
- ability to easily create new key performance indicators and alerts;
- the ability to obtain performance indicators related to industrial equipment and business indicators in one place.

This provides a broad context for decision-making on various issues.

In the case of prediction the technical condition, it should be noted that we are talking about the maintenance of equipment, according to the results of the predict. This does not apply to the planned

maintenance schedule linked to the actual use and schedule of the production load, and, especially, the repair after the fact, when, for example, the clutch bearing of the conveyor engine burst and expensive equipment failed, which led to production downtime and associated losses. The probability of such an event can be predicted from the readings of the sensors and the data on the heating and vibration of the engine clutch transmitted by them. These data are transmitted for verification with the so-called historical data accumulated earlier in the operation of this engine. Thus, it can be predicted not only accurately the critical time for repair, but also, for example, in advance to order the necessary repair kit. The very same preventive maintenance can be carried out not in an emergency, with the forced stop of the production line, and, say, during its planned changeover.

Applying technologies allow to centrally prepare and conduct tests simultaneously recording many parameters of the transmission to observe what is happening in the test area, to store and process obtained in the experiment, the data give experimental data to remote workstations using the local informational network of the enterprise.

For success of the IoT projects, it is necessary to create working ecosystems that cover not only the modernization or retrofitting of equipment and the deployment of new management systems, but also the optimization of production processes, training and training of personnel, close work with the enterprise's suppliers, customers and other stakeholders [14]. To implement this approach, it is required that all the necessary information about the actual state of resources (raw materials and materials, electricity, machines and industrial equipment, vehicles, production, marketing, sales) be available, both within one and at different enterprises, management systems of different levels. This connection is provided by the cloud – connection of any devices and systems to it is implemented by using the application programming interface mechanism.

54.3.1 Expert evaluation of state of products based on fuzzy sets and IoT methods

The importance and background of technical diagnostics can be easily explained by the wide application in technology and medicine,

where often the knowledge obtained from the expert may not be enough or they may not be complete.

As theoretical bases of technical diagnostics are emerging technologies pattern recognition, artificial neural networks, fuzzy systems, optimization. The basis for decision-making are the precedents.

The general problems is a need of model complexity reduction and a model construction and working speed increasing. Caused by these problems, as a rule, too large sizes of the analyzed samples and the structure and parameters of the model.

The task of diagnostic model construction by precedents based on neural-fuzzy networks can be divided into two tasks:

- The task of diagnostic model structural-parametric synthesis on the neural-fuzzy networks basis in the optimization statement;
- The task of diagnostic model structural-parametric synthesis on the neural-fuzzy networks basis in the constructivist statement. For integrated neural-fuzzy networks: formation of fuzzy terms, determining the number of neurons in the neural-fuzzy networks and in each of its layers, weight assignment and activation functions of neurons, defining the network topology, calculation of the weight coefficients of interneuronal connections based on heuristic rules [15].

54.3.2 Selection of geometric parameters and synthesis of the model of the compressor frequency response

Method of exhaustive search stipulates evaluating each of the $2^M - 1$ possible control points Xe of the search space XS . Due to the full search of all possible solutions $Xe \in XS$, this method allows to find a solution P^* , which is characterized by the optimal value of the target function $V(P^*) = \min_{Xe \in XS} V(Xe)$. Since the computational complexity of this method $O(2^M)$ depends significantly on the initial number of features of the training sample $S = \langle P, T \rangle$, this method can be used to select features from small samples. This significantly complicates and makes it impossible the using of this method for processing large amounts of data [16].

Heuristic methods use greedy search strategy, using of which involves the successive addition (removal) of features to the current set of features. This approach is simpler than a full search and requires less computing time.

However, the combinations of characteristics P^* , found by these methods, generally are characterized by unacceptable values of the optimality criterion $V(P^*)$ as heuristic methods explore a very limited region of the search space.

As a result, combinations of features that have an optimal (or acceptable) value of the target criterion $V(P^*)$. The computational complexity of such methods is proportional to the square of the number of features M of the initial sample $S = \langle P, T \rangle : O(M^2)$. Therefore, the use of this approach, if necessary, for the feature selection from large samples of data is also difficult [16].

Stochastic methods [1, 17-21] are based on the using of probabilistic procedures in the control point $Xe \in XS$ processing, and usually work on each iteration with some set of solutions $R(iter) = \{\chi_1, \chi_2, \dots, \chi_{N_\chi}\}$. Each k -th solution $\chi_k \in R(iter)$ corresponds to the k -th control point Xe_k researching at the iteration $iter$ in the search space $XS : \chi_k \rightarrow Xe_k$. Such methods can use an evolutionary, multi-agent or other approaches of computational intelligence as the mathematical basis. Stochastic methods search for the specified number of iterations $Iter$ processing $Iter \cdot N_\chi$ of control points (where N_χ is the number of solutions being processed at each iteration of the stochastic search). Therefore, the computational complexity $O(Iter \cdot N_\chi)$ of this approach does not depend directly on the number of features M in the original sample, which allows it to be used for reducing the large amounts of data.

However, such methods tend to loop in the areas of local optima (in the search process there is a concentration of a set of test points χ_k near the areas of local extrema), which reduces the effectiveness of their application and increases the search time. Therefore, the expansion of the search space of researching areas XS is ensured by

using a large number N_χ of control points χ_k researched at each iteration. Such an approach is also not effective because of the low diversity of solutions in the set $R(iter)$. In addition, using a large number of checkpoints per iteration increases the search time [16].

Also the approach providing ranking of features p_m on values of their individual importance $V(p_m)$ in relation to an output parameter T can be used for feature selection. This approach is computationally simple (its computational complexity $O(M)$), but it does not take into account the mutual dependence of features.

Therefore, in practice, in the conditions of mutual dependence of features, this approach does not allow the selecting sets of features characterized by optimal or acceptable value of the evaluation criterion of group informativeness $V(P^*)$ [16].

Thus, the presence of disadvantages of existing methods of feature selection leads to the expediency of development of a new method based on stochastic approach and high-productive calculations and free from the identified shortcomings.

Evolutionary selection of informative features. The generalized method of evolutionary search can be written as follows [17].

Step 1. Start at start time $t = 0$.

Step 2. Generation of the initial population of individuals $P(t)$.

Step 3. Calculation of fitness function for all individuals in population $F(P(t))$.

Step 4. Check the search completion conditions (time, number of iterations, fitness function value, etc.). If the end criteria are met, go to step 12.

Step 5. Increase time counter (iterations): $t = t + 1$.

Step 6. Select part of the population (parent species) to cross P' .

Step 7. Cross the selected parent species $P'(t)$.

Step 8. To apply the mutation operator to the individuals of $P'(t)$.

Step 9. Calculate the new fitness function of population $F(P'(t))$.

Step 10. Select the surviving species based on the level of fitness.

Step 11. Go to step 4.

Step 12. Stop.

The selection of informative features using evolutionary search can be carried out in the following sequence:

Step 1. Generate initial combinations of informative features in the form of K_p codes ($p = 1, 2, \dots, M$, where M is the number of generated codes) of dimension n (number of features).

Step 2. For each code K_p to obtain the dependence $y_{calc} = (K^p, X, Y)$ given the informativeness of the i -th characteristic.

If $K_i^p = 0$ ($K_i^p - i^{th}$ bit of K^p code), the i^{th} sign is considered to be uninformative and is not taken into account for the construction of the ursch model (K^p, X, Y) . If $K_i^p = 1$, then the i^{th} characteristic is considered informative and is taken into account to build the model $y_{calc} = (K^p, X, Y)$.

Since this operation will be repeated quite often, it is advisable to choose a mathematical model for the $y_{calc} = (K^p, X, Y)$ so that it does not put forward large demands on computer resources such as memory, computing power and processor speed. A multidimensional linear regression model can be used as such.

Step 3. For all K^p calculate model error:

$$E = \frac{1}{m} \sum_{i=1}^m (y^i - y_{calc}^i)^2$$

where y_{calc}^i is the value of the function calculated by the model $y_{calc} = (K^p, X, Y)$, y^i is the actual value of the function, m is the number of instances.

Step 4. Check the conditions of the search completion: reaching the time limit T , the number of iterations I , the level of the maximum permissible error E_{max} . If the end criteria are satisfied, go to step 6.

Step 5. Applying genetic search, generate a new array of codes. Go to step 2.

Step 6. Depending on the code K^p , which gives the minimum RMS error to be the optimal function $y_{calc} = (K^p, X, Y)$, but with the application of more complex mathematical models to ensure high accuracy of the approximation.

Step 7 . Stop [17].

Developed using MatLab software module contains functions CalculateDivergence (calculates the error of the model derived from multivariate linear regression. This function is the target in search methods) and DimensionReduction_EM (performs evolutionary search for the optimal combination of informative features). As the target functions used CalculateDivergence.

On the basis of the found combination of informative features, a model of the natural oscillation frequency of the blades using artificial neural networks is constructed.

This software structure is quite convenient and flexible for the transition to solving other optimization problems. With the help of the developed functions, several combinations of the most informative features are obtained, among which the best one is selected.

After making decisions about the informative features of the training set were excluded uninformative features ($x_2, x_3, x_5, x_7, x_8, x_{10}, x_{11}, x_{13}$). The obtained regression model of the blade natural oscillation frequency has the following form:

$$f = 154.2675 + 17.733B_{3-3} + 94.6056C_{23-3} - 23.57C_{\max 5-5} - 6.1395B_{8-8} - 37.06C_{28-8}$$

Regression models of the blade natural oscillation frequency for each section were built separately. The obtained models had the form:

- for section A_{3-3} : $f = 14.64B_{3-3} + 87.05C_{13-3}$;
- for section A_{5-5} : $f = -542 - 14.64B_{5-5} - 66 \times C_{15-5} + 4542C_{25-5}$;
- for section A_{8-8} : $f = 1018 - 59C_{28-8} - 14B_{8-8}$.

The relative errors of these regression models are 0.0072, 0.0069, and 0.0074, respectively. The accuracy of the regression model obtained is 0.0060, which makes it more acceptable for use in comparison.

As is known, neural network methods allow obtaining much more accurate models than linear regression. Thus, further modeling of frequency of natural oscillations of blades on the basis of the selected informative signs by means of the two – layer perceptron which first

layer contained 3 neurons, and the second layer-1 neuron was carried out. All neurons had a sigmoid activation function $\psi(x)=1/(1+e^{-x})$. The neural network inputs were supplied with the values of pre-normalized features. The network output was supplied with the hardening coefficient value for the corresponding instance. As a target function, the minimum standard error of the network for the entire sample $goal = 10^3$ was used.

Neural network training was based on the Levenberg-Marquardt algorithm. The average value of the relative error of the obtained FNS model was 0.0028. The matrix of weight coefficients of the obtained neuromodel is given in table 54.1. The high accuracy obtained in the simulation of the natural oscillation frequency of the blades allows us to conclude about the high degree of influence of the geometric parameters of the pen on the value of the natural oscillation frequencies of the blades.

The results of the experiments show that the models obtained by the evolutionary selection of informative features are more accurate compared to the models obtained on the basis of statistical data analysis.

Thus, evolutionary search can be recommended for use in problems of technical and biomedical diagnostics, economic and mathematical modeling, management and decision support.

However, the classical evolutionary search is highly iterative, the duration of this method strongly depends on the initial search conditions, which means that its efficiency is not high enough.

Therefore, to improve the efficiency of the classical method of evolutionary search in solving the problems of selection of informative features, it is recommended to analyze the informative features at the stage of initialization of the parameters of the evolutionary method by using traditional non-iterative methods for assessing the individual informative features.

Table 54.1 – The matrix of weight coefficients of the model

Number of layer	The number of the neuron in the layer	Number of neuron input					
		0	1	2	3	4	5
1	1	-489.6770	647.2856	671.6672	64.2427	-17.0205	-353.9352
	2	-35.5424	20.4147	49.8359	200.7345	-164.4796	-103.8206
	3	12.7964	-12.6995	-14.0266	-61.7603	55.1382	31.0127
2	1	83.6908	2.5554	-85.9099	85.5576		

54.3.3 *Methods and IoT technologies for the synthesis of recognition models*

Known that y depends on x_1 and x_2 , but we don't know how. It is necessary to construct a neuro-fuzzy approximation of the dependence

$y(x_1, x_2)$ from the observations presented in the form of a table (training sample). To check the approximation properties of the neuro-fuzzy model, will be using the test sample presented in the Fig. 54.6.

Training set			Test set		
x1	x2	y	x1	x2	y
25	76	2.3	15	0.86	0.9
27	79	2.2	25	0.47	2.5
23.5	91	1.8	26	0.57	2.6
15	89	1.2	15	0.98	0.9
14.5	79	1.0	13.5	0.68	0.9
17	61	1.4	16.5	0.93	1.6
20	96	2.0	19.5	0.67	1.9
23	89	2.0	22	0.58	2.1
26.5	57	2.6	25	0.82	2.0
29	59	2.7	28	0.86	2.8

Fig. 54.6 – Information about training and test sets

In MATLAB, create a training sample variable p and a test sample variable t :

```
p=[25 76 2.3; 27 79 2.2; 23.5 91 1.8; 15 89 1.2; 14.5 79 1.0; 17 61
1.4; 20 96 2.0; 23 89 2.0; 26.5 57 2.6; 29 59 2.7];
t=[15 0.86 0.9; 25 0.47 2.5; 26 0.57 2.6; 15 0.98 0.9; 13.5 0.68 0.9;
16.5 0.93 1.6; 19.5 0.67 1.9; 22 0.58 2.1; 25 0.82 2.0; 28 0.86 2.8];
```

Start the ANFIS editor by typing: `anfisedit`

In the Load data area, set the test sample variables (select Type: Training in the list and from: Worksp in the list), then press the Load data button and enter in the input variable name: p) and training set (choose in the list, Type Testing and the list from: Worksp., then press the Load data button .. and enter in the input variable name: t).

In the Generate Fis area, select: Sub. clustering and click Generate Fis. In the field of Train the FIS will select the method of optimization Optim. method: hybrid. Set the acceptable error tolerance level to 0.000001. Set the number of iterations of Epochs: 300. Press the Train now button. In the graphics area of Training Error we will observe how the error of the neuro-fuzzy network changes during the training. By

clicking the Structure button, we get an image of the generated structure of the neuro-fuzzy network.

The resulting FIS structure can then be stored on disk or used for forecasting, for example, using test sample t . To test, select the sample for which you are testing (Training - training, Testing - test), and click Test now. At the bottom of the form you will see the average testing error (Average Error), and the graph will show blue dots - the target values of the output, and red stars is the calculated values of the output of the neuro-fuzzy network [18].

54.3.4 Intelligent data processing in the IoT with the example of a gas turbine air-engine testing

The Fig. 54.7 shows how IoT technologies can be used in diagnosing and predicting the state of the gas turbine air-engine.

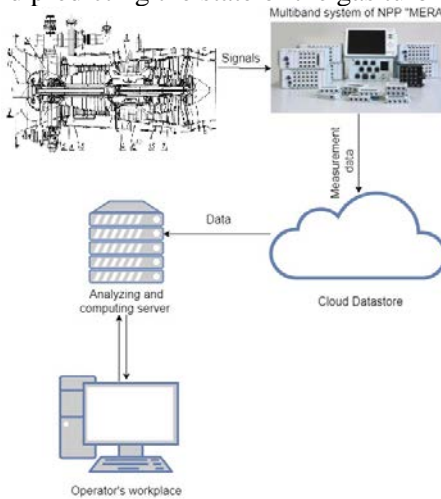


Fig. 54.7 – Plot the cross-correlation

Throughout the gas turbine air-engine mechanism installed special sensors that collect information about the current state. Information is filtered and processed on special equipment. Amounts of data are uploaded to the cloud after preprocessing. A computing server at any

time can get the necessary information and report any problems to the operator.

54.4 Work related analysis

The section is based on analysis of publications and materials of leading universities and companies in IoT technologies using in engineering.

There are a small number of companies that successfully using the IoT technology in industrial sphere. This explains a few USA and EU universities including ALIOT project partners conduct research and implement education MSc and PhD modules related to implementation IoT technologies in engineering. In particular, the following courses and programs have been considered:

- Newcastle University, United Kingdom: MSc course "Embedded Systems and Internet of Things (ES-IoT) MSc" [19]. This is a unique blend of five fields of knowledge which work well together: tools, techniques and design of ES-IoT and subsystems; scientific and engineering principles and practices of Computing Science and Electronic Engineering; embedded computer systems architecture; networking and communication systems; computer programming;

- Beijing-Dublin International College, China: BE IoT Engineering for BSc [20]. is an interdisciplinary bachelor's degree programme that combines the study of electronic engineering and computer science, with an emphasis on internet technologies, wireless communications, sensor devices, and cloud computing;

- University of Bradford, United Kingdom: IoT course for MSc [21]. This unique full-time Master's programme is designed by experts in the field with wealth of research and development experience in IoT to address this shortage of professionally qualified specialists;

- The University of Sydney, Australia: IoT course for MSc [22]. The new major aims to offer a comprehensive program with state of the art IoT technologies and students can engage in the creative development of the innovative Internet of Things.

As a complex cyber-physical system, IoT combines various devices equipped with sensing, identification, data processing, communication and network capabilities. In particular, sensors and actuators are becoming more powerful, cheaper and smaller, resulting in their

widespread use. The industry has a strong interest in deploying IoT devices for the development of industrial applications such as automatic monitoring, control, management, operation and maintenance. It is expected that due to the rapid development of technology and industrial infrastructure, IoT will be widely used in the industry.

Production companies demonstrate greater openness to new IoT technologies against the background of increasing trend of digitalization of the country's economy as a whole.

Among the benefits expected from IoT, the surveyed enterprises point out the possibility to improve the efficiency of processes, including by ensuring their transparency, as well as to reduce the risks, downtime and costs of production

Conclusion and questions

Materials are a tool for the introduction of IoT technologies in the industrial production of complex technical systems.

- Production management methodologies are described.
- The introduction of IoT in the logistics system.
- Use IoT to manage production resources.

For example, the introduction of IoT in the testing of gas turbine engines disassembled mechanism the introduction of IoT in the industrial industry.

1. In what areas Can IoT be implemented in the industry?
2. What are The IoT opportunities in the industry today?
3. What conditions must be met to be able to introduce IoT into production?
4. What areas of production can be linked using IoT tools?
5. How IoT can work in the field of logistics?
6. How does the resource management mechanism work using IoT technologies?
7. What is meant by the term Smart grid?
8. What are the main benefits IoT can provide for the mechanical engineering?
9. Why is it necessary to carry out statistical analysis?
10. What can be learned from the power spectral density value?

11. What functions can be used to perform statistical analysis in MatLab?
12. What is precision parts manufacturing?
13. Why is precision part manufacturing important?
14. What factors can affect the accuracy of parts?
15. What are the options for hardening parts of the gas turbine engine exist?
16. How you can use IoT technologies and their interactions to control the process of hardening parts?
17. How IoT technologies can be used for the diagnosis of complex technical systems?
18. How can IoT technologies be used to monitor complex technical systems?
19. What is the difference and advantages of using forecasting before scheduled inspection and repair?
20. What methods for the selection of features can be used in the workplace?
21. How can I start the synthesis of recognition models?

References

1. K. Ashton (2009) *That 'Internet of Things' Thing*, RFID Journal, vol. 22, pp. 97-114, 2009.
2. Jia, X., Feng, O., Fan, T. and Lei Q. (2012) *RFID technology and its applications in internet of things (IoT)* Proc. 2nd IEEE Int. Conf. Consum. Electron., Commun. Netw. (CECNet). China, Yichang.
3. IBM Employee Wellness and Safety solution in top 20 IoT industrial applications [Online]. Available at: <https://www.ibm.com/blogs/internet-of-things/ibm-employee-wellness-safety-solution/>.
4. Strategies in the management of Human Resources [Online]. Available at: <https://www.ukessays.com/essays/management/strategies-in-the-management-of-human-resources-management-essay.php>.
5. Zhonga, R., Xu, X., Klotz, E. and Newman S. (2017). *Intelligent Manufacturing in the Context of Industry 4.0: A Review*. Available at: <https://doi.org/10.1016/J.ENG.2017.05.015>.

6. Tadejko P. (2015). *Application of Internet of Things in Logistics - Current Challenges*. Journal Economics and Management, 7(4), 54-64 pp.

7. Lin, B. , Lin, F. and Tung, L. (2016) *The Roles of 5G Mobile Broadband in the Development of IoT, Big Data, Cloud and SDN*. Communications and Network, 8, 9-21. doi: 10.4236/cn.2016.81002.

8. Ji, Z. and Qi A. (2010) *The application of internet of things (IOT) in emergency management system in China*. Proc. 2010 IEEE Int. Conf. Technol. Homeland Security (HST).

9. Porter M. (1990) *The Competitive Advantage of Nations*. New York : TheFree Press.

10. Marques, A., Segarra, S., Leus, G and Ribeiro A. (2016) *Stationary Graph Processes and Spectral Estimation*. Available at: 10.1109/TSP.2017.2739099.

11. Power Spectral Density Estimates Using FFT [Online]. Available at: <https://www.mathworks.com/help/signal/ug/power-spectral-density-estimates-using-fft.html>

12. Boguslaev, A.V., Oleynik, Al.A., Oleynik, An.A., Pavlenko, D.V. and Subbotin S.A. (2009) *Advanced technologies for modeling, optimization and intelligent automation of aircraft engine life cycle stages [Progressivnyie tehnologii modelirovaniya, optimizatsii i intellektualnoy avtomatizatsii etapov zhiznennogo tsikla aviatsionnyih dvigateley]* Zaporozhzhia: "Motor Sich", P. 468.

13. P. P. Ray, M. Mukherjee and L. Shu (2017) *Internet of Things for Disaster Management: State-of-the-Art and Prospects* in IEEE Access, vol. 5, pp. 18818-18835.

14. Zhang Y. C. and Yu J. (2013) *A study on the fire IOT development strategy* Procedia Eng. Vol. 52.

15. Subbotin, S. A., Blagodarev, A. Yu. and Ye. A. Gofman (2017) *The neuro-fuzzy diagnostic model synthesis with hashed transformation in the sequence and parallel mode*, Radio Electronics, Computer Science, Control, Vol.1, 56-65 pp.

16. Oliinyk, A., Leoshchenko, S., Lovkin, V., Subbotin, S. and T. Zaiko (2018) *Parallel data reduction method for complex technical objects and processes*, 9th International Conference on Dependable Systems, Services and Technologies DESSERT'2018. IEEE Catalog number: CFP18P47-ART 978-1-5386-5903-8.

17. Boguslaev, A.V., Oleynik, A.A., Puhalskaya, G.V. and Subbotin S.A. (2006) *The selection of geometrical parameters and synthesis model frequency characteristics of the blades the compressor on the basis of evolutionary search's* [Otbor geometricheskih parametrov i sintez modeli chastotnoy harakteristiki lopatok kompressora na osnove evolyutsionnogo poiska], Visnik dvigunobuduvannya, pp.14-17.

18. Subbotin S.A. (2006) *Methodical instructions to performance of independent works on discipline "Mathematical foundations of knowledge representation"*, Zaporizhzhia: ZNTU, 51 P.

19. Embedded Systems and Internet of Things (ES-IoT) MSc, <https://www.ncl.ac.uk/postgraduate/courses/degrees/embedded-systems-internet-of-things-msc/#profile>

20. BE IoT Engineering, <http://www.ucd.ie/bdic/study/beinternetofthingsengineering/>

21. IoT course for MSc, <https://www.bradford.ac.uk/courses/pg/internet-of-things/>

22. Internet of Things, course University of the Sydney, <https://sydney.edu.au/courses/subject-areas/major/internet-of-things0.html>

55. DEVELOPMENT AND HARDWARE OPTIMIZATION OF CONTROL UNITS FOR IOT DEVICES IN INDUSTRY SYSTEMS

Assoc. Prof., Dr. R. M. Babakov
(Vasyl' Stus Donetsk National University, Vinnytsia)

Contents

Abbreviations	835
55.1 The problem of hardware expenses optimization in IoT devices for industry systems.....	836
55.2 The IoT device control unit in the form of finite state machine with canonical structure.....	837
55.3 The IoT device control unit in the form of finite state machine with counter	839
55.4 Generalizations for an FSM with counter.....	840
55.5 Datapath of transitions.....	850
55.6 Synthesis of IoT device control unit in the form of finite state machine with datapath of transitions	853
55.6.1 Stages of structural synthesis of FSM with DT	853
55.6.2 Algebraic synthesis of FSM with DT	854
55.6.3 Algebraic synthesis by an exhaustive search.....	856
55.7 Evaluation of the effectiveness of FSM with DT as IoT device control unit	858
55.8 Integration of FSM with DT into IoT device	859
55.9. Work related analysis	861
Conclusion and Questions	861
References	863

Abbreviations

BIMF – Block of Input Memory Functions

BMO – Block of Microoperations

CMCU – Compositional Microprogrammed Control Unit

CS – Combinational Circuit

CT – Counter

CU – Control Unit

DT – Datapath

FSM – Finite State Machine

GSA – Graph-Scheme of Algorithm

LSS – Linear Sequences of States

LUT – Look-Up Table

MCU – Microprogrammed Control Unit

MX – Multiplexor

55.1 The problem of hardware expenses optimization in IoT devices for industry systems

The hardware components of the industrial Internet of Things systems are digital devices of varying complexity – both local and distributed [1, 2]. The main criteria for designing such systems are low cost/low complexity/high reliability and low power consumption, which determine the area of their application in general and for industrial systems in particular [3, 4].

One of the main components of modern digital systems is the control unit (CU) [5]. Its function is to coordinate the work of all units of the system, and its characteristics largely determine the characteristics of the system as a whole. Recently, control algorithms implemented by CU are becoming more and more complex, which increases hardware expenses in the CU circuit. The increase in hardware expenses affects such system characteristics as cost, power consumption, size, reliability. In this aspect, the problem of hardware expenses optimization in the control units is actual [6-8].

Today, the following methods of implementing the CU are known:

- Microprogrammed finite state machine (FSM), in which the control algorithm is implemented by hardware in the form of a network of logic elements [1-3].
- Microprogrammed control unit (MCU), in which the control algorithm is specified as the contents of memory module [8].
- Compositional microprogrammed control unit (CMCU), which is a combination of FSM and MCU devices [9].

The FSM structure is capable of performing multidirectional microprogram transitions in one cycle of operation, possessing the maximum speed among other classes of control units. However, it is characterized by the maximum hardware expenses and maximum cost due to the maximum use of combinational logic.

The structure of the MCU is characterized by high regularity and low hardware expenses due to the storage of the microprogram in the memory module (usually ROM or PROM). But in each step of the work of the MUU can perform a transition, depending only on a single input signal. This feature requires the insertion of additional states into the

implemented algorithm, which increases the execution time of the algorithm to the maximum value among these CU classes.

The CMCU is the composition of FSM and MCU, has intermediate characteristics between these structures. Currently, there are many methods for CU hardware expenses optimization [5-10] such as:

- Increasing the number of levels of conversion of logical signals in the circuit.
- Consideration of the features of the elemental basis used.
- Special state coding and modification of the implemented control algorithm.

When designing a CU, one of the ways to represent control algorithms is the graph-scheme of algorithm (GSA) [5, 6]. An example of a GSA is shown in Fig. 55.1. This GSA is marked with $M = 15$ Moore FSM states $a_0 - a_{14}$, contains $N = 5$ microoperations $y_1 - y_5$, $L = 3$ logical conditions $x_1 - x_3$ and $B = 19$ microprogram transitions. Digit capacity of state code $R = \lceil \log_2 M \rceil = 4$.

55.2 The IoT device control unit in the form of finite state machine with canonical structure

There are a lot of modern hardware components applied in IoT devices [11]. These digital devices are described by FSM model. The structure of an FSM with a canonical structure is shown in Fig. 55.2 [6]. In it, the block of input memory function (BIMF block) forms the code D of the next state according to the system of equations (55.1). The block of microoperations (BMO block) forms a set of microoperations Y in accordance with the system of equations (55.2) in the case of the Mealy FSM and the system (55.3) in the case of the Moore FSM. The memory register (RG block) is used to store the current state code T . The presence of the connection shown by the dotted line makes it possible to consider this FSM as the Mealy machine, the absence of connection – as the Moore machine.

$$D = D(T, X). \quad (55.1)$$

$$Y = Y(T, X). \quad (55.2)$$

$$Y = Y(T). \quad (55.3)$$

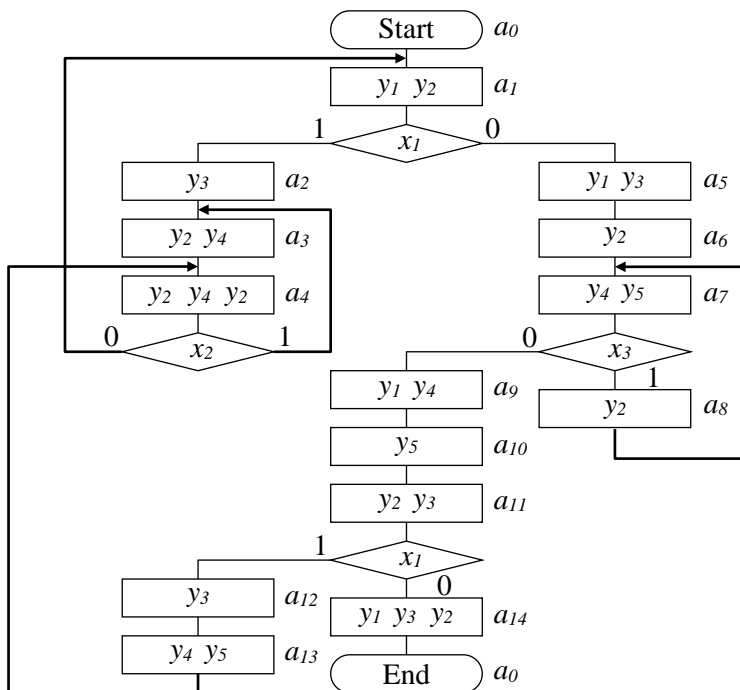


Fig. 55.1 – Graph-scheme of algorithm G

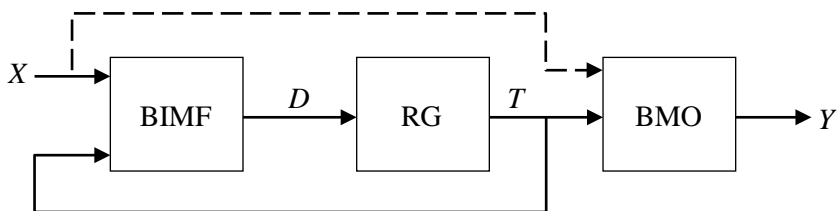


Fig. 55.2 – Finite state machine with canonical structure

The synthesis of this FSM class for a given GSA consists of the following main steps [1-3]:

- coding of states by unique binary codes;
- building a direct structural table of the FSM;
- formation of systems of Boolean equations (55.1) – (55.3);
- synthesis of an FSM circuit in a given element basis.

55.3 The IoT device control unit in the form of finite state machine with counter

The increase in the complexity of the algorithm interpreted by the FSM leads, among other things, to an increase in the number of states and microprogram transitions. The consequence of this is an increase in the number of equations and terms in the system (55.1) and the resulting increase in hardware expenses in the logical circuit of the FSM.

In [5], the so-called FSM with counter was considered, in which the memory register combines an incremental counter controlled by the *Inc* signal (see Fig. 55.3). When *Inc* = 1, the code of next state is formed by a counter and is equal to the code of previous state, incremented by one. When *Inc* = 0, the counter loads the value of the next state code from the input *D*, formed by the BIMF block in a canonical way according to the system of Boolean equations.

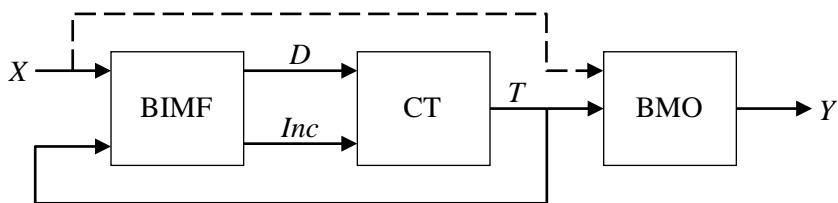


Fig. 55.3 – Structure of the FSM with counter

In the synthesis of the FSM with counter in the original GSA so-called linear sequences of states (LSS) are distinguished, between which microprogram transitions are performed using the counter [1]. In GSA in Fig. 55.1 the following LSS can be distinguished:

$\langle a_0, a_1, a_2, a_3, a_4 \rangle$, $\langle a_5, a_6, a_7, a_8, a_{10}, a_{11}, a_{12}, a_{13} \rangle$, $\langle a_{14}, a_0 \rangle$. Inside each LSS, a natural (sequential) order of state codes is used. For example, states a_0, a_1, a_2, a_3, a_4 can be encoded with binary codes 1000, 1001, 1010, 1011 and 1100.

Such coding allows using a counting circuit based on an incrementor for performing transitions within each LSS. The hardware expenses savings in an FSM with counter is achieved because the expenses for implementing the incrementor are fixed for a given digit capacity of the state code and do not depend on the number of microprogram transitions implemented using the counter. Thus, the gain in hardware expenses compared with the canonical FSM is the greater, the more transitions are implemented by the counter.

55.4 Generalizations for an FSM with counter

We can assume that the FSM with counter in each cycle of its work performs one of two operations with the current state code: an increment or a "canonical" transformation. In Fig. 55.4 the detailed representation of structure of the FSM with counter represented in Fig. 55.3 is given.

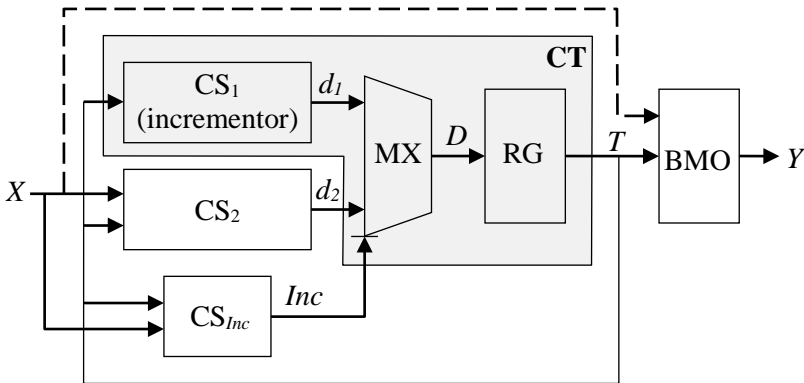


Fig. 55.4 – Detailed structure of the FSM with counter

In Fig. 55.4 combination circuit CS_1 is an R -bit incrementor and forms the result of the increment operation d_1 . The block CS_2

implements transitions between individual LSSs, is constructed according to a system of R canonical equations, and forms the result d_2 . The block CS_{inc} provides the formation of the Inc signal, which controls the multiplexer MX . At the output of MX , the code D of next FSM state is generated, which enters the memory register (block RG). The blocks CS_1 , MX and RG correspond in the structure of Fig. 55.3 block CT , blocks CS_2 and CS_{inc} correspond to the block $BIMF$.

The structure shown in Fig. 55.4 admits several generalizations:

Generalization 1. In the general case, instead of increment, another operation can be used, for example, decrement, increase by 2, bitwise shift, multiplication by a constant, a logical operation with a constant, etc. In the process of synthesizing the FSM, the method of encoding states inside linear sequences of states will change. For example, when using decrement, state codes within each LSS must be specified in decrement order.

The expediency of choosing a particular operation is determined by the following conditions:

- hardware expenses for the circuit implementation of the operation should be as low as possible and should not depend on the number of microprogram transitions implemented by this operation within the specified GSA;
- the operation should implement as many microprogram transitions as possible;
- the circuit implementation of the operation must meet the specified design requirements.

Generalization 2. In the FSM circuit, several different operations are allowed.

Let the FSM be given by GSA G (see Fig. 55.1). To encode the states in the sequence $\langle a_0, a_1, a_2, a_3, a_4 \rangle$, we will use four-digit binary codes in incremental order from 0000 to 0100, to encode the states in the sequence $\langle a_5, a_6, a_7, a_9, a_{10}, a_{11}, a_{12}, a_{13} \rangle$ we will use codes in decrement order from 1100 to 0101. For state a_{14} we will use code 1111. Obviously, the transitions in the first LSS can be implemented using the increment operation, inside the second LSS – with decrement. The transition from state a_{14} with code 1111 to state a_0 with code 0000 can be implemented using an increment operation

with discarding of carry from the high digit: $1111_2 + 1 = 0000_2$. The transition $a_4 \rightarrow a_3$ can be implemented using the decrement operation: $0100_2 - 1 = 0011_2$. Transitions $a_1 \rightarrow a_5$, $a_4 \rightarrow a_1$, $a_7 \rightarrow a_8$, $a_8 \rightarrow a_7$, $a_{11} \rightarrow a_{14}$, $a_{13} \rightarrow a_4$ are implemented in a canonical way. In this case, the state a_8 must be encoded with one of the unused codes, for example, 1110.

The FSM structure, in which increment and decrement operations are used to form microprogram transitions, is shown in Fig. 55.5. It differs from the structure in Fig. 55.4 by number of combinational circuits CS, each of which forms its own result. Also, to control the multiplexer, instead of the *Inc* signal, the *Z* signal is used, which is formed by the CS_Z block and has an R_Z digit capacity that is sufficient for multiplexing the outputs of all CS blocks (in this case, $R_Z = 2$). Thus, in the considered example, the increment operation implements 5 transitions, the decrement operation – 8 transitions and 6 transitions are implemented in the canonical way by the CS_3 block.

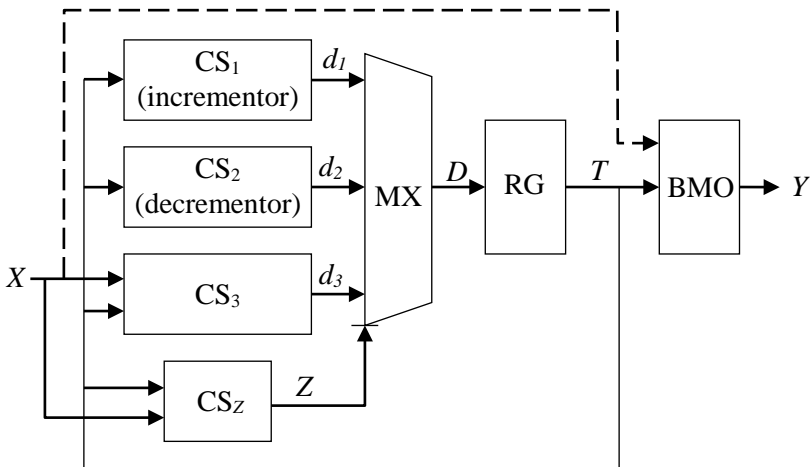


Fig. 55.5 – Structure of FSM with two operations

Block Z is synthesized in a manner similar to the block CS_{Inc} in FSM with counter according to the system of Boolean equations (55.4).

The number R_Z of equations of the system depends on the number of input directions of the multiplexer MX .

$$Z = Z(X, T). \quad (55.4)$$

The rest of the circuit in Fig. 55.5 functions in a manner similar to an FSM with counter. The presence of connection shown by the dotted line defines this structure as a Mealy machine, the absence of connection as a Moore machine. Note that the considered example does not reflect the expediency of using two operations to minimize hardware expenses, but only demonstrates the validity of the generalization 2.

Generalization 3. When choosing operations, various interpretations of state codes are permissible.

In the canonical FSM, it is customary to consider the so-called structural (binary) state codes, which are bit vectors. Each digit of the state code is formed independently of the other bits in accordance with one of the equations of the system (55.1).

When using operations such as increment or decrement, the binary code is interpreted as an unsigned integer. Such interpretation determines the order of choice of state codes inside LSS and requires the development of special methods of state coding.

In computer engineering, a bit vector allows different numerical (scalar) interpretations. Some standard ways of interpreting a bit vector are shown in Fig. 55.6. The state codes of the FSM also allow for various digital interpretations, which allows performing various arithmetic and logic operations on them. The way of interpreting binary state codes depends on the selected operations, and vice versa – the choice of operations depends on the specified method of interpretation of state codes.

With a fixed number of binary digits, each of these formats corresponds to a certain set of numbers, over which a variety of operations of different arity can be defined. In this case, any operation can receive schematic realization in most of the known element bases, often allowing for various architectural options for implementation, characterized by the cost of equipment, speed, regularity, versatility, etc.

The same microprogram transition, considered as the transformation of one binary vector into another, can be implemented with different interpretations of structural state codes. For example, suppose that an eight-bit binary code $K(a_i) = 11101011_2$ is specified for the state a_i . This code can be interpreted as an unsigned integer equal to 235_{10} , or as an integer in a sign magnitude representation, equal to -107_{SMR} , or as an integer in a two's complement format, equal to -21_{2C} .

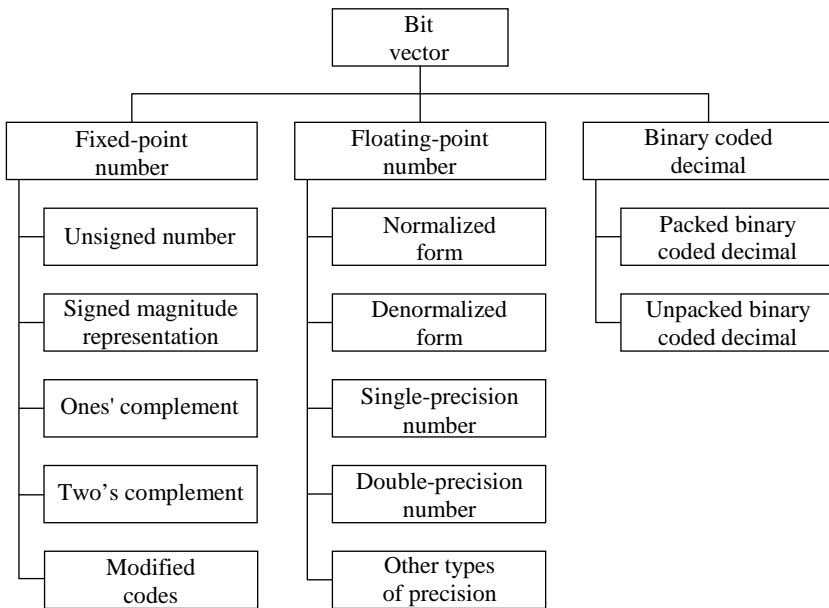


Fig. 55.6 – Some ways of numerical interpretation of the bit vector

Let the FSM performs a transition in which it is necessary to convert the state code

$$K(a_i) = 11101011_2 = 235_{10} = -107_{SMR} = -21_{2C}$$

into the code

$$K(a_j) = 00010100_2 = 20_{10} = +20_{SMR} = +20_{2C}.$$

By interpreting the bit vectors of state codes as numbers in various formats, the conversion of $K(a_i)$ into $K(a_j)$ can be performed, for example, in accordance with Fig. 55.7, where the central blocks contain the operations necessary to convert $K(a_i)$ into $K(a_j)$. In this example, all operations are performed on eight-bit binary operands with discarding of carry from the high digit. Each of these operations results in the same bit vector $K(a_j)$.

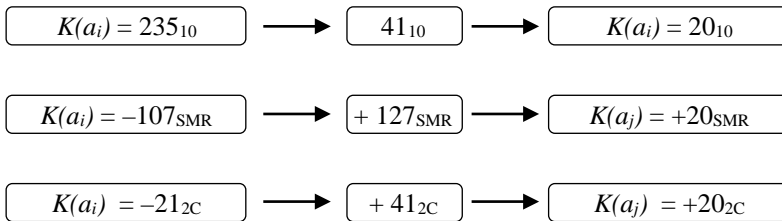


Fig. 55.7 – Equivalent bit vector conversions for its various interpretations

In Fig. 55.7, all three transformations are performed using operation of addition with a constant, but the numerical interpretation of the operands is different. In the general case, the circuit implementation of the selected operation will depend on how the state codes are interpreted.

On the other hand, with the selected interpretation of structural codes, the same transformation can be performed using various operations. So, in Fig. 55.8, several variants of the transformation of $K(a_i)$ into $K(a_j)$ for the above example when interpreting the structured state codes as numbers in the two's complement format are shown.

All operations shown in Fig. 55.7 and Fig. 55.8 allow to convert the binary vector "11101011" into the vector "00010100". Note that this transformation can also be performed using the logical bitwise inversion operation. When using this logical operation, no numerical interpretation of its operands is required.

Generalization 4. The input signals of the FSM can be used as arguments of operations.

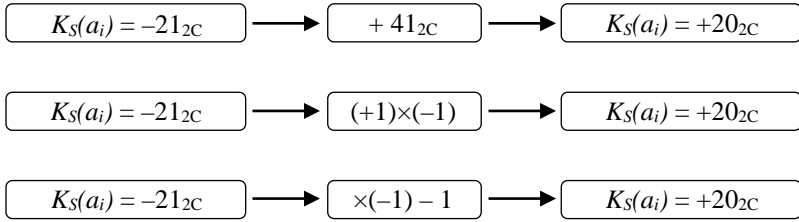


Fig. 55.8 – Equivalent bit vector conversions for "two's complement" format using various operations

In Fig. 55.9 a fragment G_1 of the previously considered GSA G shows (the contents of the operational vertices are not shown for simplicity).

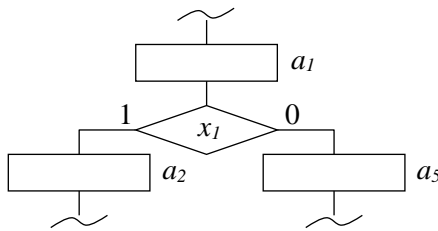


Fig. 55.9 – Fragment G_1 of the GSA G

This fragment contains two transitions from the state a_1 : transition $a_1 \rightarrow a_2$ by condition $x_1 = 1$ and transition $a_1 \rightarrow a_5$ by condition $x_1 = 0$. For any values of codes of these states, it is always possible to choose two operations for implementing these transitions. For example, if the state codes a_1 , a_2 , a_5 are equal to 0101, 0110 and 1010 accordingly, the transition $a_1 \rightarrow a_2$ can be performed using the increment operation, the transition $a_1 \rightarrow a_5$ – using the shift to the left by one digit operation.

Consider how it is possible to realize both these transition using a single operation. For example, let's choose the operation described by the expression (55.5).

$$K(a^{t+1}) = K(a^t) \cdot 2 + K(x^t). \quad (55.5)$$

Here $K(a^t)$ is the state code in the current FSM cycle t , $K(x^t)$ is the value of the logical condition checked during the transition from the state a^t , $K(a^{t+1})$ is the state code in the next cycle ($t + 1$).

Note that in expression (55.5) the value of the logical condition x^t is considered as a scalar value, which is arithmetically added to the double value of the current state code. In the case of the GSA G operation (55.5) of multiplication by 2 is implemented by shifting by 1 digit to the left, and the addition operation is based on a 4-bit adder (see Fig. 55.10). The value of the signal x_1 is added to the right digit of the first addend.

The use of an operation similar to (55.5) leads to the fact that instead of two conditional transitions, one unconditional is used, and the branching is implemented by the operation itself. This can contribute to reducing hardware expenses in the circuit of block CS_Z (see Fig. 55.5). The gain is the higher, the more times this operation is used within a given GSA.

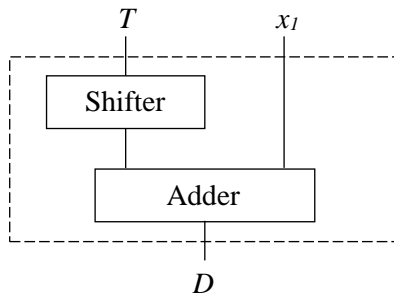


Fig. 55.10 – Schematic implementation of the operation (55.5)

It should be noted that operations similar to (55.5) can be formed for multidirectional transitions, in which more than one logical condition is analyzed. In this case, all the signals of logical conditions

in one way or another will participate in the formation of the result of the operation.

Generalization 5. In general, all transitions can be implemented in an operational way only.

The structure of the FSM with counter implies the implementation of a part of microprogram transitions in a canonical way according to the system of Boolean equations. In the structure in Fig. 55.4 this function is performed by the block CS₂. The generalizations considered above also admit such a possibility. Generalization 2 allows the use of several operations, without limiting their number. In the example made for generalization 2, the transitions $a_1 \rightarrow a_5$, $a_4 \rightarrow a_1$, $a_7 \rightarrow a_8$, $a_8 \rightarrow a_7$, $a_{11} \rightarrow a_{14}$, $a_{13} \rightarrow a_4$ are implemented in a canonical way, although each of them can be implemented using some operation. For example, for $K(a_4) = 0100$ and $K(a_1) = 0001$, a transition $a_4 \rightarrow a_1$ can be implemented using the operation of subtracting of value 0011, dividing by 4, or a logical shift to the right by two digits.

In Fig. 55.11 shows the previously considered GSA G , in which each transition is implemented by some operation and none of the transitions is implemented in a canonical way. Each GSA operational vertex contains the binary code of the corresponding state of Moore FSM, as well as its decimal equivalent. Each transition is marked by an operation that allows the corresponding conversion of state codes.

For example, the transition $a_0 \rightarrow a_1$ is the execution of an operation of division by 2 of code $K(a_0) = 0111_2 = 7$. The transition $a_3 \rightarrow a_4$ is the execution of a XOR operation of a code $K(a_3) = 1001_2$ with a binary constant 1011. The transition $a_{14} \rightarrow a_0$ is the execution of an increment operation for a code $K(a_{14}) = 0110_2 = 6_{10}$.

As we can see, all 19 transitions are implemented using three operations:

$$K(a^{t+1}) = K(a^t) \div 2; \quad (55.6)$$

$$K(a^{t+1}) = K(a^t) \oplus 1011_2; \quad (55.7)$$

$$K(a^{t+1}) = K(a^t) + 1. \quad (55.8)$$

The structure of an FSM using these operations is shown in Fig. 55.12. For each of the blocks corresponding to operations (55.6) – (55.8), the hardware expenses in its circuit do not depend on the number of implemented microprogram transitions. At the same time, there is no block in the structure responsible for implementing transitions in a canonical way.

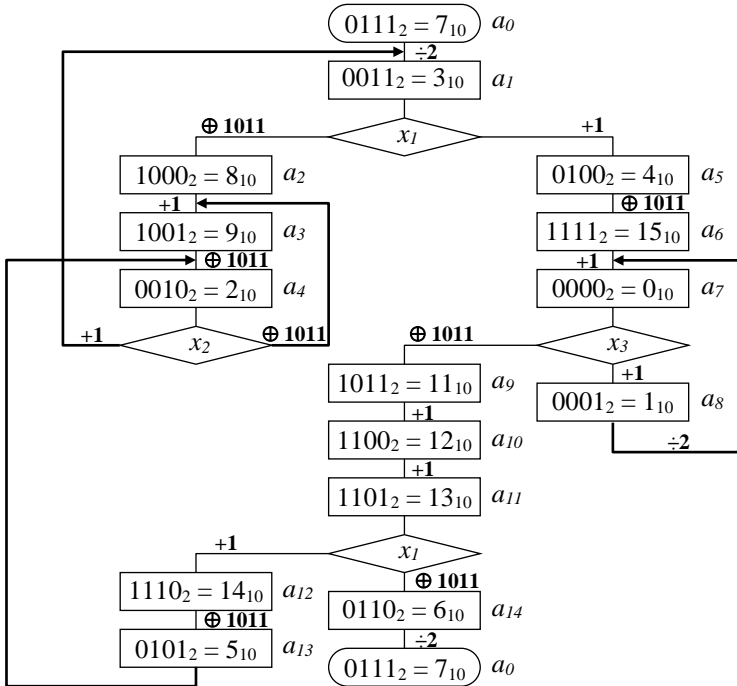


Fig. 55.11 – An example of the realization of all GSA G transitions in operational way

The implementation of all GSA transitions in an operational way considered in this example became possible due to a special selection of state codes, the selection of operations and their corresponding with microprogram transitions. It can be assumed that this choice is not the only one for this GSA and can be realized using other operations and state codes.

In accordance with [12], we will name the considered approach to the transformation of state codes in a non-canonical way using a set of arithmetic and logic operations *the principle of operational transformation of state codes*. Operations used to implement microprogram transitions we will name *transition operations (TO)*.

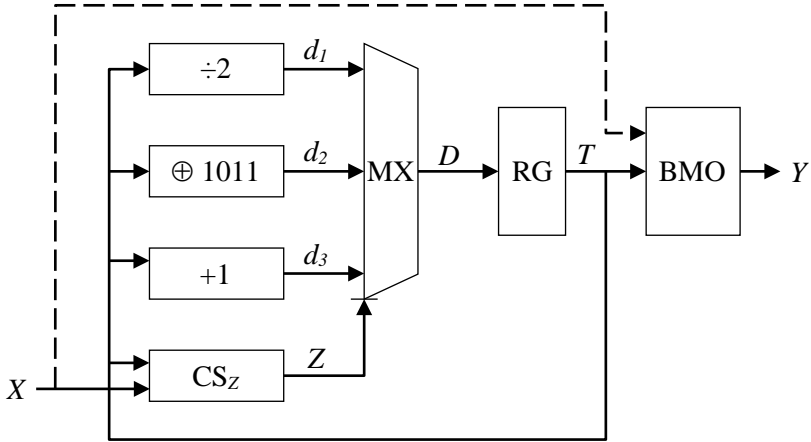


Fig. 55.12 – FSM structure for the operational implementation of all transitions of the GSA G

55.5 Datapath of transitions

Let's select in the structure shown in Fig. 55.12, fragment shown in Fig. 55.13. This fragment contains three blocks corresponding to the operations (55.6) – (55.8), the multiplexer (MX block), controlled by the signal Z , and the memory register (RG block).

Note that this fragment has a structure similar to a datapath. It contains an operational part (OP), formed by three blocks " $\div 2$ ", " $\oplus 1011$ ", " $+1$ " and the multiplexer result MX , which is controlled by external signals Z . The memory register RG acts as a register circuit for storing data. Since the function of this datapath in the FSM is the transformation of state codes, we call this datapath an datapath of transitions (DT). The general structure of the DT, including the operational part (OP block) and the memory register (RG block), is

shown in Fig. 55.14. The internal structure of the operational part in general form is shown in Fig. 55.15.

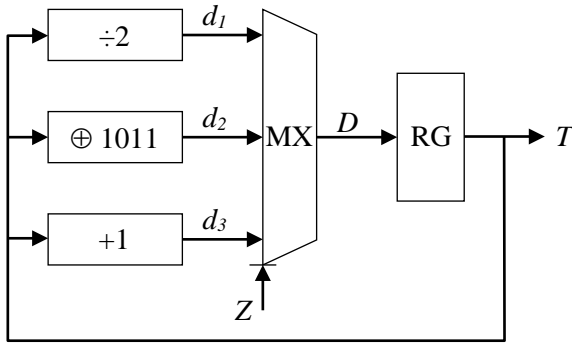


Fig. 55.13 – Fragment of FSM structure shown in Fig. 55.12

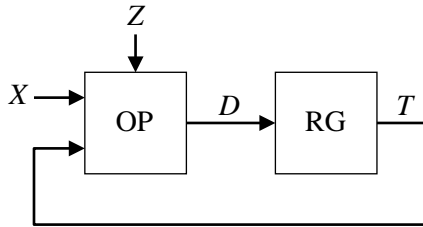


Fig. 55.14 – The structure of the datapath of transitions

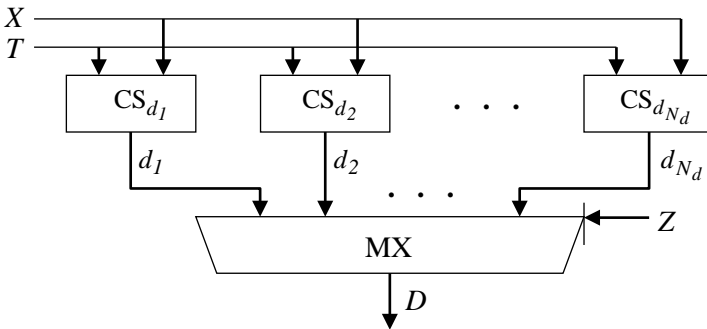


Fig. 55.15 – The generalized structure of the operational part of DT

In Fig. 5.15, blocks $CS_{d_1}, \dots, CS_{d_{N_d}}$ correspond to the N_d operations of the datapath. If part of the FSM transitions is realized in a canonical way by a system of Boolean equations, the block $CS_{d_{N_d}}$ deals with their implementation. If all transitions are implemented in an operational way, the block $CS_{d_{N_d}}$ implements one of the N_d transition operations. The result multiplexer MX generates code D of next FSM state under the control of signals Z .

In Fig. 55.16, the structure of the FSM in which the transition function is implemented on the basis of the datapath is shown.

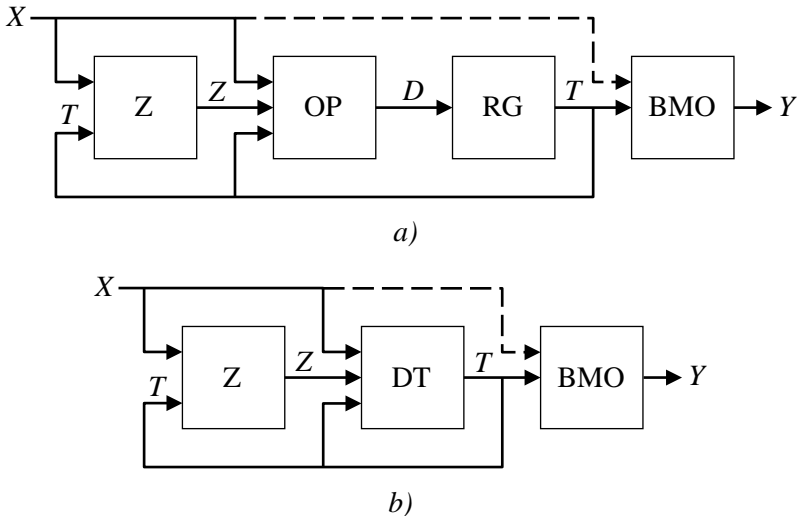


Fig. 55.16 – The structure of the FSM with datapath of transitions
 (a – datapath is shown in the form of the composition “OP + RG”,
 b – in the form of one block)

In this structure, block Z implements the system of equations (55.4) and generates the code of transition operation Z , which enters the operational part of the DT to the control inputs of the result multiplexer. DT together with block Z realize the transition function of FSM. The

block of microoperations (BMO block) implements the FSM output function. The presence of a connection shown by a dotted line defines this structure as a Mealy machine, the absence of a connection – as a Moore machine.

Thus, the difference between FSM with DT (see Fig. 55.16) and FSM with canonical structure (see Fig. 55.2) is in the way the FSM transition function is implemented. Since an FSM with DT allows the implementation of both a part and all transitions in a canonical way according to a system of Boolean equations, it can be considered as a more general structure compared to the canonical FSM and FSM with counter.

55.6 Synthesis of IoT device control unit in the form of finite state machine with datapath of transitions

55.6.1 Stages of structural synthesis of FSM with DT

The structural synthesis of FSM with DT will be understood as the synthesis of all structural blocks present in Fig. 55.16, in a given element basis. Let's formulate the necessary and sufficient conditions for the synthesis of FSM with DT:

- 1) the encoding of states of the FSM has performed using unique binary codes;
- 2) the set of transition operations is defined;
- 3) the subsets of transitions implemented by operational and canonical ways are defined;
- 4) for transitions implemented by the operational way, the necessary transformation of state codes is provided by matching required operations and FSM transitions.

Let us call the list of actions leading to the fulfillment of these conditions, *stage No. 1* of the synthesis of FSM with DT. If it is executed, the further synthesis of the FSM is the next sequence of easily formalized steps:

Stage 2. Formation of the system of Boolean equations (1) for transitions implemented in the canonical way.

Step 3. Coding of transition operations and the formation of a system of equations (4).

Stage 4. Formation of the system of Boolean equations of the output function (2) or (3).

Stage 5. Synthesis of the DT circuit based on the formed sets of transition operations and their codes.

Stage 6. Synthesis of the block Z circuit according to the results of stage 3.

Stage 7. Synthesis of the BMO circuit according to the results of stage 4.

Depending on the design conditions, one or several elements from the following list can act as the initial data of the process of synthesis of FSM with DT:

- the set of transition operations;
- state codes and their binary capacity;
- admissibility of modification of the original GSA;
- limiting restrictions on hardware expenses and design time.

The variability in the selection of source data suggests various approaches to the implementation of the first stage of structural synthesis. For example, if a set of transition operations is initially set (condition 2), then conditions 1, 3 and 4 must be fulfilled with regard to condition 2. If state codes are initially set (condition 1), then conditions 2 and 3 must be fulfilled in such a way to satisfy condition 4.

Thus, conditions 1-4, forming stage 1, cannot be considered as a sequence of actions, as a method or algorithm of synthesis. They should be considered only as a result of the first stage of the structural synthesis of FSM with DT. To obtain this result, appropriate synthesis methods should be developed, which differ in both the initial data and the quality of the result.

55.6.2 Algebraic synthesis of FSM with DT

Let us call the first stage of structural synthesis considered above, the result of which is the fulfillment of conditions (1) – (4), *the algebraic synthesis of FSM with DT*. The term “algebraic” is associated with the algebraic formalization of the FSM, given in [10], and involves the use of algebraic operations to transform state codes of the FSM. Stages 2 – 7 are called the *synthesis of the logical circuit of the FSM*. Thus, the structural synthesis of FSM with DT includes algebraic

synthesis and synthesis of the logical circuit of the FSM. It should be expected that there are many potential (not yet developed) methods for the algebraic synthesis of FSM with DT. The development and research of such methods is a separate scientific direction in the theory of finite state machines.

By the problem of algebraic synthesis of FSM with DT we will understand the problem of satisfying conditions (1) – (4), given in chapter 25.5.1. The essence of the problem is to identify and establish patterns in the transformation of binary state codes and input signals when implementing microprogram transitions.

Let, as a result of algebraic synthesis, conditions (1) – (4) are fulfilled. This means that some binary codes are associated with FSM states, and microprogram transitions associated with transition operations, as a result of which the FSM functions according to the specified control algorithm. We call the result obtained *a formal solution to the problem of the algebraic synthesis of FSM with DT*. An example of a formal solution is Fig. 55.11, reflecting the result of fulfilled conditions (1) – (4). It can be assumed that for an any FSM, in the general case, a set of formal solutions can be found.

As mentioned earlier, the purpose of developing the structure of FSM with DT is to reduce hardware expenses in the logical circuit of an FSM as compared to alternative structures. For example, the canonical FSM can act as an alternative structure (see Fig. 55.2). Suppose that on the basis of some formal solution of the problem of algebraic synthesis, a circuit of FSM with DT was designed (that is, steps 2 – 7 of structural synthesis were performed). If the hardware expenses in the resulting circuit turned out to be less than in the circuit of equivalent FSM with canonical structure, then we will call such a formal solution *an effective solution to the problem of algebraic synthesis of FSM with DT* (that is, a solution that gives at least some effect in hardware expenses reducing). In the general case, on the set of all possible formal solutions, more than one or no one effective solution of the algebraic synthesis problem can be found.

On the set of effective solutions of the problem of algebraic synthesis of FSM with DT, one or several solutions can be chosen that provide the maximum value of the economy in hardware expenses among all effective solutions. We call this solution the *optimal solution*

to the problem of the algebraic synthesis of FSM with DT. The search for optimal solutions is possible either through an exhaustive search of all possible formal solutions, or using special methods that are not currently developed.

In the general case, in the process of algebraic synthesis of FSM with DT, the formation of a set of optimal solutions is not mandatory. Also it is not necessary to form all the elements of the set of effective solutions. Nevertheless, an increase in the number of effective solutions found contributes to an increase in the effectiveness of the structural synthesis of FSM with DT, since each new solution found may turn out to be better than all the solutions found earlier.

55.6.3 Algebraic synthesis by an exhaustive search

The structure of FSM with DT, shown in Fig. 55.16, allows us to correspond the operations of transitions to individual transitions of the FSM. Let each of the M states be mapped to one of the 2^R unique binary codes of the digit capacity R , each of the B microprogram transitions is corresponded to one of the transition operations.

The number N_I of possible correspondences of 2^R binary codes to M FSM states is determined by the expression (55.9).

$$N_I = A_{2^R}^M = \frac{(2^R)!}{(2^R - M)!}. \quad (55.9)$$

The number of ways to correspond N_d transition operations to B FSM transitions is determined by the expression (55.10).

$$N_2 = (N_d)^B. \quad (55.10)$$

Then the number of variants of mutually independent correspondence of binary state codes with transition operations is determined by the expression (55.11)

$$N = N_1 \cdot N_2 = \frac{(2^R)!}{(2^R - M)!} \cdot (N_d)^B. \quad (55.11)$$

After the next variant of correspondence is chosen, it is necessary to check whether it is a formal solution of the algebraic synthesis problem. We denote by t_c the time spent on the formation of the next version of the correspondence and verification of obtaining a formal solution. Then the time t required to obtain the set of all possible formal solutions by the method of exhaustive search is determined by expression (4).

$$t = N \cdot t_c = \frac{(2^R)!}{(2^R - M)!} \cdot (N_d)^B \cdot t_c. \quad (55.12)$$

Let $t_c = 0,001$ seconds. Then the time spent on an exhaustive search of variants in the case of FSM with average complexity ($M = 50$, $R = 6$, $B = 100$) and $N_d = 10$ will be $1,45 \cdot 10^{175}$ s, which is unacceptable.

For example, in the case of $R=4$, $M=10$, $N_d=3$, $B=10$ and $t_c = 0,001$ s, the value $t = 10^{17}$ s. When reducing the value t_c to 1 ns (assuming that the search is performed on a high-performance computing system), the value of t becomes 10^{11} s, which is 3,200 years and is also unacceptable.

In expressions (55.10) – (55.12), it is assumed that the number of transition operations is fixed. In fact, it is also permissible make exhausted search for OP (for example, the choice of N_d operations from a set with power N_D , where $N_D \gg N_d$). This search will repeatedly increase the values in expressions (55.10) and (55.11), which will lead to a corresponding increase in the result of (55.12).

The above analytical expressions and the calculations performed allow us to conclude that it is practically impossible to solve the problem of algebraic synthesis of FSM with DT using the exhausted search method. The only way to find solutions is to use partial search. This requires the development of special methods and algorithms and is beyond the scope of this chapter.

55.7 Evaluation of the effectiveness of FSM with DT as IoT device control unit

The main results of research of the effectiveness of FSM with DT compared with the canonical FSM are given in [14, 15].

Let's denote the structure of an FSM with a canonical structure (see Fig. 55.2) by a symbol U_1 , the structure of an FSM with DT (see Fig. 55.16) – by a symbol U_2 . When comparing structures, we will regard the efficiency criterion as hardware expenses for the implementation of the FSM logical circuit. The effectiveness E^{U_2} of the structure U_2 is defined by the following expression:

$$E^{U_2} = H^{U_1} / H^{U_2}, \quad (55.13)$$

where H^{U_1} , H^{U_2} are numerically expressed hardware expenses in FSM with canonical structure and in equivalent FSM with DT. The structure U_2 is more efficient than the structure U_1 in the case of $E^{U_2} > 1$, and the savings in hardware expenses is equal to $(E^{U_2} - 1) / E^{U_2}$ percentage of expenses in the canonical structure. If $E^{U_2} = 1$ then compared structures are equivalent in terms of hardware expenses. If $E^{U_2} < 1$ then the structure U_2 is less effective than the structure U_1 , and its use in terms of hardware expenses is impractical.

Each of the values H^{U_1} and H^{U_2} is the sum of the numerically expressed hardware expenses in all blocks of the corresponding structure. The value H^{U_1} is determined by the expression (55.14), the value H^{U_2} is determined by the expression (55.15).

$$H^{U_1} = H_{\text{BIMF}}^{U_1} + H_{\text{RG}}^{U_1} + H_{\text{BMO}}^{U_1}; \quad (55.14)$$

$$H^{U_2} = H_{\text{Z}}^{U_2} + H_{\text{DT}}^{U_2} + H_{\text{BMO}}^{U_2}. \quad (55.15)$$

Separate blocks in these structures have an internal architecture similar to typical functional units, such as combinational circuit, register, multiplexer, memory module, adder, shifter and others. For example, in the canonical FSM, the BIMF and BMO blocks are implemented according to the system of Boolean equations in the form of a combinational circuit, and the RG block is a standard R -bit register. An exception may be the nodes in the datapath of transitions that implement non-standard operations. However, in most cases, splitting such units into simpler ones does not cause difficulties. This makes it possible to compare hardware expenses in these structures not for structural blocks, but for the corresponding functional units, applying the obtained results to structural blocks.

In the works [14, 15], the analysis of hardware expenses was carried out by VHDL simulation using CAD Xilinx ISE [16, 17]. LUT-elements (Look-Up Tables), which are regular FPGAs basis, are selected as the unit of measurement for hardware expenses. In order to save LUT elements, it is allowed to use the FPGA block memory (if the architecture of the synthesized block allows it) [18, 19].

The simulation results allowed us to obtain approximated analytical expressions for determining the hardware expenses H^{U_1} and H^{U_2} depending on a number of FSM parameters [12]. On the basis of analytical expressions, in [14, 15] it was shown that the average efficiency of an FSM with DT compared to canonical FSM is 1.1 – 1.2, which corresponds to a reducing in hardware expenses equal to 10-15%. An additional reducing is possible due to the use of a number of well-known methods for minimizing hardware expenses in the FSM circuit considered in [5 – 11].

55.8 Integration of FSM with DT into IoT device

The control unit can control both the entire IoT device and its individual module. From this point of view, the control unit and the object of control can be considered as a single operational device designed to process information in accordance with a given algorithm (see Fig. 55.17) [5, 6].

The initial data for building a control unit is a control algorithm. The logical circuit of FSM with DT is designed in accordance with the

stages of structural synthesis, considered in chapter 55.6.1. The control unit analyzes a set of signals of logical conditions X , coming from the object of control, and forms a set of microoperations Y , entering the object of control.

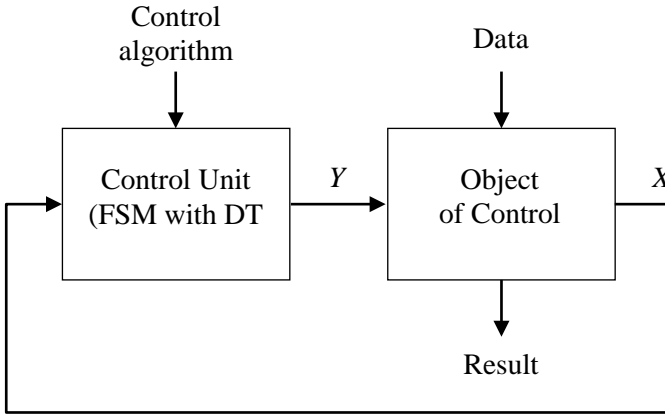


Fig. 55.17 – The structure of the operational device equivalent to an IoT device or its module

The object of control receives from the external environment some data and performs their processing using a variety of microoperations. A microoperation (an elementary action on data) that is performed in the current device clock cycle is determined by a set of signals Y , coming from the control unit. At the output of the object of control, the result of the operation and the signals of the logical conditions X are generated, which signal special situations during the execution of a microoperation.

The structure of the operational device shown in Fig. 55.17, represents the most general concept of building a digital system. The specific design of the IoT device control unit in the FPGA-type basis is a synthesizable code in the VHDL or Verilog language, which can be combined with the object of control code [16, 17].

55.9. Work related analysis

The design of the hardware components of IoT devices is closely related to such a scientific area as the design and optimization of digital devices. A lot of EU universities including ALIOT project partners conduct research and implement education MSc and PhD programs in this and related domains. In particular, the following courses and programs can be distinguished:

- Coimbra University, Portugal:
 - a) Master program in Electrical and Computer Engineering [20],
 - b) Doctoral Program in Electrical and Computer Engineering [21],
 - c) Programmable Electronic Devices (PhD Course) [22].
- KTH University, Sweden:
 - a) Master's programme in Systems, Control and Robotics [23],
 - b) Control Theory and Practice, Advanced Course [24],
 - c) Sensor Based Systems [25],
 - d) Hybrid and Embedded Control Systems [26].
- Newcastle University, United Kingdom:
 - a) Computer Science Integrated PhD [27],
 - b) Embedded Systems and Internet of Things (ES-IoT) MSc [28],
 - c) Microelectronics: Systems and Devices MSc [29],
 - d) Electrical and Electronic Engineering PhD [30].

Conclusion and questions

In this section, a concept of building IoT devices control units based on a finite state machine with optimized hardware expenses has been considered. Its essence lies in the fact that the transformation of state codes is possible both in a canonical way in accordance with a system of Boolean equations and in a non-canonical way using arithmetical and logical operations (transition operations). The use of such transition operations, the hardware expenses in the logical circuit of which do not depend or depend slightly on the number of transitions implemented by the operation, can help reduce hardware expenses in the FSM circuit compared to the implementation of the FSM transition function in a canonical way.

Splitting a set of FSM transitions into subsets is equivalent to representing transition function in the form of several partial functions. An example of the representation of the transition function in the form of two partial functions is the FSM with counter, in which part of the transitions is implemented by incrementor, and other part implemented in canonical way.

The main problem in this direction is the development of highly efficient methods that allow one to obtain solutions of the problem of algebraic synthesis of FSM with DT that are close to optimal. Also the following scientific and technical problems remain unresolved today:

- Use in FSM with DT known methods for circuit optimizing.
- Using the features of the elemental basis of FPGA in FSM with DT designing.
- The use of datapath of transitions in other classes of control devices.

These and other tasks form independent directions in the FSM theory and require separate research. Application of the described techniques for IoT devices of industrial systems such as [11] allows minimizing their complexity, power consumption, reliability.

The development and research of control devices based on finite state machine with datapath of transitions require an understanding of the following issues addressed in this chapter:

1. What is the function of the digital system control unit?
2. What are the most well-known classes of control units?
3. What are the advantages and disadvantages of a finite state machine?
4. How organized the FSM with a canonical structure?
5. What is the advantage of the FSM with counter?
6. What generalizations are allowed for the FSM with counter?
7. What is the principle of operational transformation of state codes?
8. What are the function and the internal structure of the datapath of transitions?
9. How does an FSM with datapath of transitions differ from an FSM with a canonical structure?
10. What are the main stages of the structural synthesis of FSM with DT?

11. What is the problem of algebraic synthesis of FSM with DT? What is its formal solution?

12. What can serve as the initial data of the algebraic synthesis of FSM with DT?

13. Is it possible to perform the algebraic synthesis of FSM with DT using the exhausted search method?

14. What is the effectiveness of the FSM with DT structure in comparison with the canonical FSM by the HW expenses criterion?

15. What are the actual scientific and technical problems in FSM with DT design?

16. Please analyse HW components for IoT industrial systems produced by [11] or originot.com and suggest ways to improve their characteristics by use of the techniques described in this section.

For a better understanding of the process of algebraic synthesis, the following exercises on the GSA G (see Fig. 55.1) are proposed:

1. Implement all the transitions in the operational way (like Fig. 55.11) under the following condition: it is allowed to use no more than three transition operations other than the operations in Fig. 55.11.

2. Implement all the transitions in an operational way under the following condition: it is allowed to use no more than three transition operations, one of which is the decrement operation.

3. Implement all transitions in an operational way under the following condition: it is allowed to use any transition operations, but no more than two.

4. Implement as many transitions as possible in an operational way under the following condition: state codes are given and equal to state indices recorded in four-digit binary form. The number of transition operations is no more than three.

5. Perform exercises 1-4 for other GSAs of similar complexity.

References

1. A. Gerber, "Choosing the best hardware for your next IoT project ", [Online]. Available: <https://developer.ibm.com/articles/iot-1p101-best-hardware-devices-iot-project/>.
2. J. Eller, "The Control System: An IoT Device's Brain", [Online]. Available: <https://dzone.com/articles/the-control-system-an-iot-devices->

- brain.
3. A. Mutschler, "Designing For Ultra-Low-Power IoT Devices", [Online]. Available: <https://semiengineering.com/designing-for-ultra-low-power-iot-devices/>.
 4. K. Chauhan, "4 Reasons to Use Custom ASICs in the IoT Era", [Online]. Available: <https://dzone.com/articles/4-reasons-to-utilize-custom-asics-in-the-iot-era>.
 5. Barkalov A., Titarenko L., "Logic Synthesis for FSM-Based Control Units", Berlin: Springer, 2009.
 6. Baranov S., "Logic Synthesis for Control Automata", Boston: Kluwer Academic Publishers, 1994.
 7. Czerwinski R., Kania D., "Finite State Machine Logic Synthesis for Complex Programmable Logic Devices", Berlin: Springer, 2013.
 8. Barkalov A., Wegrzyn M., "Design of Control Units with Programmable Logic", Zielona Gora: University of Zielona Gora Press, 2006.
 9. Barkalov A., Titerenko L., "Logic Synthesis for Compositional Microprogram Control Units", Berlin: Springer, 2008.
 10. Czerwinski R., Kania D., "Finite State Machine Logic Synthesis for Complex Programmable Logic Devices", Berlin: Springer, 2013.
 11. IoT Snapshot, 2018, www.m.iotone.com.
 12. A. Barkalov, R. Babakov, "Operational Formation of State Codes in Microprogram Automata", *Cybernetics and Systems Analysis*, Volume 47, Issue 2, p. 193-197, 2011.
 13. A. Barkalov, R. Babakov, "Algebraic Interpretation of a Microprogram Finite-State Machine with Datapath of Transitions", *Cybernetics and Systems Analysis*, Volume 52, Issue 2, p. 191-198, 2016.
 14. Babakov R., Barkalov A. and Titarenko L., "Research of Efficiency of Microprogram Final-State Machine with Datapath of Transitions", in *Proceedings of 14th International Conference "The Experience of Designing and Application of CAD Systems in Microelectronics (CADSM'2017)*, 2017.
 15. A. Barkalov, R. Babakov, "Determining the Area of Efficient Application of a Microprogrammed Finite-State Machine with Datapath of Transitions", *Cybernetics and Systems Analysis*, Volume 54, Issue 3, p. 366-375, 2018.
 16. Brown S., Vranesic Z., "Fundamentals of Digital Logic with VHDL Design", 3rd Ed. New York: McGraw Hill, 2000.

17. Minns P., Elliot I., "FSM-Based Digital Design Using Verilog HDL", New Jersey: J. Wiley & Sons, 2008.
18. Cong J., Yan K., "Synthesis for FPGAs with embedded memory blocks", in *Proceedings of the 2000 ACM/SIGDA 8th International Symposium on FPGAs*, 2000.
19. Tiwari A., Tomko K., "Saving power by mapping finite-state machines into embedded memory blocks in FPGAs", in *Proceedings of the Conference on Design, Automation and Test in Europe*, 2004.
20. The Master program in Electrical and Computer Engineering [<https://www.uc.pt/en/fctuc/deec/courses/mieec>].
21. The Doctoral Program in Electrical and Computer Engineering [<https://www.uc.pt/en/fctuc/deec/courses/phd>].
22. Programmable Electronic Devices [https://www.uc.pt/fctuc/deec/PhD_courses/Programmable_Electronic_Devices].
23. Master's programme in Systems, Control and Robotics [<https://www.kth.se/en/studies/master/systems-control-robotics>].
24. Control Theory and Practice, Advanced Course [<https://www.kth.se/student/kurser/kurs/EL2520?l=en>].
25. Sensor Based Systems [<https://www.kth.se/student/kurser/kurs/II2302?l=en>].
26. Hybrid and Embedded Control Systems [<https://www.kth.se/student/kurser/kurs/EL2450?l=en>].
27. Computer Science Integrated PhD [<https://www.ncl.ac.uk/postgraduate/courses/degrees/computer-science-integrated-phd/#profile>].
28. Embedded Systems and Internet of Things (ES-IoT) MSc [<https://www.ncl.ac.uk/postgraduate/courses/degrees/embedded-systems-internet-of-things-msc/#profile>].
29. Microelectronics: Systems and Devices MSc [<https://www.ncl.ac.uk/postgraduate/courses/degrees/microelectronics-systems-devices-msc/#profile>].
30. Electrical and Electronic Engineering PhD [<https://www.ncl.ac.uk/postgraduate/courses/degrees/electrical-electronic-engineering-phd/#profile>].

56. INDUSTRY 4.0/5.0 AND INDUSTRIAL INTERNET OF THINGS

O. V. Yurchak (APPAU), Prof., DrS V. S. Kharchenko,
Dr O. O. Illiashenko, Assoc. Prof., Dr M. O. Kolisnyk,
Dr Ye. V. Babeshko (KhAI), Prof., DrS S. I. Dotsenko (USURT)

Contents

Abbreviations	867
56.1. Association of Industrial Automation of Ukraine as a driver of Industry 4.0.....	868
56.2. The possibilities of Ukraine in context of Industry 4.0	869
56.3. Strategy and directions of Industry 4.0.....	872
56.3.1 National strategy 4.0.....	872
56.3.2. National movement “Industry 4.0 in Ukraine”.....	874
56.3.3. The technologies and landscape Industry 4.0 in Ukraine .	880
56.4Trends in Industry 4.0 and Industrial Internet of Things.....	883
56.4.1 Gartner top 10 strategical technology trends in 2019.....	883
56.4.2 Integrated enterprise safety and security management systems for Industry 4.0	890
56.5 Industry 5.0 and Internet of Things	893
56.5.1 Stages of Industry X.0.....	893
56.5.2 Future of Internet of Things	895
56.6 Work related analysis	896
Conclusions and questions	897
References	899

Abbreviations

AI – Artificial Intelligence

APPAU – Association of Industrial Automation of Ukraine

EAM – Engineering, Automation, Machinery

ERP - Enterprise Resource Planning

FSM – Functional Safety Management

I&C – Instrumentation and Control

IIoT – Industrial IoT

ISM – Information Security Management

M2M – Machine to Machine

MES - Manufacturing Execution System

PSM – Physical Security Management

R&D – Research and Development

TC – Technical Committee

56.1. Association of Industrial Automation of Ukraine as a driver of Industry 4.0

Association of Industrial Automation of Ukraine (APPAU), was created in 2011 [1] <https://appau.org.ua/en/>. Association has the mission of development of the local market through set-up of professional standards in technical field and in business development. It represents the interests of the Ukrainian industrial automation community. Main activities and tasks of the Association are the following:

- harmonization and promotion of international standards (IEC/ISO) in the field of industrial automation and IT;
- consolidation and development of expert groups;
- improving dialogue between different groups of stakeholders (including researchers and lecturers of universities);
- providing industry insights, outline critical development problems and suggest appropriate solutions;
- set up and provide new services for community members and partners, including promotion and export;
- developing hi-tech communities and eco-systems in cluster-like approach;
- moving innovations in line with developing countries.

The Association functions as a non-government and non-profit organization uniting legal entities. General Assembly of members is the highest body of the Association. It appoints the Management Board, which, in turn, appoints the General Director of the Association. Budget of Association is formed of membership fees, grants and sponsors donations. APPAU Association includes 7 categories of members:

- manufacturers of industrial automation products (big global brands like Siemens, ABB, Schneider Electric and others, and also local manufacturers like Mikrol, Oven and Novatek-Electro);
- local control system integrators and engineering companies;
- IT companies and IT integrators;
- machine-building enterprises;
- big industrial end users;
- universities;
- third party partners and services provides.

The Association also closely cooperates with government body in the development of innovation, export and industrial policies in Ukraine. In 2016 Association was the member of pro-government Program «Digital Agenda Ukraine» where it developed and its part, initiative for Smart Factory/ Industry 4.0. In 2017 Association created its own Technical Committee 185 (TC 185) which report to National Entity of Standardization. The tasks of TC 185 are about speed-up the process of harmonization technical standards in Industrial Automation.

In 2016 Association of Industrial Automation of Ukraine (APPAU) together with Association of Innovation Development of Ukraine formed a national movement “Industry 4.0 in Ukraine” [2] <https://industry4-0-ukraine.com.ua/> that unites today more than 80 members. The movement was positioned as the common platform for all hi-tech segments. The mission of the movement is to promote and educate the local market in 4.0 technologies:

- IoT,
- Big Data,
- AI,
- robotics,
- additive manufacturing,
- VR/AR.

Association of Industrial Automation of Ukraine is a driver of development and implementation of conception and technologies Industry 4.0 including application of industrial IoT. This section has been prepared by experts of Association of Industrial Automation of Ukraine and Kharkiv Region Centre Industry 4.0 based on KhAI and Department of computer systems, networks and cyber security as part of APPAU community.

56.2. The possibilities of Ukraine in context of Industry 4.0

1. Opportunities in hi-tech segments already exist for our internal and external stakeholders. Ukraine’s technical education is the foundation of Ukraine’s hi-tech ecosystem and this is true for all hi-tech sectors. Every year the country graduates over 150,000 students, among which 36,000 are with degrees in technical studies, including some 15,000 IT specialists.

That is the main reason why our IT-industry is so strong and fast growing. Ukrainian workforce of 90,000 IT professionals is a direct consequence of IT industry being the first in using this basis of any hi-tech ecosystem.

These numbers are the highest in Central and Eastern Europe. It's absolutely clear that current capacities of our Education System significantly exceeds demand of local market. Ukraine continues to be a donor of well educated young people for wealthier countries. This is the price for having non-effective governments during two decades.

But by taking a more pragmatic approach, it's easy to conclude that this creates great opportunities for international companies searching for young talents, as well as for neighboring European countries. Poland was the first who took advantage of this situation, launching large plans of engaging Ukrainian students into their schools. It's known that only 30% of these students return home.

2. High-tech industry. Ukraine is well known in Europe for qualified, affordable and available IT staff. With about 150000 IT-developers today ranks as no.1 IT destination in Eastern Europe. There are industrial high-tech solutions in aerospace, aviation, energy, defense and other branches. There is huge potential from various sectors of IT and innovators across Ukraine.

Ukraine ranks in top 8 countries worldwide able to ensure complete cycle of aerospace manufacturing. It is in top 5 world producers of tanks, and it has also strong position in manufacturing of heavy industry and power equipment, complex engineering and turn key projects, high sophisticated and safety critical Instrumentation and Control systems for Nuclear Power Plants and other sectors.

3. Excellent ratio of quality/price of workforce. The second reason of Ukraine's attractiveness for global value chains is, of course, excellent ratio of quality/price of workforce. We know that following hryvnia's dramatic fall against the dollar in 2014-2015 Ukraine became one of the cheapest countries to live and operate a business in.

Salaries of IT professionals start at \$400/month, QA specialists at \$300/month, while those of project managers may be above 1,000/month. When you go to other hi-tech sectors, less globalized compared with IT, it will be even less.

Table 56.1 – The report of Ukrainian IT-industry [3]

	Ukraine	Poland	Czech Republic	Bulgaria	Belarus	Slovakia
Labor force	22m	18.5m	5.3m	2.5m	4.5m	2.7m
Ease of doing business* (out of 189 countries)	83	25	36	38	44	29
Ease of starting a business** (out of 189 countries)	30	85	93	52	12	68
Living Costs*** (New York = 100)	19	25	27	21	29	29
English Proficiency****	Moderate	very high	high	n/a	n/a	moderate

4. R&D and production centers in Ukraine. The next reason is more geopolitical. After a final turn towards Europe and continuous sanctions against Russia many analysts say that it is more promising to set-up R&D and production centers in Ukraine compared with other countries in the region.

Many global brands have already determined that, and that is why we have more than 100 R&D centers here.

Let's consider a new challenge everybody talks here – cyber-security. Ukraine is #1 target for Russian hackers, but the country is first as well to define the right set of measures on coping with this new threat.

The recent Global Cyber Security Summit 2017 (held in Kyiv on the 14-15th of June 2017, [4]) with strong leadership from US experts is a good sign that the world understands this.

5. Speed and flexibility. A high activity of many professional communities and their creativity. Surviving 2 revolutions in 10 years Ukrainians know how to quickly adapt to new situations in a rapidly changing world. Many IT, OEM and industrial manufacturers lost

export to Russia. It was dramatic drop for many of them. Many companies closed but others survived and became even stronger.

If to analyse IT & Industrial Automation companies, you will notice that they are very flexible, adaptive, ambitious and with good English proficiency. So, speed and flexibility are self-sufficient values in modern world and Ukrainians demonstrates their abilities in that.

Finally, our Association is also a good example, we're the first to push the government and challenge other industries & communities with 4.0 issues, and with combining our initiatives in the 4.0 national movement.

6. State of manufacturing facilities. Last but not least, poor state of many Ukrainian manufacturing facilities create good opportunities for western capital. Many workshops, territories and even plants are cheap to buy and deploy your own manufacturing.

Last month, for example, Dutch Banke Electromotive has very fast started its manufacturing in Lviv (Western Ukraine). Rasmus Banke, CEO said that they looked through many countries in Eastern Europe but finally stopped on Ukraine.

To finalize, when we talk about 'Ukraine 4.0', we do not have ambitions to be on the same level as US, Germany or China during a few years. However, Ukraine has an impressive workforce of qualified developers and our target is to double this number by 2020 in many sectors – including industrial hi-tech.

So, the right positioning for Ukraine now would be to find its niches and to integrate into global value chains.

56.3. Strategy and directions of Industry 4.0

56.3.1 National strategy 4.0

The national strategy Industry 4.0 has been developed on December 2018 by APPAU's expert with support of OBSE [5] https://www.slideshare.net/APPAU_Ukraine/strategy-industry-4-0-of-ukraine-201921-overview. The strategy includes 13 projects and set of tasks of policy synchronization with the Government. This synchronization and harmonization is primary and urgent challenge of industrial hi-tech stakeholders as today no strategy (industrial manufacturing, innovation, export, cluster) is valid and acts in Ukraine.

The 13 mentioned projects are breakdown by 6 directions including as shown on the Figure 56.1.

The most prioritized projects where APPAU looks for donors and partners concerns of 6 main directions:

1. The audit of innovative potential, at the regional and industry level.
2. Creation of industry roadmap of digital transformation (2 sectors are in focus, Food and Machinery)
3. Fostering of innovative ecosystem at the base of network of regional Center 4.0 as well as creation of regional EAM clusters (**E**ngineering, **A**utomation, **M**achinery)
4. Development of export potential / creation of trade mission to support cluster and 4.0 developers
5. Standardization / the large implementation of new standards IEC/ISO compatible with RAMI model of Industry 4.0. The focus has to be made on standards relevant to cyber-security and safety.
6. Collaboration with EU: improving our visibility and funding.



Fig. 56.1 – Directions of the strategy

Vision till 2030 Ukraine is hi-tech, post-industrial country, that is integrated into global values chains and able to produce unique and high quality engineering products and services.

For own needs, Ukraine is self-sufficient to ensure its army and its economics by the most needed technologies. Main objectives are the following:

1. Growth of manufacturing 10% per year that gives growth in GDP from 12% (2017 p.) to 20 % (2022 p.).

2. Faster growth of industrial engineering sectors, 10- 20% per year.

3. Capital attraction into local 4.0 capacities: production, Center R&D, incubators and SMBs.

Directions of development in 2019-2022 years are the following:

1. Synchronization with Industrial and Innovation Strategies at the State level.

2. Creation of innovative ecosystem for industrial engineering sectors.

3. Speed-up of clustering processes in 4.0 at regional as well at the national levels.
4. Full-scale digitization of key sectors in manufacturing, energy and Utilities sectors.

5. Integration of technologies 4.0 into Defense strategies.

6. Launch of export programs for industrial engineering.

7. Integration into EU and WW environment of 4.0.

In 2018, this strategy has yet not been validated by Cabinet of Minister of Ukraine. APPAU and partners started the realization of it by own resources. See more information about current status on [6] <https://appau.org.ua/en/pubs/current-status-of-industry-4-0-projects/>.

56.3.2. National movement “Industry 4.0 in Ukraine”

In July 2016 first 18 companies joined to national movement ‘Industry 4.0 in Ukraine’ [1]. They included the subsidiaries of worldwide companies as Microsoft, ABB, big local industrial End Users and local system integrators.

Today the movement includes 100+ members and it is still non government initiative managed by APPAU. The main statements of

movement are fixed in the Chapter “Industry 4.0 in Ukraine”. They are as follows:

- Ukraine should remain and grow its position as hi-tech developed country;
- IT-industry is recognized as leaders in term of technologies as well as business practices;
- it should be much better integration into worldwide & EU movements, as examples it cited the German Industries 4.0 and US Industrial Internet Consortium;
- market education and development of digital transformation road map per industry is fixed up as main priorities in short term period.

The Industry 4.0 directions and activities for 2019 are described by Table 56.2.

Table 56.2 – Industry 4.0 directions and activities for 2019

N	Directions 2019	Short description	Current status	Already launched actions and initiatives	Help and opportunities for donors
1.	Audit of innovative ecosystem of industrial hi-tech (including Universities, Academy, R&D centers, parks)	Professional study of infrastructure of industrial ecosystems Target are to define current status, attractiveness, competitiveness and abilities to progress in I4-0: all that is	1) Meeting with Ministry of Education and Science regarding of possibilities of integration in their projects 2) Meeting and negotiations with donors regarding status of ecosystems in Food and	APPAU launched own on-line survey «Landscape 4.0» (it is update of innovator’s map from 2017). In May it was finalized into v2.0 Landscape. The complete guide is planned on July.	The financing can be breakdown with regard to existing projects of different stakeholders. The issue of 1st catalogue and guide about innovators 4.0 can be also 1st

		important for investors and other stakeholders.	Machinery 3) Center of TT and 4.0 from Kharkiv try to join efforts in audit of local ecosystem.		step in export activities.
2.	Development of innovative ecosystems and clusters in regions	The launch in 5 regions of network Center 4.0 on the base of chosen tech. Universities. The launch of EAM cluster in the same regions.	1) APPAU started creation of network Center 4.0 in 2018, 2 centers have created in Odessa and Kharkiv. In 2019 APPAU tries to extend the network and to integrate these Centers into EU Digital Innovation Hubs 2) The concept of clusters EAM (Engineering, Automation, Machinery) IAM is prepared and validated in Strategist 4.0	1) New Center is opened in Kyiv, yet to are planned to be open in Sumy and Zaporizhzhia 2) Memorandum about EAM cluster creation are signed with partners in Sumy and Zaporizhzhya.	The same as above. Financing 1 pilot in 1 region, than others.

			community 3) APPAU proposed to Ministry of economic development to integrate these initiative into their Smart specializatio n project.		
3.	Export developm ent in Industry 4.0 and EAM clusters IAM	The launch of trade mission for participants of Industry 4.0 movement and EAM clusters.	1) APPAU has already a part of 2 WG in EPO project. The problem is that IT-strategy is far from Industrial issues, when Machin-builders are as well far from digitization. 2) APPAU prepared for EPO the separate offer called Smart Export	1) APPAU pushes a lot local developers for integration into global value chain. 2) Meeting with new direction of EPO to consider opportunity for Industry 4.0	Export strategy for EAM clusters can be a separate chapter in new EPO strategy.
4.	Creation of industries	Creation of roadmap DT at the	APPAU has already prepared 8-	APPAU experts prepared own	We invest into Agri-Food

	roadmaps of digital transformation	level of leading enterprises and industries are well known tool to speed-up the progress in 4.0. The project is aimed to create and scale-up the mechanism of fast dissemination of best methods and also preparing the network of experts in such area.	month project FOOD DT that integrates 3 parts – a) creation of 30+ business cases for FOOD segments, б) Launch of FOOD landscape 4.0 and innovation forum 3) creation with FOOD experts of roadmap DT.	policy paper of roadmap DT for Railway. The presentation is done in March. In May 2019, we launched the new and full scale project for Agri-Food. https://agri-food.appau.org.ua/	around 100-150 k Hryvna. The needed budget is 900+ k Hryvna.
5.	Standardization	There 2 key program here: 1) defense of cyber attack and functional safety of critical infrastructure 2) speed-up of transition to	Just few exchanges with Ministry of Economic development .	APPAU supports group of expert in Technical Committee 185 'Industrial Automation'. The issue #1 is low motivation of experts and low speed of works. In July 2019 APPAU	APPAU look for any support in this area to increase experts motivation and enrich common experience.

		international standards as the set of GOST cancellation. APPAU try harmonize Ukrainian legislation of standards as IEC 62512, 62264, 62443, 61508, ISO 27001 and others.		had reached agreement with GIZ and has launched its 1 st project in this area aCampus.	
6.	Collaboration with EU networks and funds in Industry 4.0	Improving coordination and integration into EU structures of Industry 4.0 (such as I4MS, Horizon 2020, Factories of the Future, EaP Plus and so on) by establishing the special coordinator position.	There are many exchanges but there is no right coordination / communication / engagement of local SMB into such programs.	APPAU nominates 1 person responsible for H2020 and other funds. There are also 5 consultants with experience in H2020/COSME and other relative field.	SMBs need series of training and seminars about access and integration into EU structures relative to I4-0.

56.3.3. The technologies and landscape Industry 4.0 in Ukraine

Transition from Industry 3.0 to 4.0 is based on development and implementation of a set of the following technologies (Fig. 56.2) [7] <https://industry4-0-ukraine.com.ua/2019/03/03/positioning-of-innovators-4-0-why-and-how/> For Industry 3.0 set of the technologies is the following (marked by red color): Robotics, Systems ERP, MES/APS/APC, SCADA/HMI, Automatization (Instrumentation and Control), Audit and supervising, Data storages, Mobile technologies, Industry networks, Cloud computing.



Fig. 56.2 – Technologies of Industry 3.0 and 4.0

Industry 4.0 is based on the additional technologies such as (marked by green color): IIoT platforms, Smart sensors, Collaborative robotics, 3D/4d printing, Artificial intelligence, Cyber security and

safety, Virtual an augmented reality, Real-time location services, Wearable technologies, Drones.

Ukrainian Landscape Industry 4.0 for technologies and application is presented on Figures 56.3 and 56.4 correspondingly [8,9] <https://industry4-0-ukraine.com.ua/>



Fig. 56.3 – Ukrainian landscape Industry 4.0 technologies (ver. 2.0)

There are a lot of different types of landscapes. For example, landscape of Digital Twin IIoT technologies for Industry 4.0 implemented by company Alleantia [10] <https://www.alleantia.com/company/> is shown on Fig. 56.5. This company provides Application Ecosystem IIoT Apps.

56. Industry 4.0/5.0 and Industrial Internet of Things



Fig. 56.4 – Ukrainian landscape Industry 4.0 application (ver. 2.0)



Fig. 56.5 – Landscape of Digital Twin IIoT technologies for Industry 4.0 implemented by Alleantia

56.4 Trends in Industry 4.0 and Industrial Internet of Things

56.4.1 Gartner top 10 strategic technology trends in 2019

Top 10 strategic technology trends in 2019 have been presented by Gartner company [11] <https://www.gartner.com/en/doc/383829-top-10-strategic-technology-trends-for-2019-a-gartner-trend-insight-report>.

Gartner Distinguished Vice President Analyst David Cearley said at Gartner 2018 Symposium/ITxpo (<https://www.gartner.com/en/conferences/na/symposium-us> Orlando, Florida, USA):

“The future will be characterized by smart devices delivering increasingly insightful digital services everywhere. We call this the intelligent digital mesh.

- **Intelligent:** *How AI is in virtually every existing technology, and creating entirely new categories.*
- **Digital:** *Blending the digital and physical worlds to create an immersive world.*
- **Mesh:** *Exploiting connections between expanding sets of people, businesses, devices, content and services.*

Trends under each of these three themes are a key ingredient in driving a continuous innovation process as part of the continuous next strategy.”

The Gartner Top 10 Strategic Technology trends according with [11] highlight changing or not yet widely recognized trends that will impact and transform industries through 2023 (Fig. 56.6).

1. Autonomous things. Whether it's cars (<https://www.gartner.com/smarterwithgartner/4-areas-driving-autonomous-vehicle-adoption/>), robots or agriculture, autonomous things use AI to perform tasks traditionally done by humans. Autonomous things and autonomous systems exist across five types:

- robots and collaborative robots,
- vehicles and V2V systems,
- drones and drone fleets and multi-fleets,
- appliances and collaborative appliance systems,
- agents and multi-agent systems.

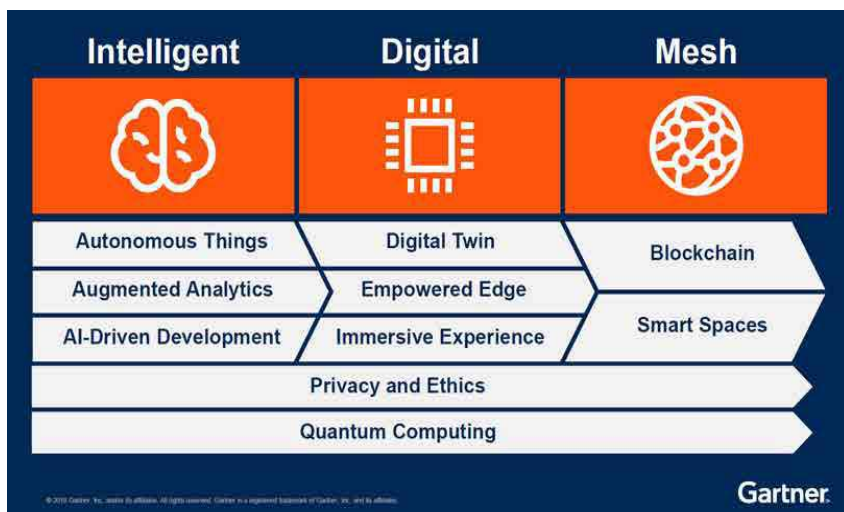


Fig. 56.6 –Gartner Top 10 Strategic Technology trends

Those five types occupy four environments: sea, land, air and digital. They all operate with varying degrees of capability, coordination and intelligence. For example, they can span a drone operated in the air with human-assistance to a farming robot operating completely autonomously in a field. This paints a broad picture of potential applications, and virtually every application, service and IoT object will incorporate some form of AI to automate or augment processes or human actions. Collaborative autonomous things such as drone swarms will increasingly drive the future of AI systems

Explore the possibilities of AI-driven autonomous capabilities in any physical object in your organization or customer environment, but keep in mind these devices are best used for narrowly defined purposes. They do not have the same capability as a human brain for decision making, intelligence or general-purpose learning.

2. Augmented analytics. Data scientists now have increasing amounts of data to prepare, analyze and group — and from which to draw conclusions. Given the amount of data, exploring all possibilities becomes impossible. This means businesses can miss key insights from hypotheses the data scientists don't have the capacity to explore. Augmented analytics represents a third major wave for data and

analytics capabilities as data scientists use automated algorithms to explore more hypotheses. Data science and machine learning platforms have transformed how businesses generate analytics insight.

By 2020, more than 40% of data science tasks will be automated. Augmented analytics identify hidden patterns while removing the personal bias. Although businesses run the risk of unintentionally inserting bias into the algorithms, augmented analytics and automated insights will eventually be embedded into enterprise applications. Through 2020, the number of citizen data scientists will grow five times faster than professional data scientists. Citizen data scientists use AI powered augmented analytics tools that automate the data science function automatically identifying data sets, developing hypothesis and identifying patterns in the data. Businesses will look to citizen data scientists as a way to enable and scale data science capabilities. Gartner predicts by 2020, more than 40% of data science tasks will be automated, resulting in increased productivity and broader use by citizen data scientists.

3. AI-driven development. AI-driven development looks at tools, technologies and best practices for embedding AI into applications and creating AI-powered tools for the development process (<https://www.gartner.com/smarterwithgartner/prepare-for-automations-impact-on-application-development/>). This trend is evolving along three dimensions:

- the tools used to build AI-powered solutions are expanding from tools targeting data scientists (AI infrastructure, AI frameworks and AI platforms) to tools targeting the professional developer community (AI platforms, AI services). With these tools the professional developer can infuse AI powered capabilities and models into an application without involvement of a professional data scientist;

- the tools used to build AI-powered solutions are being empowered with AI-driven capabilities that assist professional developers and automate tasks related to the development of AI-enhanced solutions. Augmented analytics, automated testing, automated code generation and automated solution development will speed the development process and empower a wider range of users to develop applications;

- AI-enabled tools are evolving from assisting and automating

functions related to application development (AD) to being enhanced with business domain expertise and automating activities higher on the AD process stack (from general development to business solution design).

The market will shift from a focus on data scientists partnered with developers to developers operating independently using predefined models delivered as a service. This enables more developers to utilize the services, and increases efficiency. These trends are also leading to more mainstream usage of virtual software developers and nonprofessional “citizen application developers.” Plan and time-schedule of implementing AI strategies for leading countries is shown on Fig. 56.7.

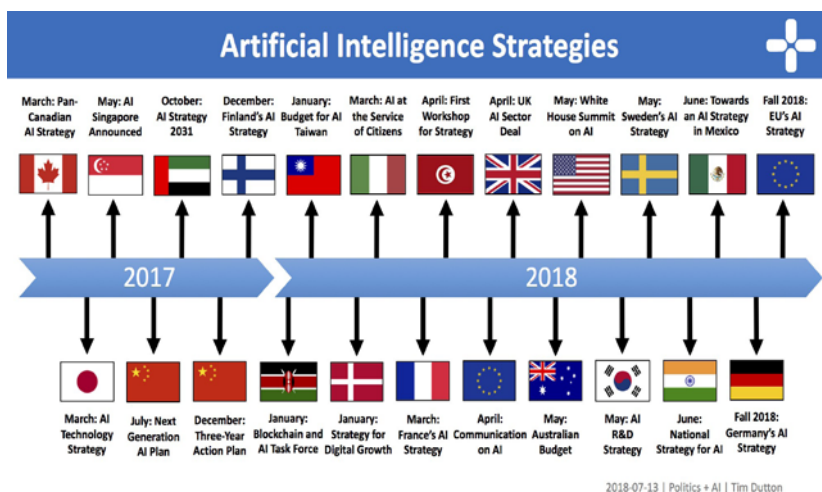


Fig. 56.7 – Implementing AI strategies for leading countries

4. Digital twins. A digital twin is a digital representation that mirrors a real-life object, process or system. Digital twins can also be linked to create twins of larger systems, such as a power plant or city. The idea of a digital twin is not new. It goes back to computer-aided design representations of things or online profiles of customers, but today’s digital twins are different in four ways:

- the robustness of the models, with a focus on how they support specific business outcomes;
- the link to the real world, potentially in real time for monitoring and control;
- the application of advanced big data analytics and AI to drive new business opportunities;
- the ability to interact with them and evaluate “what if” scenarios.

The focus today is on digital twins in the IoT (<https://www.gartner.com/smarterwithgartner/how-to-use-digital-twins-in-your-iot-strategy/>), which could improve enterprise decision making by providing information on maintenance and reliability, insight into how a product could perform more effectively, data about new products and increased efficiency. Digital twins of an organization are emerging to create models of organizational process to enable real time monitoring and drive improved process efficiencies.

5. Empowered edge. Edge computing is a topology where information processing and content collection and delivery are placed closer to the sources of the information, with the idea that keeping traffic local will reduce latency. Currently, much of the focus of this technology is a result of the need for IoT systems to deliver disconnected or distributed capabilities into the embedded IoT world. This type of topology will address challenges ranging from high WAN costs and unacceptable levels of latency.

Further, it will enable the specifics of digital business and IT solutions. Technology and thinking will shift to a point where the experience will connect people with hundreds of edge devices. Through 2028, Gartner expects a steady increase in the embedding of sensor, storage, compute and advanced AI capabilities in edge devices. In general, intelligence will move toward the edge in a variety of endpoint devices, from industrial devices to screens to smartphones to automobile power generators.

6. Immersive technologies. Through 2028, conversational platforms, which change how users interact with the world, and technologies such as augmented reality (AR), mixed reality (MR) and virtual reality (VR), which change how users perceive the world, will lead to a new immersive experience. AR, MR and VR show potential for increased productivity, with the next generation of VR

able to sense shapes and track a user's position and MR enabling people to view and interact with their world. By 2022, 70% of enterprises will be experimenting with immersive technologies (<https://www.gartner.com/smarterwithgartner/immersive-technologies-are-moving-closer-to-the-edge-of-artificial-intelligence/>) for consumer and enterprise use, and 25% will have deployed to production.

The future of conversational platforms, which range from virtual personal assistants to chatbots, will incorporate expanded sensory channels that will allow the platform to detect emotions based on facial expressions, and they will become more conversational in interactions. The technology and thinking will shift to a point where the experience will connect people with hundreds of edge devices ranging from computers to cars.

7. Blockchain. Blockchain is a type of distributed ledger, an expanding chronologically ordered list of cryptographically signed, irrevocable transactional records shared by all participants in a network. Blockchain allows companies to trace a transaction and work with untrusted parties without the need for a centralized party (i.e., a bank). This greatly reduces business friction and has applications that began in finance, but have expanded to government, healthcare, manufacturing, supply chain (<https://www.gartner.com/smarterwithgartner/why-blockchain-matters-to-supply-chain-executives/>) and others.

Blockchain could potentially lower costs, reduce transaction settlement times and improve cash flow. The technology has also given way to a host of blockchain-inspired solutions that utilize some of the benefits and parts of blockchain. Pure blockchain models are immature and can be difficult to scale. However, businesses should begin evaluating the technology, as blockchain will create \$3.1T in business value by 2030. Blockchain inspired approaches that do not implement all the tenets of blockchain deliver near term value but do not provide the promised highly distributed decentralized consensus models of a pure blockchain.

8. Smart spaces. A smart space is a physical or digital environment in which humans and technology-enabled systems interact in increasingly open, connected, coordinated and intelligent ecosystems. As technology becomes a more integrated part of daily life,

smart spaces will enter a period of accelerated delivery. Further, other trends such as AI-driven technology, edge computing, blockchain and digital twins are driving toward this trend as individual solutions become smart spaces. Smart spaces are evolving along five key dimensions: openness, connectedness, coordination, intelligence, scope.

Essentially, smart spaces are developing as individual technologies emerge from silos to work together to create a collaborative and interaction environment. The most extensive example of smart spaces is smart cities <https://www.gartner.com/smarterwithgartner/use-ai-to-make-cities-smarter/>, where areas that combine business, residential and industrial communities are being designed using intelligent urban ecosystem frameworks, with all sectors linking to social and community collaboration.

9. Digital ethics and privacy. Consumers have a growing awareness of the value of their personal information, and they are increasingly concerned with how it's being used by public and private entities. Enterprises that don't pay attention are at risk of consumer backlash. Conversations regarding privacy must be grounded in ethics and trust. The conversation should move from "Are we compliant?" toward "Are we doing the right thing?" Governments are increasingly planning or passing regulations with which companies must be compliant, and consumers are carefully guarding or removing information about themselves. Companies must gain and maintain trust with the customer to succeed, and they must also follow internal values to ensure customers view them as trustworthy.

10. Quantum computing. Quantum computing is a type of non-classical computing that is based on the quantum state of subatomic particles that represent information as elements denoted as quantum bits or "qubits. Quantum computers are an exponentially scalable and highly parallel computing model.

A way to imagine the difference between traditional and quantum computers is to imagine a giant library of books. While a classic computer would read every book in a library in a linear fashion, a quantum computer would read all the books simultaneously.

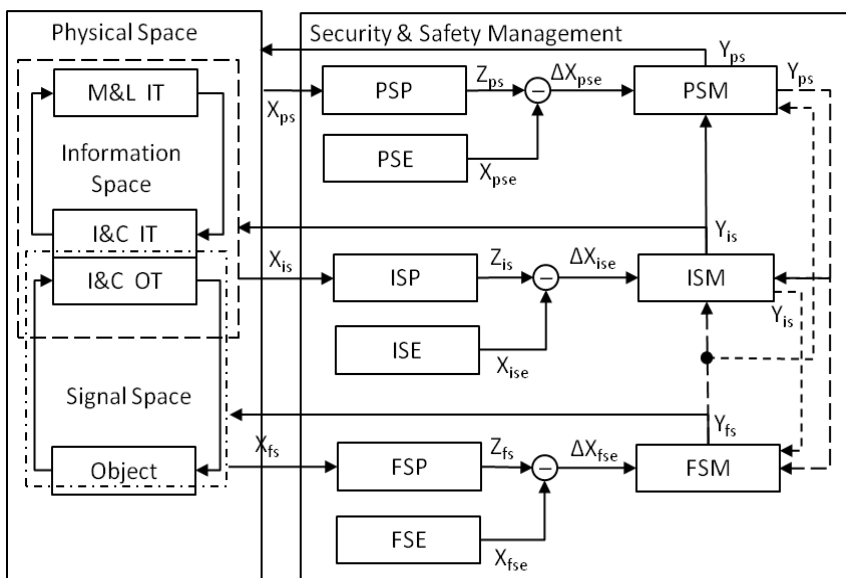
Quantum computers are able to theoretically work on millions of computations at once. Quantum computing in the form of a

commercially available, affordable and reliable service would transform some industries.

56.4.2 Integrated enterprise safety&security management systems for Industry 4.0

Additional challenge of implementation of mentioned trends is cyber security and safety aspect. This is one of the focus for concept Industry 4.0 [12, 13]. Main problem is embedding of security and safety management system into enterprise management system as whole.

The integration of enterprise management systems is based on the series of standards IEC 62264-1-2014. Fig. 56.8 presents an integrated enterprise security management system, which is proposed in [13]. The architecture of each of the channels of this management system is similar to the architecture of the operation management system.



M&L – management & logistic; I&C – instrumentation & control;
 OT – operation technical; IT – information technical; PS – Physical Security
 IS – Information Security; P – processing; E – Etalon; M - Maker

Fig. 56.8 – Integrated Safety-Security Management System

To the composition of the system, it is proposed to introduce three mutually connected areas of security on the levels of physical, information and signal spaces. Let's examine the work of the system on the example of the safety management channel "Physical Space". Signals about the enterprise security state as a physical object (X_{ps}) are transmitted to the PSP block where the appropriate diagnosis (Z_{ps}) is formed. This diagnosis is transferred to the adder. In the adder it is compared with the reference value (X_{pse}), which is formed in the PSE block, and the formation of the control signal as the difference (ΔX_{pse}) = (Z_{ps}) - (X_{pse}) is provided. Under the action of the resulting signal in the PSM block, a control action is formed that guides to the processes in the "Physical Space". A similar algorithm is implemented in the "Information Space" and "Signal Space" channels.

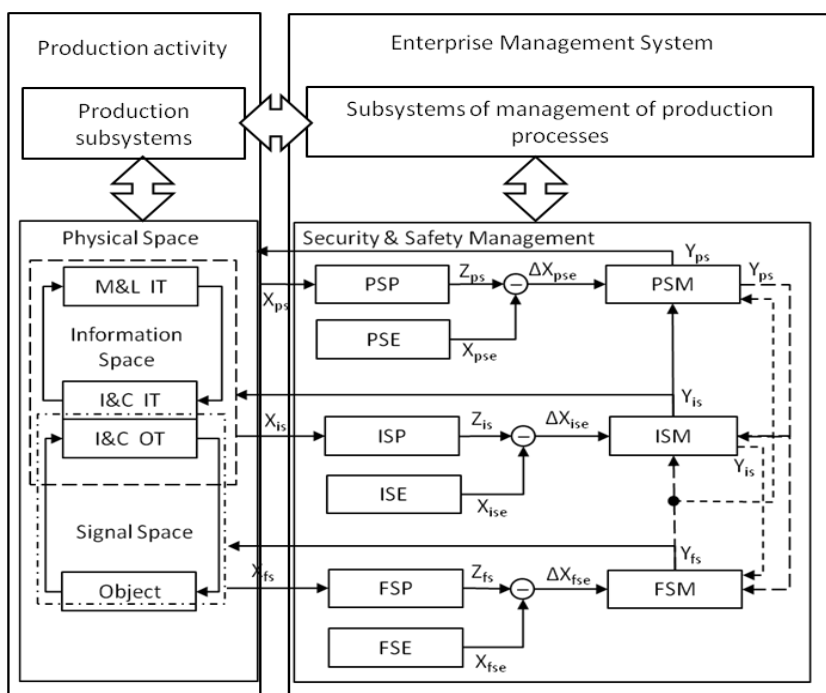
The integration of control channels is carried out by transferring control signals from the "Physical Space" (PSM block) channel to the inputs of the ISM and FSM units. Due to this, "Information Space" and "Signal Space" channels are controlled taking into account the state of the "Physical Space" management channel. Additionally, the control commands from the ISM and FSM units proceed to the PSM block. For this reason control action in the PSM block is formed taking into account the state of the channels "Information Space", and "Signal Space".

The enterprise security management system (Figure 56.8) corresponds to the principle of constructing hierarchical control systems based on the integration of the appropriate channels of the control system. By the content of the control law, this system refers to cybernetic control systems with feedback, so it can be described with the appropriate mathematical apparatus. This will ensure its formation as an automated system of enterprise security dialogue management, or a decision support system in the management of enterprise security. It should also be noted that the usage of the developed security management system has certain features. It differs for enterprises that are software developers or project designers. They don't have a level of functional security (I&C OT) and a sub-level of information security (I&C IT).

The considered system (Fig. 56.8) is part of the overall enterprise management system. Integrated enterprise management system with

enterprise security management system is presented in Fig. 56.9. The integration of the enterprise security management system into the enterprise management system involves the interaction of the subsystems of production process management with the security management subsystems. Similar interaction exists between production subsystems and subsystems that describe the signaling, information and physical security levels.

It should be noted that the formation of security subsystems the indicated levels can be carried out using various methods of forming management systems, and management, which were described above. It



M&L – management & logistic; I&C – instrumentation & control;
 OT – operation technical; IT – information technical; PS – Physical Security
 IS – Information Security; P – processing; E – Etalon; M - Maker

Figure 56.9 – Integrated enterprise management system with the enterprise security management system

has been shown above that the developed and applied information technologies are based on a functional representation. At the same time, the standard of the IEC series 62264-1-2014 [14] establishes that the most for receiving, transmitting, storing and presenting data and information significant should be the methodology of modeling the enterprise in which the *physical*, *informational* and *cybernetic* (in the form of data transmission) views should be presented in an explicit form. This requirement is especially important for Industry 4.0. Global industry digitization raises the problem of cybernetic threats for any of the information processes implemented with the use of digital technologies.

56.5 Industry 5.0 and Internet of Things

56.5.1 Stages of Industry X.0: Toward Industry 5.0

In spite of the fact that Industry 4.0 is only at the initial stage of the development and the main achievements can be expected not earlier than 2020-2025, the image of a new paradigm of Industry 5.0 could be seen.

According with [15] <https://www.linkedin.com/pulse/what-industry-50-dr-marcell-vollmer> the following stages of Industry X.0 (X = 1,2,3,4,5):

Industry 1.0: 1780 – Mechanization (industrial production based on machines powered by water and steam);

Industry 2.0: 1870 – Electrification (mass-production using assembly lines);

Industry 3.0: 1970 – Automation (using electronics and computers);

Industry 3.5: 1980 – Globalization (offshoring of production to low-cost economics);

Industry 4.0: 2010 - Today – Digitalization (introduction of connected devices, data analytics and AI technologies to automate processes further);

Industry 5.0: Future (2025+) – Personalization (cooperation between man and machine as human intelligence works in harmony with cognitive computing. By putting humans back into industrial

production with collaborative robots, workers will be upskilled to provide value-added tasks in production, leading to mass customization and personalization for customers).

Paradigm of Industry 5.0 involves the penetration of Artificial Intelligence in man's common life, their "cooperation" with the aim of enhancing the man capacity and the return of the man at the "Centre of the Universe".

Industry 5.0 will revolve around the interactions between man and machine. Greater collaboration between the two is expected as cognitive computing will be better equipped to work alongside human intelligence [16, 17].

Probably, the more exact term instead of Industry 5.0 is "Society 5.0" (SuperSmart Society) that was offered in 2016 by Japan's most important business federation, Keidanren and being strongly promoted by Council for Science, Technology and Innovation; Cabinet Office, Government of Japan [15].

Unlike the concept of Industry 4.0, Society 5.0 is not restricted only to a manufacturing sector, but it solves social problems with the help of integration of physical and virtual spaces. In fact, Society 5.0 is the society where the advanced IT technologies, IoT, robots, an artificial intelligence, augmented reality (AR) are actively used in people common life, in the industry, health care and other spheres of activity not for the progress, but for the benefit and convenience of each person. The task is to provide the transformation from Industry 4.0 to Society 5.0 considering modern technologies – from IoT up to emergent intelligence.

Industry 5.0 will give us the ability to close the loop so we can push the boundaries of physics on design. If you're trying to make the next-generation aircraft, for example, you're constrained by today's manufacturing capabilities. You're also constrained by the amount of data that you have coming back from the infield service of an aero engine or aircraft and your ability to feed that in-service data back into the design process.

With Industry 5.0, you'll be able to automate the manufacturing process better, which means you'll have real-time data coming in from the field. If you take that to the next stage and you have true, seamless data between the field, the manufacturing process and the design,

you're taking humans out of the manufacturing route, but they'll be more involved in how the product is being used and how it can be designed because they have more information.

Flipping the aero and automotive industries from a fossil-fuel world to an electrical world, for example, is going to be a significant design challenge and it will be much easier for humans to solve if the mundane tasks are being dealt with by AI techniques and robots.

56.5.2 Future of Internet of Things

Kevin Ashton, who coined the term IoT in 1999, explained that the IoT is not simply barcoding of objects nor robots executing predetermined computer scripts [18]:

“In the twentieth century, computers were brains without senses—they only knew what we told them. That was a huge limitation: there is many billion times more information in the world than people could possibly type in through a keyboard or scan with a barcode. In the twenty-first century, because of the Internet of Things, computers can sense things for themselves. It’s only been a few years, but we already take networked sensors for granted. One example is GPS-based location sensing”.

Ten years later he wrote [19]:

Our economy, society and survival aren't based on ideas or information – they're based on things. You can't eat bits, burn them to stay warm or put them in your gas tank. Ideas and information are important, but things matter much more. Yet today's information technology is so dependent on data originated by people that our computers know more about ideas than things.

If we had computers that knew everything there was to know about things—using data they gathered without any help from us—we would be able to track and count everything, and greatly reduce waste, loss and cost. We would know when things needed replacing, repairing or recalling, and whether they were fresh or past their best.

We need to empower computers with their own means of gathering information, so they can see, hear and smell the world for themselves, in all its random glory. RFID and sensor technology enable computers

to observe, identify and understand the world—without the limitations of human-entered data.

Ten years on, we've made a lot of progress, but we in the RFID community need to understand what's so important about what our technology does, and keep advocating for it. It's not just a "bar code on steroids" or a way to speed up toll roads, and we must never allow our vision to shrink to that scale. The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more so".

In 2019 we see how IoT has changed world and better understand how IoE can be changed in future and how it'll change a world. It concerns as human domains and industry systems. IoE becomes Internet of micro- and nano-Things for new generation of cyber physical systems, and Internet of macro-Things, such as an Internet of Data Centers, Internet of Infrastructures.

56.6 Work related analysis

This section has been prepared considering:

- experience and activities of Association of Industrial Automation of Ukraine [1-9] <https://appau.org.ua/en/about-en/> (subsections 56.1-56.3);

- international trends in development of modern paradigms, concepts and technologies in context of Industry 4.0, first of all using technical report of Gartner (subsection 56.4.1) and publications [10-12];

- R&D activities of Kharkiv Region Centre Industry 4.0 based on KhAI and Department of computer systems, networks and cyber security [11] as part of APPAU community (subsection 56.4.2) [13];

- publications related to forming of concept Industry 5.0 [15-19].

Besides, the following courses and programs have been analysed and taken into account:

- Coimbra University, Portugal: IoT course for MSc [20]. The courses represents a new stage in the digital evolution and focuses on the Internet of Things for smart transport and cities, and the development of tools to transform city infrastructure;

- KTH University, Sweden: MSc programs including IoT related topics in Information and Network Engineering [21];

- The National University of Singapore [22]: The NUS Master of Science in Industry 4.0 is an interdisciplinary graduate degree programme to help you keep pace with the changing nature of industries amid technological disruptions, and lead transformation to enhance productivity in the workplace;

- University of Salford Manchester [23]: MSc Leadership for Industry 4.0 is designed to help build a new generation of leaders who can take the opportunities and mitigate the challenges that come with the fourth industrial revolution;

- University of Strathclyde, Glasgow [24]: Master on Digital Manufacturing course covers Industry 4.0 technologies such as Cyber-Physical Systems, Industrial Internet of Things, Additive Manufacturing and Autonomous Mechatronic Systems. Digital Manufacturing also feeds into new business models such as Through-Life Engineering and Cloud Manufacturing – all extremely hot topics with vast industrial as well as academic potential.

Conclusions and questions

This section is final one of three-volume book on different aspects of Internet of Things. Methodology and a set of technologies related to Internet of Thing are extremely developed in context of general evolution of society and industry and movement to World 4.0 and 5.0. Development and implementation of Internet of Things and, in particular, industrial IoT is one of the most important trends of general digitalization and integration. IoT becomes smart circulatory system of enterprises and industry as a whole.

Depending on level of on-board things intellect and restrictions of communication traffic three methodologies of modern systems are applied, developed and integrated: sensor networks, Internet of Things and edge computing.

In [25] <https://www.netobjex.com/a-strategists-guide-to-the-fourth-industrial-revolution/> respondents from different domains were asked: “How would you classify the current level of digitalization and integration (due to IoT as well) in your company and industry branch? What level are you expecting in the next five years?”



















Results of assessment and prediction are presented on Table 56.3. Similar question we address to you. Please make your predicting

digitalization of domains and argue your differences with Table 56.3 if it's needed.

Besides, we invite you to answer the following questions to better understand and assimilate the educational material presented in this section.

1. What does Industry 4.0 mean in point of view evolution of:
 - paradigms of industry and society development;
 - technologies including IoT;
 - processes of industry systems creation and operation.
2. What are main direction of national strategy and movement 4.0 in Ukraine and other countries?
3. What are key challenges in implementation of concept Industry 4.0 for education, employment, manufacturing and operation?
4. What does landscape mean for company/university/country in point of view Industry 4.0?

Table 56.3 – The results of assessment and prediction of digitalization and integration

NOW			IN FIVE YEARS	
	45%	Electronics		77%
	32%	Aerospace and Defense		76%
	35%	Industrial Manufacturing		76%
	32%	Chemicals		75%
	38%	Forest Products, Paper, Pkg.		72%
	28%	Transportation and Logistics		71%
	30%	Engineering and Construction		69%
	41%	Automotive		65%
	31%	Metals		62%

5. Can landscape be formalized as a model of description for directions, technologies such as IoT and domains for application? Please, suggest your variant such models based on analysis of Figures 56.3-56.5.

6. Please, list top trends of technology development in 2019 according with Gartner report. Can we add any other technologies?

7. What are criteria of introducing a technology to top trends list? Do you agree with 3 top criteria/themes as Intelligent, Digital, Mesh?

8. How does introducing of technology in Top Trends depend (or not depend) on its position on Gartner Hype cycle? <https://www.gartner.com/en/research/methodologies/gartner-hype-cycle>

8. Could you describe connections of IoT with technologies of Gartner top trend (subsection 56.4.2)? Please, argue your answer for:

- autonomous things and systems,
- augmented, virtual and mixed reality,
- AI-driven development (platforms, services),
- digital twins,
- empowered edge,
- blockchain,
- quantum computing,
- safety, security and privacy assurance technologies.

9. What are features of methodology of (cyber) safety and security assurance for manufactures Industry 4.0?

10. How does implementation of industrial IoT influence on safety and security in this case?

11. How can safety&security control system be integrated into general management system of enterprise Industry 4.0?

12. What is a difference between Industry 4.0 and 5.0 paradigms? How do you predict evolution of IoT/IOE in context Industry/Society/World 5.0?

References

1. Association of Industrial Automation of Ukraine
[<https://appau.org.ua/en>]

2. National movement “Industry 4.0 in Ukraine”
[<https://industry4-0-ukraine.com.ua>]

3. The report of Ukrainian IT-industry
[http://www.uadn.net/files/ua_hightech.pdf]

4. Global Cyber Security Summit 2017, Kyiv, 14-15th of June 2017 [<https://www.techrepublic.com/videos/video-the-global-cybersecurity-summit-aims-to-address-the-worlds-most-urgent-cybersecurity/>]

5. The national strategy Industry 4.0 [https://www.slideshare.net/APP AU_Ukraine/strategy-industry-4-0-of-ukraine-201921-overview]

6. APPAU and partners started the realization of national strategy Industry 4.0 [<https://appau.org.ua/en/pubs/current-status-of-industry-4-0-projects>]

7. Transition from Industry 3.0 to 4.0 [<https://industry4-0-ukraine.com.ua/2019/03/03/positionning-of-innovators-4-0-why-and-how>]

8. Ukrainian Landscape Industry 4.0 for technologies and application [<https://industry4-0-ukraine.com.ua>]

9. O. Yurchak. "Industry 4.0 Landscape of Ukraine 2017", Carte Blanche, 2017, 1 (138), pp.3-5.

10. Landscape of Digital Twin IIoT technologies for Industry 4.0 implemented by company Alleantia [<https://www.alleantia.com/company>]

11. Top 10 strategical technology trends in 2019 have been presented by Gartner company [<https://www.gartner.com/en/doc/383829-top-10-strategic-technology-trends-for-2019-a-gartner-trend-insight-report>]

12. Smarter Security for Manufacturing in Industry 4.0. Era Industry 4.0 Cyber Resilience for the Manufacturing of the Future. White HITE Paper [<https://www.symantec.com/content/dam/symantec/docs/solution-briefs/industry-4.0-en.pdf>]

13. V. Kharchenko, S. Dotsenko, O. Illiashenko, S. Kamenskyi, "Integrated Cyber Safety and Security Management System: Industry 4.0 Issue," Proc. of the 10th IEEE Dependable Systems, Services and Technologies Conference, DESSERT 2019, pp. 197-201.

14. IEC 62264-1-2014 Enterprise-control system integration. Part 1. Models and terminology.

15. Why it is Industry 5.0? [<https://www.linkedin.com/pulse/what-industry-50-dr-marcell-vollmer/>]

16. What is Industry 5.0? [<https://www.robotics.org/blog-article.cfm/What-is-Industry-5-0-and-How-Will-Industrial-Robots-Play-a-Role/99>]

17. Guide to Industry 4.0 & 5.0 [<https://blog.gesrepair.com/2017/11/16/industry-4-and-5>]

18. Vural Özdemir, Nezhir Hekim. Birth of Industry 5.0: Making Sense of Big Data with Artificial Intelligence, “The Internet of Things” and Next-Generation Technology Policy [https://www.researchgate.net/publication/322216652_Birth_of_Industry_50_Making_Sense_of_Big_Data_with_Artificial_Intelligence_The_Internet_of_Things_and_Next-Generation_Technology_Policy]

19. Kevin Ashton. That 'Internet of Things' Thing [<https://www.rfidjournal.com/articles/view?4986>]

20. Internet Of Things Course - Immersive Program Master in City and Technology [<https://apps.uc.pt/search?q=Internet+of+Things>]

21. Master's program in Information and Network Engineering [<https://www.kth.se/en/studies/master/information-and-network-engineering/master-s-programme-in-information-and-network-engineering-1.673817>]

22. The NUS Master of Science in Industry 4.0 [https://scale.nus.edu.sg/programmes/graduate/MSc-Industry-4_0]

23. University of Salford, Manchester. MSc Leadership for Industry 4.0 [<https://beta.salford.ac.uk/courses/postgraduate/leadership-industry-40>]

24. University of Strathclyde [<https://www.masterstudies.com/MScPG-DipPG-Cert-in-Digital-Manufacturing/United-Kingdom/USFE>]

25. A Strategist's Guide To The Fourth Industrial Revolution. [<https://www.netobjex.com/a-strategists-guide-to-the-fourth-industrial-revolution>]

УДК 62:004=111

173

Рецензенти: Dr. Mario Fusani, ISTI-CNR, Піза, Італія
Dr. Olga Kordas, KTH University, Стокгольм, Швеція
Viktor Kordas, KTH University, Стокгольм, Швеція

173 Інтернет речей для індустріальних і гуманітарних застосунків. У трьох томах. Том 3. Оцінювання та впровадження / За ред. В. С. Харченка. - Міністерство освіти і науки України, Національний аерокосмічний університет ХАІ, 2019. - 918с.

ISBN 978-617-7361-83-0

Книга, що складається з трьох томів, містить теоретичні матеріали для лекцій та тренінгів, розроблених в рамках проекту Internet of Things: Emerging Curriculum for Industry and Human Applications / ALIOT, 573818-EPP-1-2016-1-UK-EPPKA2- CBHE-JP, 2016-2019, що фінансується програмою ЄС ERASMUS +. Том 3 описує методи і інструменти для створення, оцінки та впровадження Інтернету речей (IoT) в різних областях індустрії та гуманітарних застосунків. Книга складається з 6 частин для відповідних навчальних курсів: IoT для інтелектуальних енергосистем (розділи 32-35), IoT для інтелектуальних будівель і міст (розділи 36-39), IoT для інтелектуальних транспортних систем (розділи 40-43), IoT для медичних систем (розділи 44-47), IoT для систем моніторингу екології та безпеки (розділи 48-51), IoT для промислових систем (розділи 52-56).

Книга підготовлена українськими університетськими командами за підтримки колег з академічних закладів країн ЄС, що входять в консорціуму проекту ALIOT.

Книга призначена для магістрантів і аспірантів, які вивчають технології IoT, програмну і комп'ютерну інженерію, комп'ютерні науки. Може бути корисною для викладачів університетів і навчальних центрів, дослідників і розробників систем IoT.

Рис.: 350. Посилань: 721. Таблиць: 66.

АНОТАЦІЇ РОЗДІЛІВ

У розділі 32 представлено огляд компонентів смарт грід та відповідних інформаційних технологій в контексті Інтернету речей. Проведено огляд різних комунікаційних додатків і технологій смарт грід, їх переваг, характеристик і вимог. Обговорюються проблеми, пов'язані з використанням для смарт грід нових технологій, таких як хмарні обчислення і великі дані.

У розділі 33 розглянуто компоненти вбудованих систем та їх роль в організації локальної частини смарт енергогрід (СЕГ) як складової частини IoT інфраструктури. У цьому розділі проведений огляд підходів до організації локальної частини СЕГ. У контексті апаратних пристроїв, також були розглянуті програмні компоненти для повного представлення зв'язків між технологіями у даній області. У розділі підкреслюється, що незважаючи на те, що локальний сегмент СЕГ є найнижчим рівнем в організації СЕГ, він є комплексним рішенням, яке інтегрує програмні і апаратні складові, що взаємодіють на локальному рівні, так і з вищими рівнями СЕГ.

У розділі 34 описуються системи смарт грід з IT-структурою на основі IoT. У цьому розділі представлена вичерпна інформація щодо оцінки надійності IT-інфраструктури на основі IoT, класифікації відмов інформаційно-керуючих систем, основні моделі надійності та методи її оцінки та забезпечення. Розглянуто метод оцінки безпеки з урахуванням надійності компонентів та підсистем (систем). Описано особливості впровадження машинного та глибокого навчання нейронних мереж, прогностичної аналітики для систем Інтернету речей. Описано та досліджено Марковські моделі функціонування систем Інтернету речей для смарт грід.

У розділі 35 представлено опис підходів до моделювання функціональної та кібербезпеки смарт грід, заснованої на IoT. Крім того, надано огляд проблем в області безпеки і захисту смарт грід в контексті IoT, існуючих завдяки взаємовпливу між системами в смарт грід. Описано низку підходів до оцінки безпеки і надійності, а також стратегії забезпечення безпеки смарт грід в контексті IoT. Представлено системний підхід до менеджменту

безпеки смарт грід, а також проаналізовано роль пристроїв IoT в реалізації процесів менеджменту безпекою. Наводяться основні положення з оцінювання якості сервісів смарт грід з урахуванням резил'єнтності, а також описується підхід до безпечного середовищі розроблення та експлуатації резил'єнтних цифрових підстанцій.

У розділі 36 наведено методи оцінки ризиків в системі Інтернету речей. Для виконання оцінки пропонується ієрархічний поділ Шнтернету речей на підсистеми відповідно до функціонального призначення підсистем. Для цього використані елементи загальної теорії систем. Розроблено шкалу ризиків і описано алгоритм оцінювання методом експертних оцінок. Показано, що найбільші ризики для підсистем виникають при відмовах суміжних підсистем, і сформульовано практичні рекомендації.

Розділ 37 присвячено аналізу та принципам роботи систем розумного будинку. Розглядаються промислові давачі контролю зовнішнього середовища та їх взаємодія з мікропроцесорними пристроями. Детально розглянуто побудову і функціонування всіх систем розумного будинку - освітлення, кліматичний контроль, система безпеки. Розглянуто взаємодію пристроїв розумного будинку з використанням технологій інтернету речей.

У розділі 38 проаналізовано сучасні технології та інструментарій для розробки програмно-апаратної платформи для системи Розумний будинок. Наведено особливості проектування вбудованих систем як основи інфраструктури Інтернету речей. Обговорюються питання розробки архітектури системи Розумний будинок, а також особливості застосування платформ Raspberry Pi та OpenHAB для управління системою. Докладно описані можливості застосування віддаленої лабораторії Smart House&IoT для прототипування системи Розумний будинок.

У розділі 39 розглянуто технології взаємодій систем розумного будинку і міста в їх архітектурі, поведінці і синхронізації. Визначено формальні специфікації сутностей, їх відношенні, даних, умов, подій, дій і функцій архітектури. Представлено моделювання взаємодій в процесах систем

розумного будинку і міста. Розглянуто специфікації і моделювання взаємодій на функціональному рівні для систем розумного будинку, на рівні синхронізації для систем розумного міста.

У розділі 40 представлено інтелектуальну систему контролю транспортного потоку, яка використовує інформацію з відеокамер, здійснює її подальшу обробку, передачу та прийняття рішень з використанням технології інтернет речей. Проведено огляд апаратних та програмних засобів, потрібних для реалізації даної задачі. Проаналізовано методи розпізнавання та класифікації транспортних об'єктів у відеопотоці. Розроблено інтелектуальну систему контролю інтенсивності транспортного потоку.

У розділі 41 відображено результати розробки і впровадження архітектури для розгортання інфраструктури інформаційних послуг для громадського пасажирського транспорту. Основним внеском цього розділу є інтегрована, формальна і автоматизована методологія для інформаційних служб громадського транспорту. Була розроблена концепція збору даних в реальному часі і вибору ефективної моделі для прогнозування часу прибуття транспортного засобу. Формулюються висновки, як поліпшуються послуги громадського транспорту, використовуючи дані GPS і дані, що надаються додатками IoT.

У розділі 42 розглянуто принципи і вимоги до проектування кооперативних людино-машинних інтерфейсів інтелектуальних транспортних систем. Запропоновано архітектуру системи на основі Інтернету речей і протоколт взаємодії. Розглянуто питання оцінки ефективності та функціональної безпеки людино-машинних інтерфейсів для таких систем. Наведено прототип кооперативного інтерфейсу транспортної IoT системи.

У розділі 43 представлено концептуальну архітектуру флоту дронів. Розглянуто комунікаційні технології, які використовуються для безпілотних літальних апаратів. Продемонстровані основні можливості технології Інтернету дронів. Висвітлено основні питання безпеки, пов'язані з використанням систем на основі Інтернету дронів. Обговорено етапи оцінки ризику безпеки безпілотних авіаційних систем. Представлено концепцію системи післяаварійного моніторингу на

основі Інтернету дронів, а також розроблені моделі надійності для різних варіантів побудови такої системи.

У розділі 44 розглянуто інфраструктуру Інтернету речей в галузі охорони здоров'я. Представлений аналіз вимог стандартів до інфраструктури інтернету речей для систем охорони здоров'я. У цьому розділі пояснюються існуючі і перспективні технології Інтернету речей для реалізації систем охорони здоров'я. Показано процес розробки і моделювання інфраструктури Інтернету речей для систем охорони здоров'я.

У розділі 45 описано проблеми безпеки і приватності IoT для систем охорони здоров'я. Представлені вимоги безпеки і приватності стандартів до таких систем. Розроблено ієрархічну модель кібербезпеки для такого роду систем. Представлено огляд відмов і атак на такі системи. Проаналізовано інфраструктуру за допомогою методу аналізу дерев відмов/атак. Розроблено множину марковських моделей, яка дозволяє враховувати специфіку пристроїв користувачів, канали зв'язку, потоки даних і питання безпеки цих компонентів.

У розділі 46 представлено матеріали для модуля курсу «Переносні IoT-системи для біомедичних застосувань». Їх можна використовувати для підготовки до лекцій і самонавчання. Мета розділу: дати глибокі знання щодо принципів і методів, заснованих на IoT технологіях для охорони здоров'я та створення біомедичних систем; практичні рекомендації щодо розроблення і тестування інтелектуальних біомедичних пристроїв, виконання аналізу даних в режимі реального часу.

У розділі 47 представлено матеріали для модуля «Devices with reconfigurable architecture for biomedical IoT based applications». В розділі надано узагальнену інформацію про хворобу Паркінсона, вибір певних фізіологічних показників. Описано системи моніторингу рухових симптомів хвороби Паркінсона, давачів, приладів, обладнання, параметрів виявлення і методів аналізу даних. Представлено архітектуру системи, описано її функціональність, основні характеристики, а також методика обробки даних. Описано результати впровадження розробленої

системи, а саме: мобільний додаток, тести, методики збору, передачі та обробки даних.

У розділі 48 розглянуто основні засади застосування Інтернету речей у різних сільськогосподарських технологіях, таких як, керування станом штучних екологічних систем на зразок теплиць чи іригаційних систем, моніторинг стану погодних умов та стану посівів на відкритому ґрунті. Розглянуто особливості використовуваних давачів та фізичних параметрів, які вимірюються, основні методи оброблення інформації від давачів.

У розділі 49 представлено матеріали для модуля «IoT для систем моніторингу екології, безпеки і охорони». Проаналізовано поточні дослідження давачів IoT для моніторингу навколишнього середовища і аналітичні методи для різних систем на основі IoT для додатків моніторингу води. Розглядаються перспективи та проблеми при розробленні IoT системи моніторингу якості води: визначення параметрів та їх вимірювання для всіх типів водних об'єктів; інструменти збору даних та можливості співіснування різних систем IoT, які є частиною комплексу управління водними об'єктами. Описано процес розроблення IoT-системи: пристроїв апаратно-програмних засобів, панелі для онлайн-моніторингу водних об'єктів. Розглянуто задачі управління водними ресурсами з використанням IoT і аналізу великих даних.

У розділі 50 запропоновано класифікацію систем радіаційного моніторингу та проаналізовано структури таких систем. Описано загальну структуру та основні принципи створення багатoversійної системи післяаварійного моніторингу на основі технології Інтернету дронів. Побудовано структурні схеми надійності цієї системи та її підсистем для різних варіантів використання датчиків, організації передачі даних та способів прийняття рішень. На основі структурних схем надійності розроблено і проаналізовано моделі, сформульовано практичні рекомендації щодо забезпечення надійності системи та її підсистем.

У розділі 51 розглянуто теоретичні та практичні аспекти системи фізичної безпеки (СФБ) будівель і кампусів на базі Інтернету речей. Пояснюється необхідність впровадження систем

фізичної безпеки, пропонуються структури і підходи до розробки та впровадження СФБ на основі IoT. Описана методика PSMECA для критичної оцінки відмов СФБ.

У розділі 52 розглянуто структури, моделі і технології для розробки промислових IoT систем. Основні тенденції та особливості в промислових IoT системах оглянуто на базі великого числа IoT застосувань. Крім того, розглядаються програмні компоненти і протоколи дротових і бездротових технологій для побудови IoT мереж. Аналізуються проблеми безпеки в промислових IoT системах: основні типи атак, стандарти шифрування даних і політика безпеки промислових IoT систем.

У розділі 53 розглянуто сучасні методи та засоби для проектування, модернізації та впровадження промислових IoT систем. Надано опис IoT систем управління та моніторингу для плаваючих доків, процесів розроблення та підтримки відповідних IoT систем, а також апаратно-програмних засоби для їх реалізації. Розглядаються підходи до модернізації складних об'єктів у різних промислових IoT системах: для спеціалізованого піролізного комплексу та промислового робота з адаптивним захватом.

Розділ 54 присвячено впровадженню і використанню IoT технологій в авіації, зокрема, діагностиці стану авіаційних двигунів і літальних апаратів. З огляду на великий обсяг даних, характеризуючих технічний стан авіаційної системи, використовується технологія хмарного зберігання і передачі даних. На її основі реалізовано стратегію застосування нейронних мереж для аналізу даних, прийняття рішення і віддаленого управління об'єктом діагностування. Використання апарату нейронних мереж допомагає з високою точністю визначити технічний стан і скласти прогноз про подальші зміни. Впровадження IoT технологій і апарату нейронних мереж дозволяє знизити вартість тестування і обслуговування обладнання, запобігати фатальним відмовам і зберегти людські життя.

В розділі 55 розглянуто питання оптимізації витрат апаратури в логічній схемі пристрою управління вузлом індустріальної IoT системи, що реалізований у вигляді мікропрограмного автомату. Детально описано принцип операційного перетворення кодів

станів, відповідно до якого функція переходів мікропрограмного автомата імплементується операційним автоматом. Розглянуті питання структурної організації, синтезу та визначення ефективності мікропрограмного автомата з операційним автоматом переходів для індустріальної IoT системи. Сформульовано питання покращення технічних характеристик апаратних компонентів для індустріальних систем IoT.

Мета, стратегія і ландшафт руху Індустрія 4.0 в Україні проаналізовано у розділі 56. Розглянуто завдання і напрями діяльності Асоціації підприємств промислової автоматизації України (АППАУ), яка є драйвером руху Індустрія 4.0. Дискутуються виклики впровадження індустріального Інтернету речей в контексті Індустрія 4.0. Описано топ-тренди технологій за результатами аналізу компанії Gartner (intelligence, autonomy, mesh). Система управління інтегрованою IT-безпекою підприємств Індустрія 4.0 описується. Сутність і майбутні тренди Індустрія 5.0 аналізуються.

УДК 62:004=111

173

Рецензенты: Dr. Mario Fusani, ISTI-CNR, Пиза, Италия
Dr. Olga Kordas, KTH University, Стокгольм, Швеция
Viktor Kordas, KTH University, Стокгольм, Швеция

173 Интернет вещей для промышленных и гуманитарных приложений. В трех томах. Том 3. Оценивание и внедрение /
Под ред. В. С. Харченко. - Министерство образования и науки Украины, Национальный аэрокосмический университет ХАИ, 2019. - 918с.

ISBN 978-617-7361-83-0

Книга, состоящая из трех томов, содержит теоретические материалы для лекций и тренингов, разработанных в рамках проекта Internet of Things: Emerging Curriculum for Industry and Human Applications /ALIOT, 573818-EPP-1-2016-1-UK-EPPKA2- CBHE-JP, 2016-2019, финансируемого программой ЕС ERASMUS +. Том 3 описывает методы и инструменты для создания, оценки и внедрения Интернета вещей (IoT) в различных областях промышленности и гуманитарных приложений. Книга состоит из 6 частей для соответствующих учебных курсов: IoT для интеллектуальных энергосистем (разделы 32-35), IoT для интеллектуальных зданий и городов (разделы 36-39), IoT для интеллектуальных транспортных систем (разделы 40-43), IoT для медицинских системы (разделы 44-47), IoT для систем мониторинга экологии и безопасности (разделы 48-51), IoT для промышленных систем (разделы 52-56).

Книга подготовлена украинскими университетскими командами при поддержке коллег из академических организаций стран ЕС, входящих в консорциум ALIOT.

Книга предназначена для магистрантов и аспирантов, изучающих технологии IoT, программную и компьютерную инженерию, компьютерные науки. Может быть полезна для преподавателей университетов и учебных центров, исследователей и разработчиков систем IoT.

Рис.: 305. Ссылки: 721. Таблиц: 66

АННОТАЦИИ РАЗДЕЛОВ

В разделе 32 представлены данные о компонентах smart grid и используемых информационных технологиях в контексте Интернета вещей. Проведен обзор различных коммуникационных приложений и технологий smart grid, их преимуществ, характеристик и требований. Обсуждаются проблемы, связанные с использованием новых технологий для smart grid, таких как облачные вычисления и большие данные.

В разделе 33 рассмотрены компоненты встраиваемых систем и их роль в организации локальной части SEG (smart energy grid) как составной части IoT инфраструктуры. Выполнен обзор подходов к организации локальной части SEG. В контексте аппаратных устройств рассмотрены программные компоненты для полного представления связей между технологиями в данной области. Подчеркивается, что несмотря на то, что локальный сегмент является низшим уровнем в организации SEG, он является комплексным решением, которое интегрирует программные и аппаратные составляющие, взаимодействующие как на локальном уровне, так и с более высокими уровнями SEG.

В разделе 34 описаны системы smart grid с ИТ-инфраструктурой на основе IoT. Представлена исчерпывающая информация, касающаяся оценки надежности ИТ-инфраструктуры на основе IoT, классификации сбоев информационно-управляющих систем, основных моделей надежности и методов ее оценки и обеспечения. Рассмотрен метод оценки безопасности с учетом надежности компонентов и подсистем (систем). Описаны особенности реализации машинного и глубокого обучения нейронных сетей, прогнозной (предиктивной) аналитики для систем Интернета вещей. Исследованы Марковские модели функционирования систем Интернета вещей для интеллектуальной сети.

В разделе 35 представлено описание подходов к моделированию функциональной и кибербезопасности smart grid, основанной на IoT. Проводится обзор проблем в области безопасности и защиты smart grid в контексте IoT, существующих из-за взаимовлияния между системами в smart

грид. Описывается ряд подходов к оценке безопасности и надежности, а также стратегии обеспечения безопасности смарт грид в контексте IoT. Представлен системный подход к менеджменту безопасности смарт грид, а также приведена роль устройств IoT в реализации процессов менеджмента безопасности. Приводятся основные положения по оцениванию качества сервисов смарт грид с учетом резильентности, а также описывается подход к безопасной среде разработки и эксплуатации резильентных цифровых подстанций.

В разделе 36 приведены методы оценки рисков в системе Интернета вещей. Для выполнения оценки предлагается иерархическое разделение Интернета вещей на подсистемы в соответствии с их функциональным назначением. Для этого использованы элементы общей теории систем. Разработана шкала рисков и описана методика оценивания методом экспертных оценок. Исследования показали, что наибольшие риски для подсистем возникают при отказах смежных подсистем. Сформулированы практические рекомендации.

Раздел 37 посвящен анализу и принципам работы систем умного дома. Рассматриваются промышленные датчики контроля внешней среды и их взаимодействие с микропроцессорными устройствами. Подробно описано построение и функционирование всех систем умного дома - освещения, климатического контроля, безопасности. Рассмотрено взаимодействие устройств умного дома с использованием технологий Интернета вещей.

В разделе 38 представлены современные технологии и инструментарий для разработки программно-аппаратной платформы для системы Умный дом. Показаны особенности проектирования встроенных систем как основы инфраструктуры Интернета вещей. Обсуждаются вопросы разработки архитектуры системы Умный дом, а также особенности применения платформ Raspberry Pi и OpenHAB для управления системой. Описаны возможности применения удаленной лаборатории Smart House&IoT для прототипирования системы Умный дом.

В разделе 39 рассматриваются технологии взаимодействий систем умного дома и города в их архитектуре, поведении и

синхронизации. Определены формальные спецификации сущностей, их отношения, данных, условий, событий, действий и функций архитектуры. Представлены алгоритмы моделирования взаимодействий в процессах систем умного дома и города. Рассмотрены спецификации и моделирование взаимодействий на функциональном уровне для систем умного дома, на уровне синхронизации – для систем умного города.

В разделе 40 представлена интеллектуальная система контроля транспортного потока, которая использует информацию с видеокамер, осуществляет ее дальнейшую обработку, передачу и принятие решений с использованием технологии Интернета вещей. Проведен обзор аппаратных и программных средств, необходимых для реализации интеллектуальной системы. Проанализированы методы распознавания и классификации транспортных объектов в видеопотоке. Разработана интеллектуальная система контроля интенсивности транспортного потока.

В разделе 41 отражены результаты разработки и внедрения архитектуры для развертывания инфраструктуры информационных услуг для общественного пассажирского транспорта. Основным вкладом этого раздела является интегрированная, формальная и автоматизированная методология для информационных служб общественного транспорта. Разработана концепция сбора данных в реальном времени и выбора эффективной модели для прогнозирования времени прибытия транспортного средства. Показано, что в результате улучшаются услуги общественного транспорта, используя данные GPS и данные, предоставляемые приложениями IoT.

В разделе 42 рассмотрены принципы и требования к проектированию кооперативных человеко-машинных интерфейсов интеллектуальных транспортных систем. Предложена архитектура системы на основе Интернета вещей и протокол взаимодействия. Рассмотрены вопросы оценки эффективности и функциональной безопасности человеко-машинных интерфейсов. Приведен прототип кооперативного интерфейса транспортной системы.

В разделе 43 представлена концептуальная архитектура флота дронов. Рассмотрены коммуникационные технологии, используемые для беспилотных летательных аппаратов. Продемонстрированы основные возможности технологии Интернета дронов. Освещены основные вопросы безопасности, связанные с использованием систем на основе Интернета дронов. Обсуждены этапы оценки риска безопасности беспилотных авиационных систем. Представлена концепция системы послеаварийного мониторинга на основе Интернета дронов, а также разработаны модели и рекомендации по обеспечению надежности для различных вариантов построения такой системы.

В разделе 44 рассмотрена инфраструктура Интернета вещей в области здравоохранения. Представлен анализ требований стандартов к инфраструктуре Интернета вещей для систем здравоохранения. Описаны существующие и перспективные технологии Интернета вещей для реализации систем здравоохранения. Показан процесс разработки и моделирования инфраструктуры Интернета вещей для систем здравоохранения.

В разделе 45 описаны проблемы безопасности и приватности IoT для систем здравоохранения. Представлены требования безопасности и приватности стандартов к таким системам. Разработана иерархическая модель кибербезопасности для этих систем. Представлен обзор отказов и атак на системы. Проанализирована инфраструктура с помощью метода анализа деревьев отказов/атак. Разработано множество марковских моделей, которое позволяет учитывать специфику устройств пользователей, каналы связи, потоки данных и вопросы безопасности этих компонентов.

В разделе 46 представлены материалы для модуля «Носимые IoT-системы для биомедицинских применений». Их можно использовать для подготовки к лекциям и самообучения. Цель раздела - дать глубокие знания принципов и решений, основанных на IoT технологий в здравоохранении и биомедицинских системах: научить разрабатывать и тестировать интеллектуальные биомедицинские устройства, выполнять анализ данных в режиме реального времени.

В разделе 47 представлены материалы для модуля «Devices with reconfigurable architecture for biomedical IoT based applications». Приводится сводная информация о болезни Паркинсона, выборе определенных физиологических показателей. Обсуждаются обзор систем мониторинга двигательных симптомов болезни Паркинсона, датчиков, приборов, оборудования, параметров обнаружения и методов анализа данных. Представлена архитектура системы, функциональность, основные характеристики, а также методика обработки данных. Представлен проект разработанной системы, а именно: мобильное приложение, тесты, методики сбора, передачи и обработки данных.

В 48 разделе рассматриваются основные принципы применения Интернета вещей в различных сельскохозяйственных технологиях, таких как, управление состоянием искусственных экологических систем, таких как, теплицы или ирригационные систем, мониторинг состояния погодных условий и состояния посевов на открытом грунте. Проанализированы особенности используемых датчиков и измеряемых физических параметров, основные методы обработки полученной от датчиков информации.

В разделе 49 представлены материалы для модуля «IoT для систем мониторинга экологии, безопасности и охраны». Дан обзор исследований датчиков IoT для мониторинга окружающей среды и аналитических методов для различных IoT систем для мониторинга воды. Рассматриваются перспективы и проблемы разработки IoT систем мониторинга качества воды, в частности анализируются: параметры, измеренные для всех типов водных объектов; инструменты сбора данных и возможности сосуществования различных систем IoT, участвующих в управлении водными объектами. Дана разработка собственной IoT-системы, включая: аппаратные и программные средства, приборную панель для онлайн-мониторинга водных объектов, а также управление водными ресурсами посредством IoT (сбор, обобщение и анализ данных о качестве воды в режиме реального времени, применение систем управления для анализа больших наборов данных).

В разделе 50 предложена классификация систем радиационного мониторинга и проанализированы их структуры. Описана общая структура и основные принципы создания многоверсионной системы послеаварийного мониторинга на основе технологии Интернета дронов. Построены структурные схемы надежности этой системы и ее подсистем для различных вариантов использования датчиков, организации передачи данных и способов принятия решений. Разработаны модели надежности системы и ее подсистем, сформулированы практические рекомендации по выбору структур и реализации систем мониторинга на основе Интернета дронов.

В разделе 51 рассматриваются теоретические и практические аспекты системы физической безопасности (СФБ) зданий и кампусов на базе Интернета вещей. Поясняется необходимость внедрения СФБ, предлагаются структуры и подходы к их разработке и внедрению на основе IoT. Описана методика PSMECA для оценки критичности отказов СФБ.

В разделе 52 рассмотрены структуры, модели и технологии для разработки промышленных IoT систем. Проанализированы основные тенденции и особенности промышленных IoT системах, базируясь на большом числе IoT применений. Кроме того, рассматриваются программные компоненты и протоколы проводных и беспроводных технологий для построения IoT сетей. Анализируются проблемы безопасности промышленных IoT систем: основные типы атак, стандарты шифрования данных и политики безопасности.

В разделе 53 рассмотрены методы и средства для проектирования, модернизации и внедрения промышленных IoT систем. Дается описание IoT систем управления и мониторинга для плавучих доков, процессов разработки и внедрения IoT систем. Подробно проанализированы аппаратно-программные средства для реализации IoT систем управления и мониторинга. Рассматриваются подходы к модернизации сложных объектов в промышленных IoT системах для пирозлизного комплекса и промышленного робота с адаптивным захватом.

Раздел 54 посвящен внедрению и использованию IoT технологий в авиации, в частности, диагностике авиационных двигателей и летательных аппаратов. Учитывая большой объем данных, характеризующих техническое состояние авиационной системы, используется технология их облачного хранения и передачи данных. На ее основе реализована стратегия применения нейронных сетей для анализа данных, принятия решения и удаленного управления объектом диагностики. Внедрение IoT технологий и аппарата нейронных сетей позволяет снизить стоимость тестирования и обслуживания оборудования, предотвратить фатальные отказы и сохранить человеческие жизни.

В разделе 55 рассматриваются вопросы оптимизации аппаратных затрат устройства управления узлом индустриальной IoT-системы, реализованного микропрограммным автоматом (МПА). Описан принцип операционного преобразования кодов состояний, в соответствии с которым функция переходов МПА имплементируется операционным автоматом (ОА). Рассмотрены вопросы структурной организации, синтеза и определения эффективности МПА с ОА переходов. Формулируются задачи по применению описанных методов для улучшения характеристик устройств управления известных производителей оборудования индустриальных IoT-систем.

Цель, стратегия и ландшафт движения Индустрия 4.0 в Украине проанализированы в разделе 56. Рассмотрены задачи и направления деятельности Ассоциации предприятий промышленной автоматизации Украины (АППАУ), являющейся драйвером движения Индустрия 4.0. Обсуждаются вызовы внедрения индустриального Интернета вещей в контексте движения Индустрия 4.0. Описаны топ-тренды технологий по результатам анализа компании Gartner (intelligence, autonomy, mesh). Анализируются система управления интегрированной IT-безопасностью предприятий Индустрия 4.0, сущность и будущие тренды направления Индустрия 5.0.

Роман Маркович Бабаков, Тетяна Олександрівна Білобородова,
Андрій Олександрович Бойко, Віктор Володимирович Бушер,
Євген Віталійович Брежнев, Павло Євгенович Биковий,
Марина Володимирівна Деркач, Збігнєв Іванович Домбровський, Сергій Ілліч Доценко,
Олександр Валентинович Дрозд, Герман Володимирович Фесенко,
Олександр Сергійович Герасін, Григорій Михайлович Гладій,
Олег Олександрович Ілляшенко, Вячеслав Сергійович Харченко,
Володимир Володимирович Кочан, Марина Олександрівна Колісник,
Юрій Пантелейович Кондратенко, Олексій Володимирович Коробко,
Олексій Валерійович Козлов, Ярослав Михайлович Крайник, Яна Олександрівна Критська,
Сергій Дмитрович Леощенко, Дмитро Андрійович Масвський, Олена Юріївна Масвська,
Олександр Миколайович Мартинюк, Сергій Володимирович Моршавка,
Максим Павлович Мусієнко, Андрій Олександрович Олійник,
Олександр Олександрович Оршов, Олександр Романович Осолінський,
Анжеліка Володимирівна Пархоменко, Дмитро Вікторович Павленко, Анатолій
Олексійович Саченко, Інна Сергіївна Скарга-Бандурова,
Олександр Олександрович Солов'єв, Анастасія Олександрівна Стадник,
Анастасія Андріївна Стрелкіна, Сергій Олександрович Субботін,
Андрій Миколайович Топалов, Дмитро Дмитрович Узун, Аль-хафаджі Ахмед Валід,
Олександр Володимирович Юрчак, Діана Іванівна Загородня, Ірина Миколаївна Журавська

Інтернет речей для індустріальних і гуманітарних застосунків.

Том 3. Оцінювання та впровадження

(англійською мовою)

Редактор *Харченко В.С.*

Комп'ютерна верстка *Ілляшенко О.О.*

Зв. план, 2019

Підписаний до друку 22.08.2019

Формат 60x84 1/16. Папір офс. No2. Офс. друк.

Умов. друк. арк. 53,36. Обл.-вид. л. 57,38. Наклад 150 прим.

Замовлення 220819_3

Національний аерокосмічний університет ім. М. Є. Жуковського

"Харківський авіаційний інститут"

61070, Харків-70, вул. Чкалова, 17

<http://www.khai.edu>

Випускаючий редактор: ФОП Голембовська О.О.

03049, Київ, Повітрофлотський пр-кт, б. 3, к. 32.

Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру видавців,
виготовлювачів і розповсюджувачів видавничої продукції

серія ДК No 5120 від 08.06.2016 р.

Видавець: ТОВ «Видавництво «Юстон»

01034, м. Київ, вул. О. Гончара, 36-а, тел.: +38 044 360 22 66

www.yuston.com.ua

Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру видавців,
виготовлювачів і розповсюджувачів видавничої продукції

серія ДК No 497 від 09.09.2015 р.