



**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

173 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.Iliashenko, 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-CBHE-JP

2019

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-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.

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. Масвський, 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.

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.

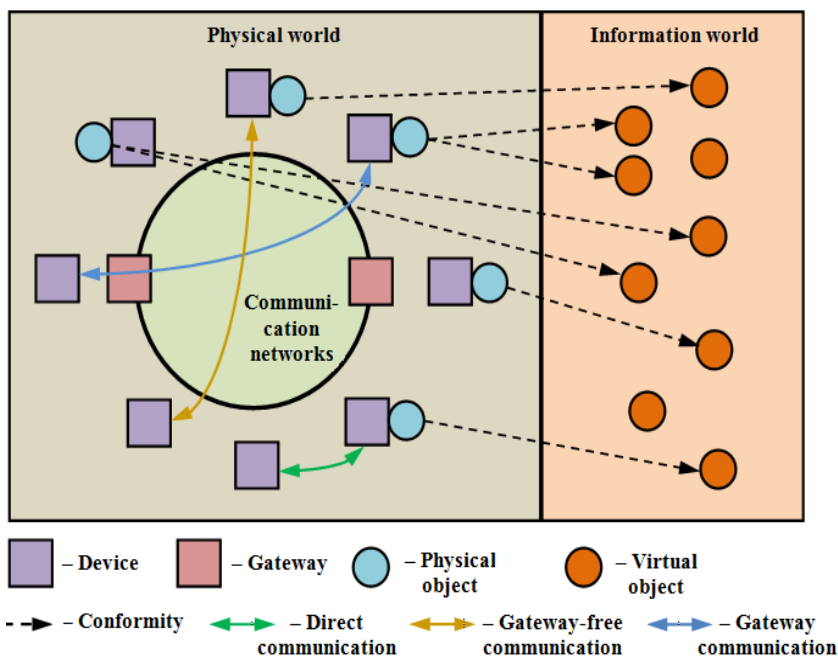


Fig. 52.1 – Scheme of reflection of physical and virtual things

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.

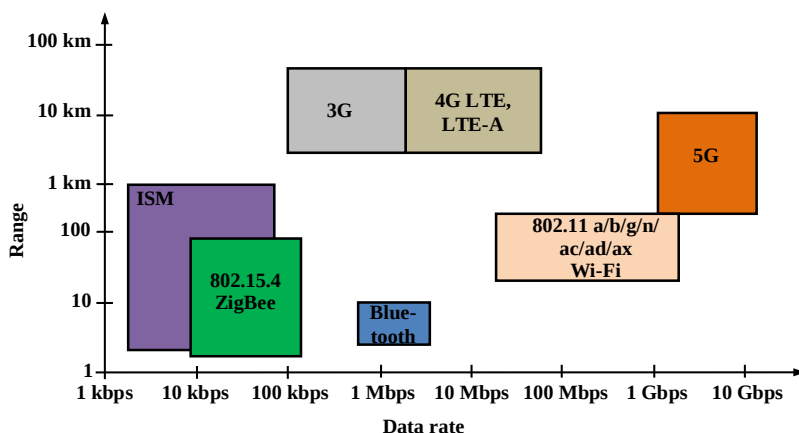


Fig. 52.2 – Graph of speed and range of main wireless networks in terms of direct visibility

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 stigmergic 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).

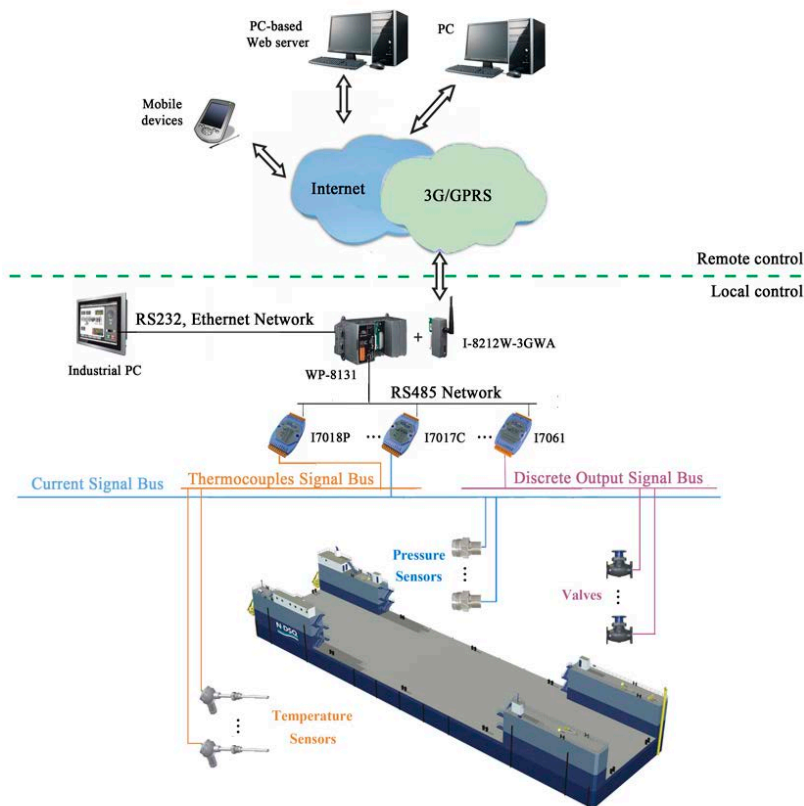


Fig. 53.1 – Functional structure of the IoT-based control and monitoring system for the floating dock

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).

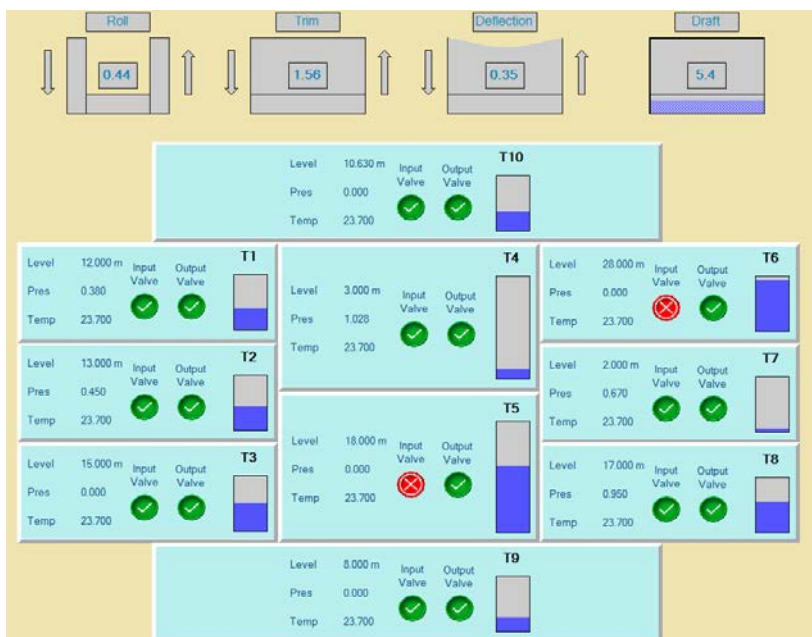


Fig. 53.2 – Human-machine interface of the industrial IoT-based control and monitoring system for floating dock

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.

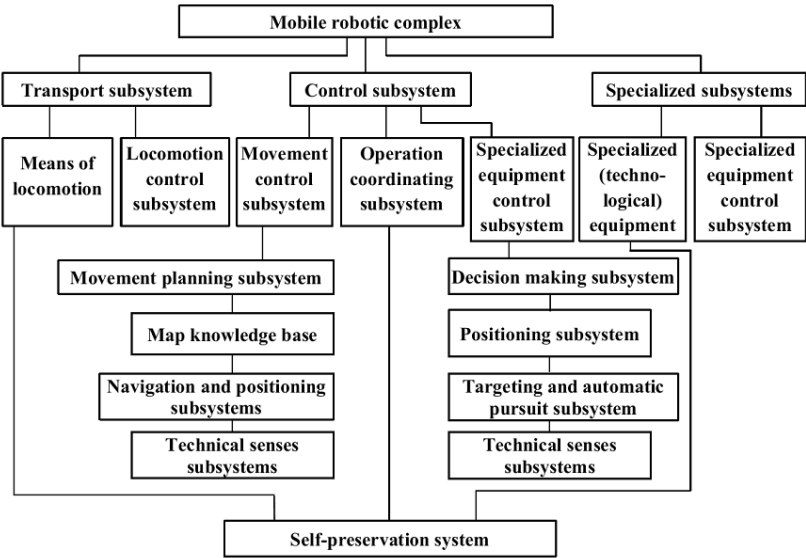


Fig. 53.3 – Generalized structure of a mobile robotic complex

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;

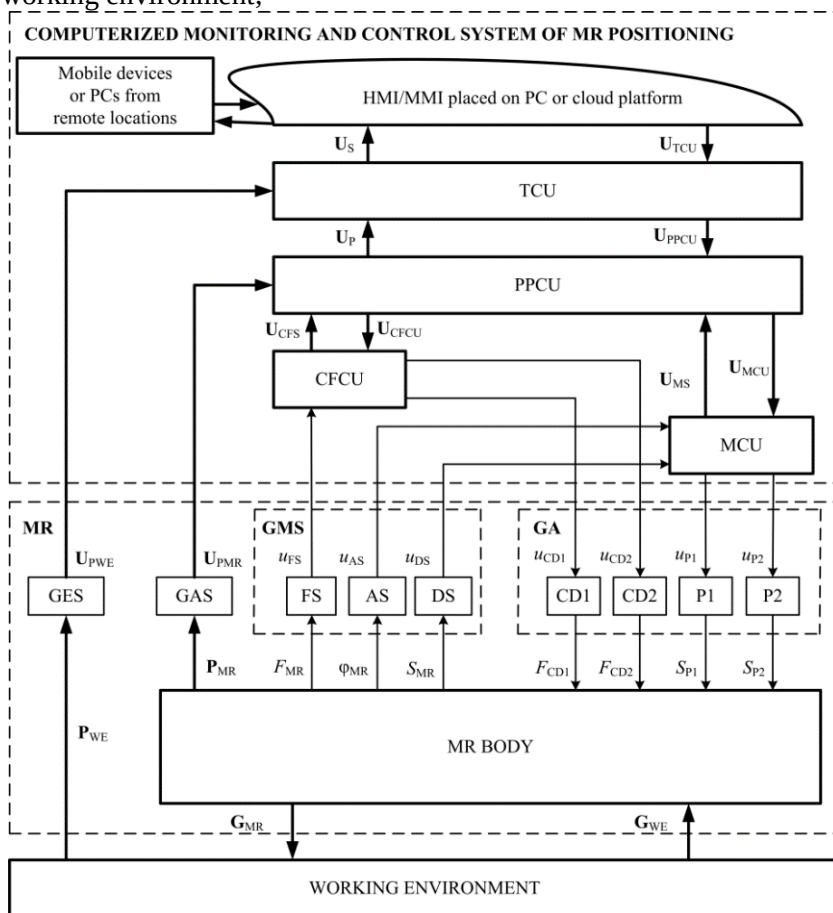


Fig. 53.4 – Functional structure of the IoT-based system of monitoring and control of MR positioning

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; $\mathbf{U}_{CFS}$ – the output signals of the clamping force sensor; $\mathbf{U}_{CFCU}$ – the control signals for the MR's clamping force control unit; $\mathbf{U}_{MS}$ – the output signals of the MR's movement sensors (angle sensor and linear displacement sensor); $\mathbf{U}_{MCU}$ – the control signals for the MR's movement control unit; $\mathbf{U}_P$ – the output signals of the MR's main operating parameters; $\mathbf{U}_{PPCU}$ – the control signals for the positioning programming control unit; $\mathbf{U}_S$ – the output signals of the sensors of the MR's main operating parameters considering the state of the working environment; $\mathbf{U}_{TCU}$ – 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.

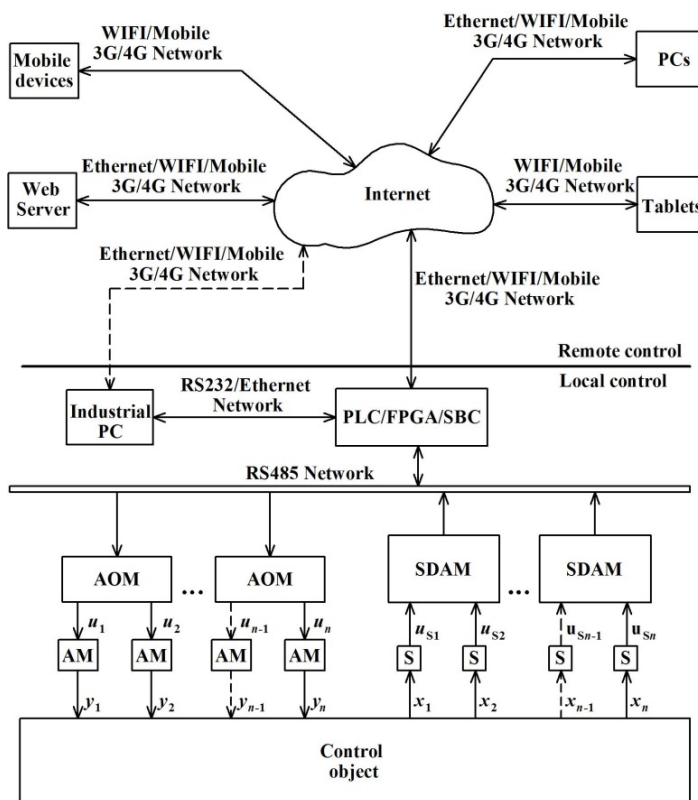


Fig. 53.5 – Basic diagram of the generalized industrial IoT-based system for complex industrial objects and processes based on IoT approach

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.

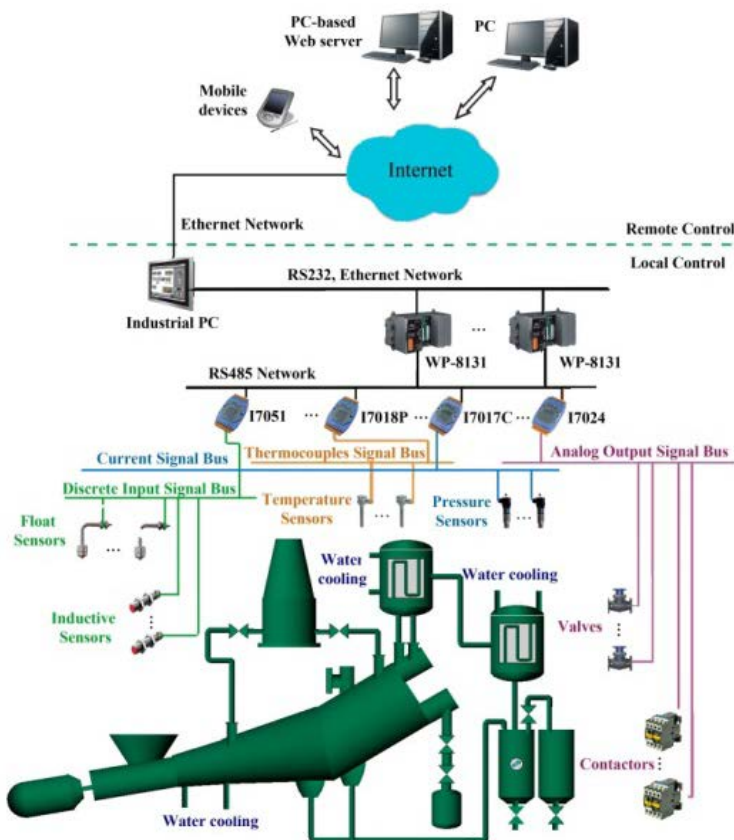


Fig. 53.6 – Functional structure of industrial IoT-based control and monitoring system of specialized pyrolysis complex

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.

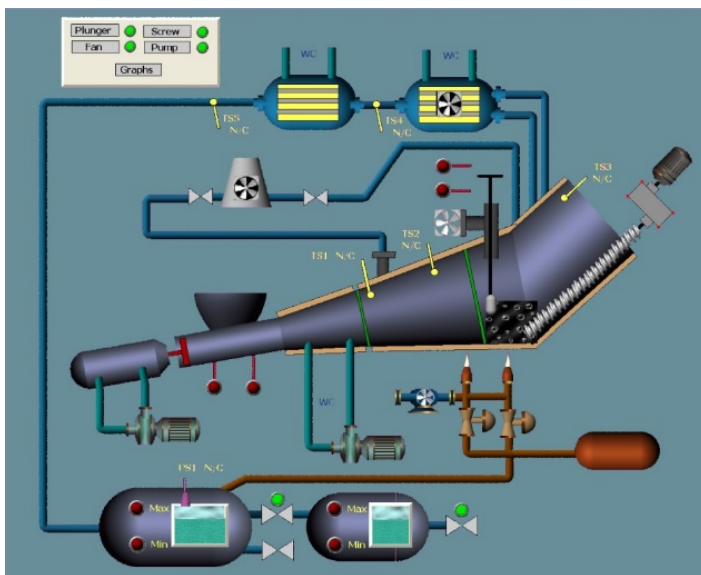


Fig. 53.7 – Human-machine interface of industrial IoT-based control and monitoring system of specialized pyrolysis complex

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].

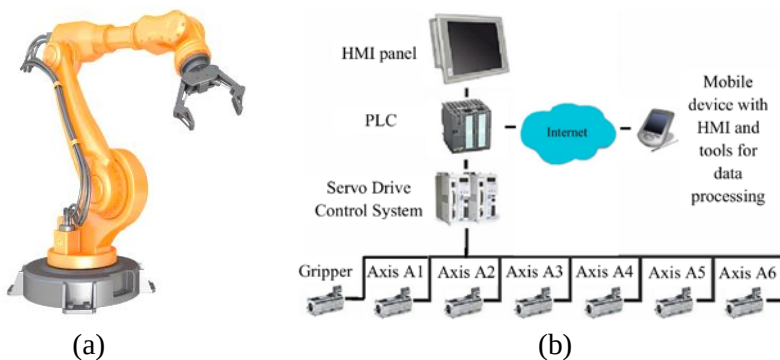


Fig. 53.8 – Robot manipulator: appearance (a) and structure of its control system (b)

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.

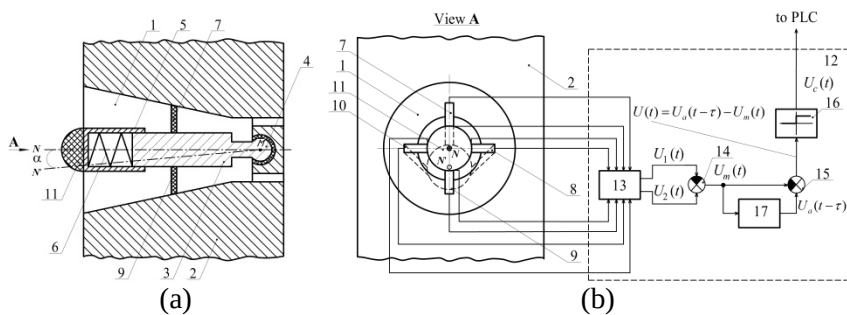


Fig. 53.9 – SDS with electro-conductive plates: mechanical (a) and electronic (b) components: 1 – conical groove; 2 – adaptive robot gripper sponge; 3 – rod; 4 – spherical hinge; 5 – tip; 6 – spring; 7,8,9,10 – plates made of conductive rubber; 11 – tip working surface; 12 – clamping force correction 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 Wheatstone 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 Ricerche - 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.