UDC 004.056

V.B. Dudykevych, G.V. Mykytyn, T.B. Kret

Lviv Polytechnic National University, Lviv

THE CONCEPT OF CREATION OF MULTI-LEVEL COMPLEX SYSTEM OF CYBER-PHYSICAL SYSTEMS SAFETY

On the basis of systematic and synergetic approaches there has been elaborated the paradigm and the concept of creation of multi-level complex system of safety (CSS) of cyber-physical systems (CPS), which aims to create the conceptual bases of protected interaction of levels and components within the context of "privacy - integrity - authenticity" according to the stages of creation and implementation of CPS, as a large and reconfigured universal platform, for the implementation of the complex of functional problems in subject areas.

Keywords: *cyber-physical system, cyberspace, communication environment, physical space, complex systems of safety, paradigm, concept.*

Introduction

The creation of approaches, methods and technologies of cyber-physical systems formation, particularly in terms of interaction with segments of processing and protection of information, is an actual focus area in the context of solving the scientific, technical, social and economic tasks of the main vectors - doctrine of information security of Ukraine, national paradigm of sustainable development of Ukraine, military (defense) doctrine of Ukraine. Development of methodological bases of information protection in CPS, processing of measurement data are important in the context of security of the system "control of target objects - data processing - management" and provide grounds for effective implementation of the complex of tasks according to the safety vector of the Strategy for Sustainable Development "Ukraine - 2020" and systemic solution of scientific tasks of the EU Framework Programme for Research and Innovation "Horizon - 2020".

Analysis of recent researches and publications

Cyber-physical system (CPS) – combines cyber-physical and physical spaces by integrating computational and physical processes by means of sensors and actuators. The development of CPS has been initiated by the Institute of Standards and Technologies ((NIST, USA), while the term "cyber-physical system" was proposed in 2006 by Helen Gill, USA. The development of approaches to build cyber-physical systems is actual now. In the work [1] there are presented architectural models of CPS:

1) two-component interrelation of physical and cyber technologies that interact with the person as a user, and socio-techno-economic environment;

2) three-component interrelation of physical, synergistic, cyber technologies that interact with the person as a user, and socio-techno-economic environment; There have been examined the principles of implementing CPS models: system (integral) relations; specifications based on models; developments based on platforms; calculations in real time; management based on events; services-oriented functionality; intrusiveness minimum.

There have been revealed technologies of three-component CPS implementation: cyber component is implemented as software technologies, technologies of transmission and communication, network technologies; synergistic component is implemented through digital circuits technologies, sensor technologies and networks, mini electromechanical technologies; physical component is implemented as technologies of advanced materials, advanced energy and robot technologies. In the work [2] there are presented the principles of designing the industrial cyber-physical systems in the context of architecture: connection, transformation, cyber, knowledge, configurations. In the work [3] there is proposed the universal platform for building applications cyber-physical systems: object of research and management; organization of measurement and computing processes; collection, previous processing and transmission of measurement and service information; organization and implementation of object management actions; secure exchange, processing and storage of measurement and service information; user.

There are actively discussed the areas of using CPS in the context of:

1) the creation of intellectual production, intellectual energy supply, intellectual buildings, intellectual transport, intellectual defense systems;

2) development of the Internet of things (the term was introduced by Kevin Ashton, 1999), as a network

of physical objects with embedded sensors to record and transmit data on the status of diverse objects, environments and patterns of interaction "object - environment".

The functionality of the Internet of Things in subject areas: scalability, availability, manageability, data management, safety, ease of use. Today the following things are promising: "Internet of Everything" (the term was proposed by Dave Evans, 2012), as a complex system – peoples, processes, data, technical devices in order to create the necessary and effective information level of network connections; industrial Internet (the term was introduced by the Industrial Internet Consortium: CISCO, IBM, Intel), as a complex self-configured adaptive system of the networks of sensors and smart objects, whose purpose is to connect all things, including household and industrial objects.

The level of safety of energy and defense facilities, ecological systems of the environment in the global space is conditional on designing and implementing secure multi-level cyber-physical systems. The systematic approach in building multi-level CSS of cyber-physical systems will enable protection of the information in the level of interrelation - interaction - complementarity of the structures: multi-level CPS - multi-level protection; multi-functionality of CPS - protected control, processing/exchange, management, dependability of CPS - functional and information safety and to implement synergistic effect of multi-level defense, considering the CPS as a multi-level structure that has properties of scalability and reconfiguration according to functional tasks in subject areas. The purpose of work is to build a new paradigm of the development of protected CPS, the core of which is the concept of creating CSS of cyber-physical systems and a model of the concept of CPS information safety management in order to ensure the secure exchange of information in the context of: privacy – integrity – authenticity.

The paradigm and concept of creating a multi-level CSS of cyber-physical systems

The paradigm "multi-level CPS - multi-level CSS". The cyber-physical system combines cyber and physical spaces (CS, PS) by integrating computational and physical processes through sensors and actuators. The multi-level CPS according to the structure "architecture - features - requirements - use": physical space, communication environment (CE) cyberspace - control, processing, management - dependability, reference model OSI, requirements for sensors - scalability, reconfiguration in the context of a multifunctional research of the complex of the factors of impacts on diverse objects of subject areas. The structure of the paradigm of the multi-level complex system of safety of CPS is shown in fig. 1. According to the structure of the paradigm: complex systems of safety CS, CE, PS as a sub-system of CSS protection: access control; identification and authentication; cryptography; auditing; ensuring the integrity, confidentiality, authenticity of information. The system of CPS complex safety management: the model "plan - do - check - act"; the concept "object - threat - protection".

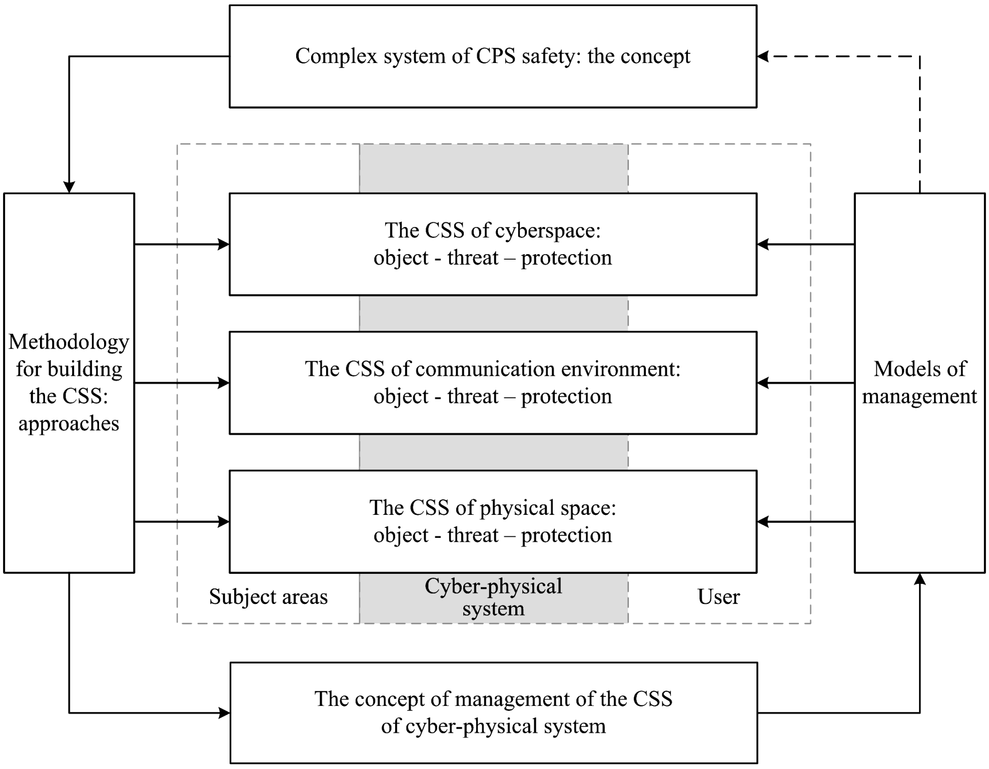

Complex system of CPS safety: the concept
Methodology for building the CSS: approaches
The CSS of cyberspace: object - threat – protection
The CSS of communication environment: object - threat – protection
The CSS of physical space: object - threat – protection
Models of management
Subject areas
Cyber-physical system
User
The concept of management of the CSS of cyber-physical system

Fig. 1. The structure of the paradigm of building a multi-level CSS of cyber-physical systems

Methodological approaches to create the CSS of CPS: systematic approach - principles of hierarchy, structure, integrity that provide grounds for the creation of a complex system of CPS with the optimal combination of: normative-methodical, organizational, informational, technological (hardware), software in the stages of life cycle of the automated systems; synergistic approach - a property of emergency that shows one of the faces of the integrity of information protection in CPS:

assumes that there are properties that are peculiar to the complex system of CPS safety in general, but are not peculiar to its individual elements - complex systems of safety of the CS, CE, PS.

The concept of creating a multi-level CSS of cyber-physical system is shown in fig. 2.

The structure of the concept is conditional on the structure: classification of threats/attacks - formation of protection criteria - creation of a multi-level CSS of the CPS - safety policy model argumentation - choosing the method of evaluation of CPS safety state [4, 5]. The classification: of threats based on characteristics; of attacks based on the final result, the method of implementation; methods of classification of STRIDE threats based on categories (substitution of objects, data modification, denial of authorship, disclosure, denial of servicing, increasing privileges - creating a model of threats "information/CPS - sources of threats arising - ways to implement the threat."

The criteria for information safety in the CPS: architecture of confidentiality, integrity, availability, observability, guarantees.

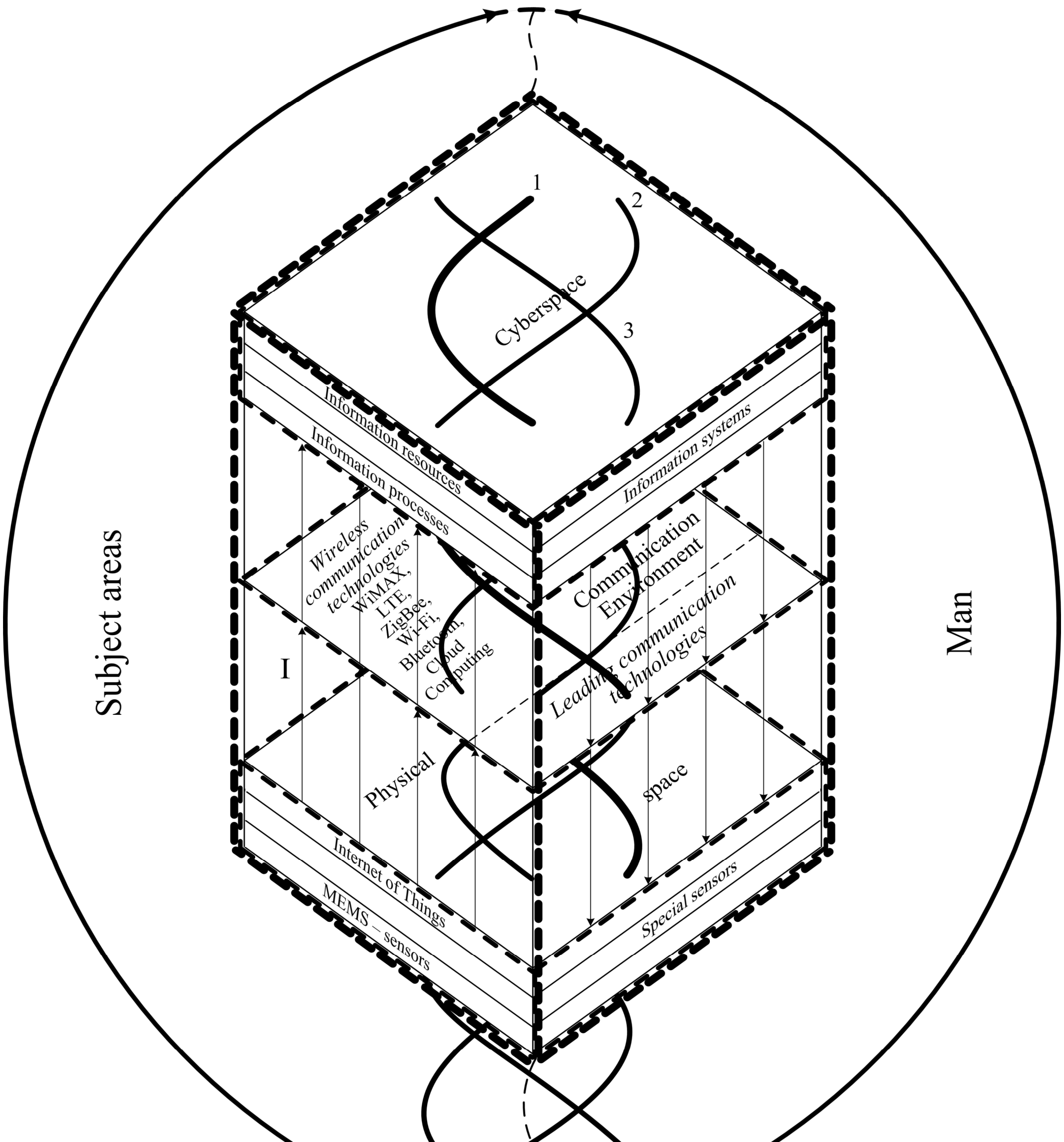


Fig. 2. The structure of the concept of building a multi-level CSS of the cyber-physical systems:
I ——→ – information (selection, management); ▬ ▬ ▬ – CSS of CS, CE, PS;
▬▬▬ – CSS of the CPS; 1.2.3 – threats for CS, CE, PS respectively

The creation of multi-level CPS: guidelines for the development of a technical task on creating the CSS - argumentation of the requirements for a complex system of safety in the context of protection from unauthorized access and guarantees. The argumentation of CPS safety policy: analysis of models and selection criteria. The evaluation of CPS protection level: use of standardized methods of dependability [6].

Complex systems of CS safety are formed on the basis of the concept of "object - threat - protection" according to segments: information resources - databases, knowledge bases, base models, arrays of information, storage place for data; automated systems - model of dependability; model of multi-level and multi-tier protection; information processes - phases, operations, processing.

Complex systems of CE safety are based on the concept of "object - threat - protection" according to segments: wireless communication technologies - ZigBee, Wi-Fi, Bluetooth, WiMAX, LTE, Cloud Computing: model of open systems interconnection (OSI); structure "information security - data integrity - reliability - level of servicing - utilization of information"; leading communication technologies - optical fiber systems, coaxial (copper) systems: general specifications and requirements.

Complex systems of PS are based on the concept of "object - threat - protection" according to segments: sensors embedded in disparate objects (Internet of Things); special sensors embedded in devices (electronic and aerospace search, remote monitoring of the parameters of ecosystems of the planet, monitoring the state of emergency, identifying the movable and stationary objects in military situations, finding objects); MEMS-sensors (a wide range of applications, particularly in safety systems) - requirements to the parameters of sensors in order to ensure the accuracy of selection, registration and transmission of the information in CS, measurement data processing by the systems and transmission of the information for its management in PS.

The concept of management of the CSS of cyber-physical systems is based on methodology development: analysis of models and methods - argumentation of their use in the system of management of information safety of multi-level CPS - corrective action in the context of modification of the structure of the concept of CPS of cyber-physical systems [7].

Elements of complex system of CS cyber-physical system safety

In the context of the creation of complex systems of CS cyber-physical systems safety let's consider the concept of "object - threat - protection" for Zigbee sensor network according to the levels of OSI model (Tables 1, 2). In the Table 2 there are presented the elements of CSS of communication environment of CPS at OSI levels of Zigbee sensor network.

Table 1

Model OSI: ZigBee

Levels of the model OSI: Zigbee (IEEE 802.15.4)	Network/Protocol	Functions
Application (1)	APL (APS, ZDO i Application Objects) ZigBee	Messages transmission; devices detection; defining the role of devices.
Presentation (2)	-	Organizing the data that are transmitted from application level to the network; ensuring the unification of data when they are exchanged between platforms with different encoding schemes; control of data compression and encryption.
Session (3)	-	Facilitating the exchange of information by establishing, support, synchronization, management and termination of a possible identification and authentication of the parties.
Transport (4)	-	Packages and datagrams delivery from a sender to a recipient; targeting increased productivity of information transmission.
Network (5)	NWK ZigBee	Safety, routing; registration in the network of a new device and its exclusion from the network; ensuring safety when the frames are transmitted; indication of frame route to the destination; routing between devices in the network; identifying the nearest neighbors in the network; memorization of necessary information about neighboring nodes.
Link (6)	LLC IEEE 802.15.4	CSMA/CA, beacons transmission; synchronization; development and delivery of a frame without errors.
	SSCS IEEE 802.15.4	
	MAC IEEE 802.15.4	
Physical (7)	PHY IEEE 802.15.4	Physical link between final workstations.

Table 2

The concept of "object - threat - protection": Zigbee

Zigbee/ OSI-level	Threat	Protection/ Standards: ISO/IEC 7498-1:2004; ISO 7498-2:2004; ISO/IEC 27033-1:2009; ISO/IEC 27033-2:2012.
1	Using free resources and programs of unknown origin; disadvantages of software; backdoors availability; traversal of standard means of safety management; insufficient control of protection means by the principle "all or nothing", too complicated mechanism of safety control; software failures at high loads.	The control at the level of programs determines and provides access to resources; simple and transparent mechanism of safety ensuring, with the purpose of avoiding the difficulties in configuring; implementation of cryptographic and antivirus protection of data.
2	Poor data processing can result in program crashing; unintentional use of external data that are entered in the context of control can lead to remote manipulation/ leak of data; cryptographic disadvantages can be used for traversing the protection of privacy.	Checking the data that are entered in the program; control of users' actions and management functions; continuous overview of cryptography solutions for the provision of current safety tasks regarding the threat that are constantly updated.
3	Weak or missing authentication mechanisms; transmission during a session of the information (username, password) in clear text, that allows its interception and unauthorized use; the identification of a session may be subject to spoofing and hijacking; leak of information based on authentication failures; the attack on credentials to access in case of an unlimited number of attempts for establishing a session.	The encrypted exchange and storage of passwords; limited validity period for passwords and users' powers; protection of the information on session identification using cryptographic means; limitation of unsuccessful attempts to establish a session using the synchronization mechanism, but not a blocking one.-
4	Incorrect transmission of packages; differences in the implementation of the transport protocol allow to carry out unauthorized access; transport level overload due to the large number of requests to port numbers restricts the opportunities for effective filtering of traffic; packages transmission mechanisms can be subject to spoofing and attacks based on the existing packages and lead to destruction/ seizure of the control over network.	Hard firewall rules limit the access to certain information transmission protocols such as the number of TCP/UDP ports; packages checking by the firewall based on the analysis of the content and connection allows to close the access to the malicious packages; strengthening mechanisms for identifying the connection to prevent the attack and seizure of the control over network.
5	Route spoofing is the spread of network false topology; IP spoofing as a source of erroneous decision after the action of harmful packages; one-time identification problems.	Applying the policies of routes management: stringent filters for routes and anti-spoofing; using network firewalls with powerful filtering policies; software monitoring, for minimizing possible abuses.
6	MAC-address spoofing; VLAN technologies traversal; using the errors of algorithm; Spanning Tree for the transmission of the packages in unending iteration; unauthorized connection to the network; flooding by switches of all VLAN ports.	MAC-address filtering; not to use VLAN networks for information protection; physical isolation of different zones of the network using firewalls; protection of wireless networks: embedded encryption, authentication, MAC-address filtering
7	Loss of power; physical theft of data and equipment; physical damage/destruction of data and equipment; unauthorized changes in the functional environment; switching-off the physical channels of data transmission; covert interception of data from a keyboard or other means of entering the information.	Closing the network perimeter and corpuses; electronic locking mechanism for the registration and authorization, video and audio surveillance; using pin-codes and passwords; biometric authentication systems; electromagnetic shielding.

The Zigbee sensor network research has been conducted on the equipment DRF2618A (Fig. 3), which operates on the basis of the Zigbee 2007 protocol.

This device supports two modes of operation: a coordinator and router, with radio frequency 2460 MHz (default), and 2405 - 2480 MHz, at a pitch of 5 MHz.

Fig. 3. Device DRF2618A

The difference between the coordinator and the router is in their hierarchical placement. The coordinator is hierarchically at the highest level and manages the network. The router in its turn can be considered both intermediate device and final data recipient that is directly subordinate to the coordinator or another router.

The communication between the coordinator and routers is possible by two methods:

1) star network topology where the data package is transmitted to all routers simultaneously (fig. 4);

2) point-to-point topology where the data package is transmitted to the final router (fig. 5).

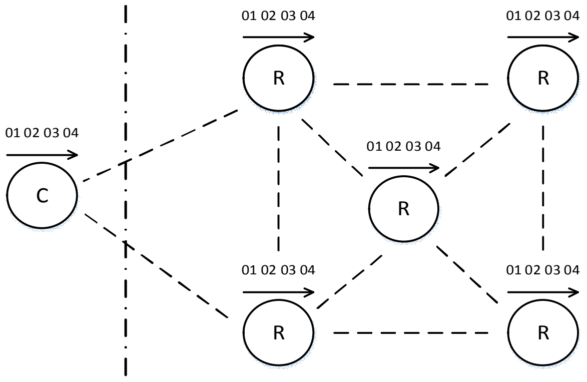


Fig. 4. Data transmission in a star network topology

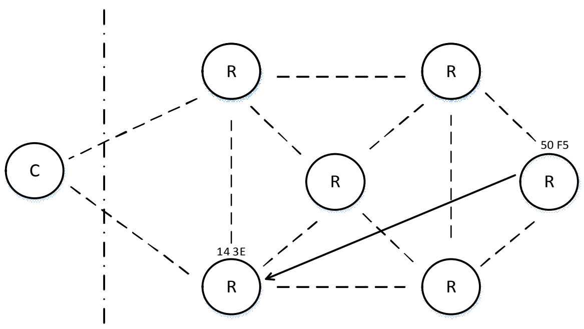


Fig. 5. Point-to-point data transmission

Star network data transmission is the main function for the devices of series DRF. Different flavors of data transmission between nodes:

1) information is transmitted through the channel (if the first byte is not 0xFE, 0xFD or 0xFC);

2) the coordinator, which receives information automatically circulates it to all nodes, similarly, when the node receives the information, then it forwards it to the coordinator;

3) transmission can occur between any node and coordinator.

Point-to-point data transmission allows a connection between any two network nodes. When the coordinator is switched there may be possible to transfer data between routers. The router's address remains unchanged since its network connection.

For ensuring the Zigbee functionality let's consider the steps of sensor network control. During the first connection it is necessary to (Fig. 6):

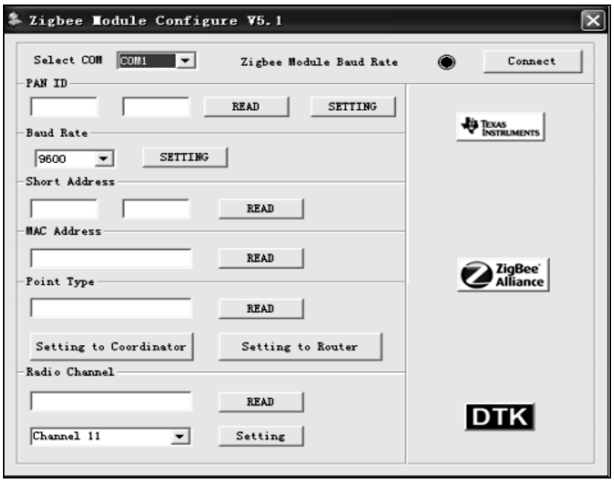
1) choose one module and change its mode to coordinator and restart it.

2) change coordinator's PAN ID and arbitrary address (for example, 0x1234).

3) choose a different module, change its mode on the router and turn it off.

4) turn coordinator (gives one long signal about turning on the LED and blinks shortly).

5) turn the router on, after 3 seconds it will be connected to the network, that will be seen from the two long glows of light diodes).



Zigbee Iodule Configure V5.1

Select COM: COM1

Baud Rate: 9600

Radio Channel: Channel 11

Fig. 6. The program window where mode settings and PAN ID are set

For visualizing the network there is used ZigBee Sensor Monitor Program, which shows the network topology while clicking on each device the button TEST (when sending test signal).

As shown in fig. 7, a, the second router connects to the coordinator through the first one, while the first router is not active and only sends signals of the second. In fig. 7, b one can see a similar picture, but in this case the first router is active (sends its own test signal). As shown in fig. 7, c, the two routers are active and connected to the coordinator, while the third one is connected to the coordinator through one of them.

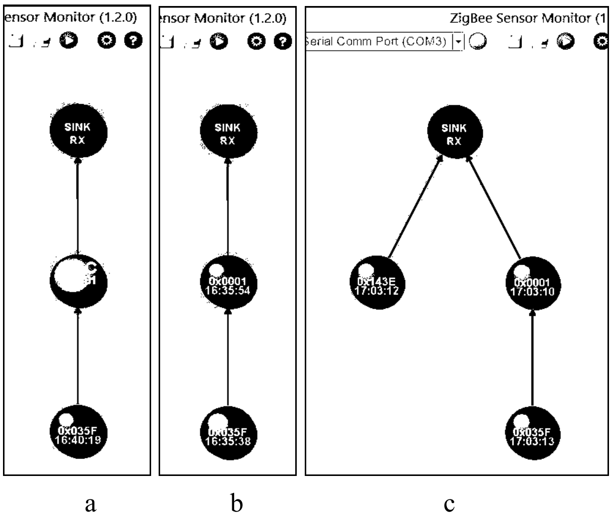


Fig. 7: a – connection of the second router through the first one; b – sending a signal from the second router through the first active router; c – connection to the coordinator through one of the active routers

Conclusion

There has been developed a new paradigm of building the protected CPS based on methodological approaches - systematic and synergetic. There has been created the concept of developing CSS of cyber-physical systems that provides systematic and synergetic effects of information protection in accordance with the architecture: cyberspace – communication environment - physical space.

There has been developed the concept of Zigbee "object - threat - protection", as components of the communication environment of CPS: there have been considered the data transmission schemes, has been demonstrated test control of sensor network by OSI model. The developed paradigm and concept are transformed into different subject areas and can be modified at the level of structure "multi-level CPS - multi-level protection".

References

1. Imre Horváth, Bart H. M. Gerritsen. Cyber-physical systems: concepts, technologies and implementation principles // 9th International Symposium on Tools and Methods of Competitive Engineering (TMCE), May 7–11, 2012, Karlsruhe, Germany.

2. Jay Lee, Behrad Bagheri, Hung-An Kao. A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems // NSF Industry/University Cooperative Research Center on Intelligent Maintenance Systems (IMS), University of Cincinnati, Cincinnati, OH, United States, 2014.

3. Мельник А.О. Кібер-фізичні системи: проблеми створення та напрями розвитку / А.О. Мельник // Вісник НУ "Львівська політехніка". Комп'ютерні системи та мережі. – 2014. – № 806. – С. 154-161.

4. Space product assurance. Methods and techniques to support the assessment of software dependability and safety. - ECSS-Q-80-03, 2006. – 122 p.

5. Information processing systems. Open Systems Interconnection. Basic Reference Model - Part 2: Security Architecture, ISO 7498-2:1989. – 32 p.

6. National Institute of Standards and Technology Special Publication 800-53. -NIST SP 800-53, Rev. 4, 2013. – 462 p.

7. Information technology. Telecommunications and information exchange between systems. Security framework for ubiquitous sensor networks: ISO/IEC 29180:2012. – 34 p.

Надійшла до редколегії 18.02.2015

Рецензент: д-р техн. наук, ст. наук. співр. С.Г. Семенов, Національний технічний університет «ХПІ», Харків.

КОНЦЕПЦІЯ СТВОРЕННЯ БАГАТОРІВНЕВОЇ КОМПЛЕКСНОЇ СИСТЕМИ БЕЗПЕКИ КІБЕРФІЗИЧНИХ СИСТЕМ

В.Б. Дудикевич, Г.В. Микитин, Т.Б. Крет

На основі системного і синергетичного підходів розроблено парадигму та концепцію створення багаторівневої комплексної системи безпеки (КСБ) кібер-фізичних систем (КФС), яка спрямована на створення концептуальних основ захищеної взаємодії рівнів та компонентів у просторі "конфіденційність – цілісність – автентичність" відповідно до етапів створення та реалізації КФС, як масштабованої та конфігурованої універсальної платформи, для реалізації комплексу функціональних задач у предметних сферах.

Ключові слова: *кіберфізична система, кібернетичний простір, комунікаційне середовище, фізичний простір, комплексні системи безпеки, парадигма, концепція.*

КОНЦЕПЦИЯ СОЗДАНИЯ МНОГОУРОВНЕВОЙ КОМПЛЕКСНОЙ СИСТЕМЫ БЕЗОПАСНОСТИ КИБЕРФИЗИЧЕСКИХ СИСТЕМ

В.Б. Дудыкевич, Г.В. Микитин, Т.Б. Крет

На основе системного и синергетического подходов разработаны парадигма и концепция создания многоуровневой комплексной системы безопасности (КСБ) киберфизических систем (КФС), которая направлена на создание концептуальных основ защищенного взаимодействия уровней и компонентов в пространстве "конфиденциальность - целостность - аутентичность" в соответствии с этапами создания и реализации КФС, как масштабируемой и конфигурируемой универсальной платформы для реализации комплекса функциональных задач в предметных областях.

Ключевые слова: *киберфизическая система, кибернетическое пространство, коммуникационная среда, физическое пространство, комплексные системы безопасности, парадигма, концепция.*