Information Technology and Management Science

doi: 10.1515/itms-2014-0019

2014 / 17

State of the Art in the Healthcare Cyber-physical Systems

Alyona Skorobogatjko [1], Andrejs Romanovs [2], Nadezhda Kunicina [3], [1-3] *Riga Technical University*

***Abstract* – For several years, experts from different fields are interested in virtual and physical world interaction opportunities. Cyber-physical systems (CPSs) are developed to integrate real physical processes and virtual computational processes. CPSs are used in multiple areas such as medicine, traffic management and security, automotive engineering, industrial and process control, energy saving, ecological monitoring and management, avionics and space equipment, industrial robots, technical infrastructure management, distributed robotic systems, protection target systems, nanotechnology and biological systems technology. CPS sensors generate the sensitive data that must be protected and shared only in a secure manner. This paper provides an overview of CPSs, their application in medicine and compliance with existing standards and possibilities for further advanced system development.**

***Keywords* – Embedded systems, healthcare cyber-physical system, sensor networks.**

I. Introduction

New competitive approach to the physical and virtual world integration with cyber-physical systems (CPSs) is one of the European Union research priorities. Cyber-physical systems will change the way people interface with systems, the same way as the Internet has transformed the way people interface with information.

The aim of the current research is to develop application strategies for cyber-physical system use in medical organizations and telemedicine. Topicality of the theme is based on the fact that cyber-physical systems are a promising area, development of which is critical for medical progress. One of the main challenges of this research is to design strategy for CPS application to be safe, secure, resistant to abnormalities and resilient in a variety of unforeseen and rapidly changing environments.

There are currently no available standards for healthcare cyber-physical systems. Therefore, it is necessary to conduct an in-depth research to identify medical systems' best practices and standards, which can be applied to healthcare cyber-physical systems.

CPS usage analysis will be performed within the framework of the research, and CPS possible application in disease prevention, diagnosis, treatment and patients' rehabilitation will be investigated. Particular attention will be paid to such essential components as usage, architecture, sensitivity, data management, data security and information exchange between multiple systems. As a result, healthcare cyber-physical system's overall requirements will be formulated and an application strategy will be developed.

This paper is organized as follows. In Section II, the definition and concept of a cyber-physical system are introduced, and the embedded system development history is overviewed. In Section III, goals and activities of this area are observed in Latvian organizations. In Section IV, examples of CPS application in different fields, including healthcare, are given. In Section V, CPS design process features are discussed. Section VI includes a brief summary and conclusion.

II. Cyber-physical System Overview

Cyber-physical systems are developed to integrate real physical processes and virtual computational processes. Many objects used in a modern daily life are cyber-physical systems. Concept of CPS is complicated, but it can be illustrated with a concept map (see Fig. 1).

The definition of cyber-physical system from Cyber-Physical Systems Week [1] is as follows: "Cyber-physical systems (CPSs) are complex engineering systems that rely on the integration of physical, computation, and communication processes to function".

Cyber-physical systems have not appeared from anywhere, they have a long history of development, which continues. This chapter is an introduction to cyber-physical systems, their history and overview of the main components and characteristics.

A. From Embedded Systems to Cyber-physical Systems

Always a growing need for different purpose information management systems leads to the optimization of computing tool design techniques. Most of the world's currently used information management systems are embedded systems and networks. They are closely related to the control or management objects.

From certain common computing system classifications, the best suited to the modern situation is the classification proposed by David Patterson and John Hennesy [2]. Their classification was guided by the use of the system. They divided computing system into 3 categories: desktop computers, servers and embedded systems. Embedded systems by the area of use are separated into:

- Automatic control systems;
- Measuring systems and systems that read information from sensors;
- Real-time "question – answer" type information systems;
- Digital data transmission systems;
- Complex real-time systems;
- Moving objects management systems;
- A general purpose computer system subsystems;
- Multimedia systems.

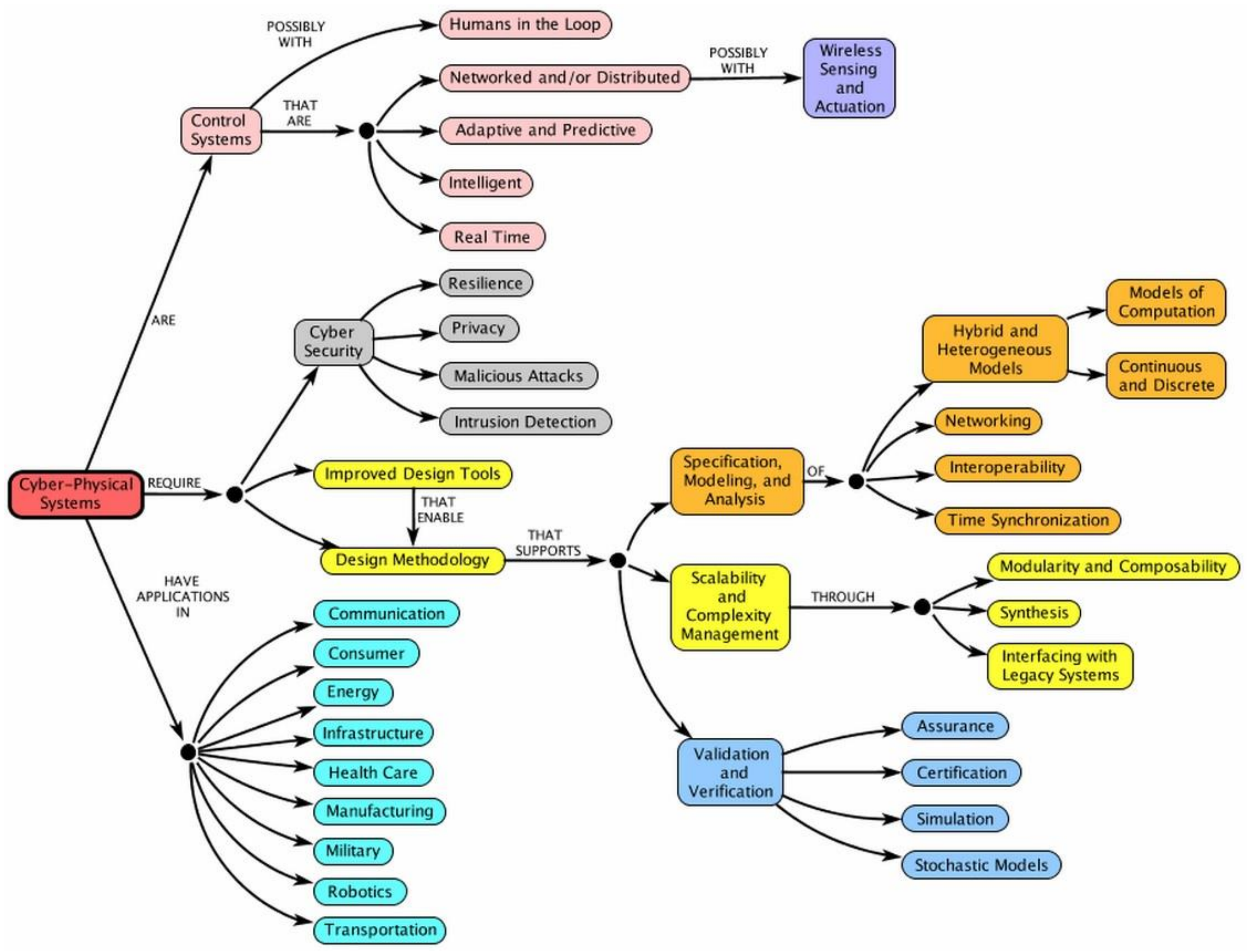

Fig. 1. A concept map of cyber-physical systems [3].

The concept of embedded systems appeared in the early 50s and it is in rapid development even today. It is interesting to view the evolution of embedded systems:

- Information management systems, 1960s;
- Embedded computing systems, 1970s;
- Embedded distributed systems, 1990s;
- Cyber-physical systems, since 2006.

Information management system is a computing system designed for management purposes, but it is the most alienated from the control object. Integrated micro-scheme and microprocessor development led to information management system bringing directly to the management object. The world has entered the era of embedded systems. System elements are gradually becoming cheaper and their integration increases, as well as the security level and the opportunity to combine them in controlled networks.

Downturn in embedded systems' elements prices and increasing connection with physical management objects led to the appearance of cyber-physical systems.

Cyber-physical systems are specialized computing systems that interact with control or management objects. Cyber-physical systems integrate computing, communication, data storage with real world's objects and physical processes. All the above-mentioned processes must occur in real-time, in a safe, secure and efficient manner. Cyber-physical systems must be scalable, cost-effective and adaptive. Cyber-physical systems are in use in various areas, such as smart medical technologies, environmental monitoring and traffic management.

Wireless sensor networks can become an important part of cyber-physical systems, because of high sensitivity capability that is one of the main driving factors of CPS application distribution. The rapid development of WSN, medical sensors and cloud computing systems makes cyber-physical systems impressive candidates for use in inpatient and outpatient health care improvement [4]. Cloud computing maturity is a direct result of a few technologies, such as distributed computing, internet technology, system management and hardware development [5].

B. Concept of Cyber-physical Systems

Helen Gill, which at that time was the United States National Science Foundation Director of the embedded and hybrid systems sector, coined the term "cyber-physical system" in 2006. The new term highlighted NSF CPS Workshop originality. The seminar organizers sought to review the role of embedded systems, and they succeeded. They saw the overall industry trend: after a few years cyber-physical system elaboration suddenly started in the world. Many countries recognized CPS as a priority research direction.

Cyber-physical systems integrate computing and physical processes. Compared with embedded systems, much more physical components are involved in CPSs. In embedded systems, the key focus is on the computing element, but in cyber-physical systems, it is on the link between computational and physical elements. Cyber-physical system parts exchange information with each other that is why the third component – communication (see Fig. 2) is added there. For this reason, cyber-physical system is denoted by the symbol C3 (Computation, Communication and Control).

Link improvement between computational and physical elements extends CPS usage possibilities.

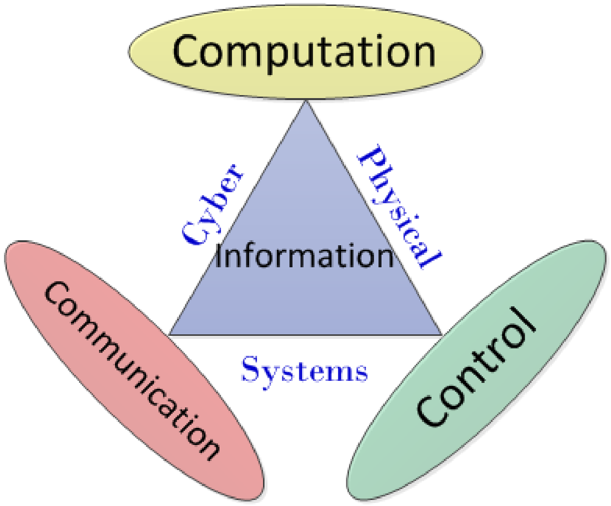

Fig. 2. Three main components of cyber-physical system [6].

III. Situation in Latvia

One of the main National Research Program aims in the period of 2014–2017 is: “to develop the scientific expertise of the next generation of ICT systems, creating a new competitive approach to the physical and virtual world integration cyber-physical systems, the development of competitive smart sensor networks and innovative hardware and software platforms, exploring and further developing competitive models based on the new information and communication technologies and their use in today’s environment”.

In the discussion within the Working Group of Smart Specialization Strategies, Modris Greitans (Director of the Electronics and Computer Science Institute) expressed the view that cyber-physical system is a large area and Latvia, as a small country, cannot overlay all aspects; however, certain aspects of this field have been studied and implemented in several institutions in Latvia with a certain specialization. Below, Latvian organizations are listed that develop cyber-physical systems:

- Electronics and Computer Science Institute: signal processing, intelligent embedded systems and their networks, testing and profiling environments;
- University of Latvia: different types of software for CFS;
- Riga Technical University: robotics and artificial intelligence, electrical and optical systems;
- Latvian University of Agriculture: biological principle-based computer-controlled systems;
- Ventspils University: smart sensor systems;
- Transport and Telecommunication Institute: smart transport systems.

These institutions do not compete among themselves but complement each other with different aspects. Together they fail to cover all the challenges in this field of research.

IV. Cyber-physical System Application

Cyber-physical systems are used in multiple areas, such as medicine, traffic management and security, automotive engineering, industrial and process control, energy saving, ecological monitoring and management, avionics and space equipment, industrial robots, technical infrastructure management, distributed robotic systems, protection target systems, nanotechnology and biological systems technology.

A. Smart Technologies

Modern construction technology enables the creation of intelligent building designed with minimum energy consumption or even without it. However, they need constant monitoring. Engineers must attach smart buildings to smart grids, and add control mechanism – cyber-physical systems [7].

Smart transport is equipped with various types of computerized embedded control systems. Cyber-physical solution use in this field makes it possible to create a full-fledged single system that will link the vehicles with other vehicles, environment and infrastructure [8]. An example of cyber-physical systems known to the general public is Google car, which does not require a driver.

B. Internet of Things and Industry 4.0

In several sources [5], [9], [10] it is predicted that within ten years almost half of the electronic devices will be connected to the World Wide Web. This network is termed as the Internet of Things. It connects not only household appliances such as refrigerators, thermostats, but also sophisticated production equipment.

Industry 4.0 concept aims at the comprehensive cyber-physical system use in manufacturing, customer relationship management and supply chain management processes, combining it all into one system. Smart manufacturing lines communicate with each other in order to optimize the production process.

Comprehensive use of cyber-physical systems for commerce, industry and public health, military and civilian purposes, makes the protection of these systems a matter of national significance. That is why embedded system security systems, mainly anomaly detection system that allows resisting spoofing and service failure type attacks, are currently actively developed [11].

C. Healthcare Cyber-physical Systems

There are hospitals, where robots already bring dishes to patients, sort mail, change bed linen and collect waste. Robotic beds transport patients to the surgery room. However, a fully automated healthcare system has not been implemented yet. Currently, a number of hospitals in the world remote operations are carried out with the help of a robotic hand and high-resolution cameras [12]; however, there is still a long way to autonomous surgery when a cyber-physical system itself, without human management, performs the operation.

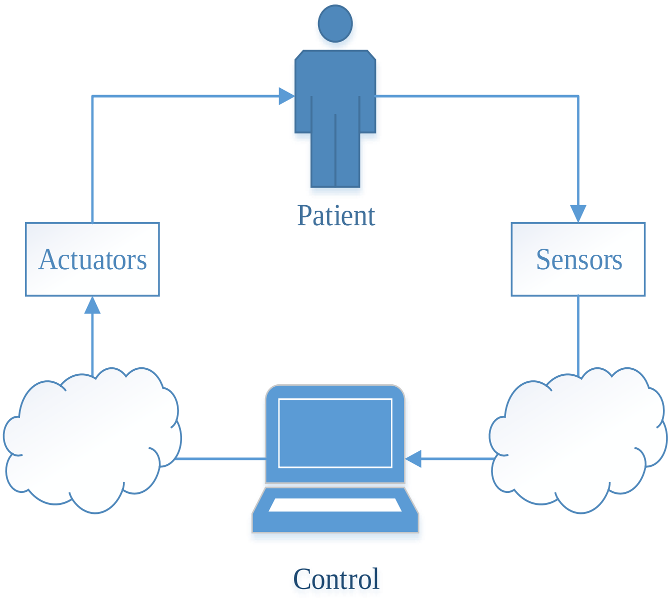

Fig. 3. An example of healthcare cyber-physical system.

Human-in-the-loop cyber-physical systems can greatly improve lives of people with special needs. Human-in-the-loop cyber-physical systems formulate opinions about the user's intentions based on his cognitive performance by analyzing data from sensors attached to the body or head. Embedded system converts these findings to robot control signals, which, thanks to robotic management mechanisms, allow users to interact with the surrounding natural environment. Example of human-in-the-loop CPS is robotic assistance systems and intelligent prosthesis [13].

From the examples above, it is clear that the cyber-physical systems are widely used all over the world in various industries, including medicine and healthcare. However, only one research was found [14], which summarizes the current situation related to the CPS application in healthcare, and it offers a detailed taxonomy.

Healthcare cyber-physical systems were categorized by application (assisted, controlled), architecture (infrastructure, data requirement, composition system), sensing (sensor type, method, parameter), data management (data integration, data storage, data processing), computation (modeling, monitoring), communication (scheduling, protocol), security (privacy, encryption), control/actuation (decision-making, mechanism).

Existing healthcare cyber-physical systems were mapped to this taxonomy, and a number of healthcare CPS groups (with several examples) were allocated: notable CPS applications (*Electronic Medical Records*, *Medical CPS and Big Data Platform*, *Smart Checklist*), daily living applications (*LiveNet*, *Fall-Detecting System*, *HipGuard*), medical status monitoring applications (*MobiHealth*, *CodeBlue*, *AlarmNet*), medication intake applications (*iCabiNET*, *iPackage*.).

Using this taxonomy and mapping, different cyber-physical systems can be categorized. In addition, it is quite convenient to use this taxonomy for formulation of new cyber-physical system requirements.

V. Design Process

Cyber-physical system, as well as any embedded system design process includes requirements management and project management, as well as test and safety plan. However, cyber-physical system development process is not possible without the involvement of a different sector professional. CPS development requires the knowledge of computers, software, networks, and physical processes, which will be integrated into the system.

Real-time operating systems manage embedded systems. There software correctness is associated not only with the correct ending, but also, for a certain task implementation compliance of spent time with the planned time. It is quite difficult to transfer these properties to the cyber-physical systems. Different types of processors and memory architectures, as well as a variety of operation systems and programming environments are used in CPSs.

The development of cyber-physical systems, which closely interact with physical processes, requires a technically sophisticated low-level design. CPS developers are forced to fight with break controllers, memory architecture, processes planning, assembler level programming, network interface design and installation of drivers. However, it would be better to focus on system functionality and behavior definition.

The great complexity is not determinate due to the real environment, in which the cyber-physical system is used. Cyber-physical system may change by the time and no one of the system's component is completely safe.

All the above-described deviations from the final task solving encouraged looking for new approaches to cyber-physical system design. Experts from the University of Berkeley [15] believe that cyber-physical system's design should be based on the common system behavior modeling and hardware, software, network and physical process single design.

CPS design process is an iterative process, which consists of three phases: modeling, design and analysis (see Fig. 4). In order to develop systems, which are able to work in the real world, a new approach – model designing is used.

Firstly, the real world analysis should be performed, and physical processes identified, which will interact with cyber-physical system. Then it is possible to start development of an abstraction of the real world processes. Model design allows overcoming some of the fundamental problems in the cyber-physical system design, such as security, determinism and time.

Every system is designed to address a specific problem or complete a task. System requirements can be described in a simple language, in formal way or with models. The formal description reduces the number of possible errors, but modeling serves to illustrate the system dynamics.

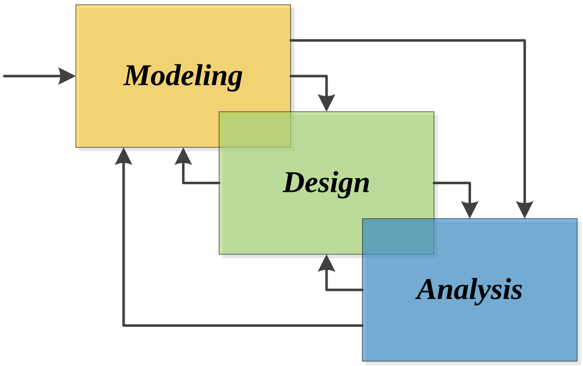

Fig. 4. Cyber-physical system design process.

During the process of analysis, the extent to which the system has met the requirements specification can be determined. CPSs are either commissioned or altered in accordance with the previous and the new requirements. New desires, needs and requirements to a cyber-physical system will also arise in the use process.

In real conditions, for the research purposes only a verified and validated cyber-physical system that successfully passed safety tests must be used. It also applies to the new version of the system or a supplement. Nevertheless, in healthcare facilities only certified cyber-physical systems must be in use.

A set of regulations and standards is applied to all medical systems, which indicates that the system is electrically, physically, biologically and chemically safe for the end user. Cyber-physical system sensors generate the sensitive data that must be protected and shared only in a secure manner. Currently, there are no standards and regulations, which relate directly to healthcare cyber-physical systems [8], [14]. However, it is worthwhile to be acquainted with medical equipment standards, regulations and clinical standards.

According to the European Union Glossary of Terms [16]:

- Standard is national or international level detailed engineering characteristics that determine the optimal requirements – performance, safety and reliability.
- Regulation is a set of rules with the force of law issued by the executive authority.

As shown, the regulations are mandatory, while standards – desirable. Although the regulations of medical equipment are similar in several countries, they are not identical. This means that the same medical device can be recognized as safe for use in medical institutions of the European Union, but not in the United States.

The CE marking certifies that a product has been approved for use and distribution in Europe – a direct translation of the French term “Conformité Europen” or “Approved in Europe”. By contrast, in the United States U.S. FDA (United States Food and Drug Administration) shall indicate the medical equipment compliance with their regulations. Countries, which have not developed or adopted any medical equipment regulations primarily, apply the WHO (World Health Organization) regulations.

While standards of healthcare cyber-physical systems are not yet developed, a number of industrial, communications (for example, Bluetooth – IEEE 802.15.1, Wi-Fi – IEEE 802.11), quality (ISO 9001, ISO 13845, ISO 14971), medical equipment (ISO/IEEE 11073, HL7 – Health Level 7, DICOM – Digital Imaging and Communications in Medicine) and clinical standards can be applied to them.

ISO/IEEE 11073 is a standard set for personal healthcare devices. The general context of it is data communication and interface between the agent and the manager.

Health Level 7 is a group of standards for the exchange, integration, sharing, and retrieval of electronic health information. HL7 determines many adaptable standards, guidelines, and methodologies that enable communication of various computer systems in hospitals and different healthcare providers.

Generalizing, medical equipment standards have been drawn up to improve the quality and number of facilities, and equipment interoperability.

VI. Conclusion

Healthcare cyber-physical systems can reach the level of functionality, adaptability, and effectiveness previously unattainable for medical devices.

During the first part of research, the authors reviewed healthcare cyber-physical system application and compliance with existing standards and possibilities for further system development.

After identification of main tasks of the healthcare cyber-physical system and looking at the above-mentioned regulations and standards, a requirement definition can be initiated so that the CPSs comply with appropriate regulations and standards.

Acknowledgement

This research has been supported by the Latvian state research program 2014–2017 project “The Next Generation of Information and Communication Technologies (NexIT)”.

References

[1] “Cyber-Physical Systems Week” [Online]. Available: http://www.cpsweek.org/ [Accessed: Sept. 1, 2014].

[2] D. Patterson, J. Hennessy, *Computer Organization and Design: The Hardware Ssoftware Interface. 5th edition*. Morgan Kaufmann, 2013.

[3] “Cyber-Physical Systems” [Online]. Available: http://cyberphysicalsystems.org/ [Accessed: Sept. 1, 2014].

[4] A. Milenkovic, C. Otto, E. Jovanov, “Wireless sensor networks for personal health monitoring: issues and an implementation,” *Computer Communications*, vol. 29, no. 13–14, 2006, pp. 2521–2533. http://dx.doi.org/10.1016/j.comcom.2006.02.011

[5] R. Buyya, J. Broberg, A. Goscinski, *Cloud Computing: Principles and Paradigms*, John Wiley & Sons, Hoboken, NJ, USA, 2011. http://dx.doi.org/10.1002/9780470940105

[6] N. Wu and X. Li, *RFID Applications in Cyber-Physical System, Deploying RFID – Challenges, Solutions, and Open Issues*. InTech, 2011.

[7] Cyphers, *Cyber-Physical Eurobean Roadmap & Strategy*. Deliverable D5.1: CPS: State of the Art, 2014.

[8] Steering Committee for Foundations in Innovation for Cyber-Physical Systems, *Foundations for Innovation: Strategic R&D Opportunities for 21st Century*, 2013.

[9] AENEAS Industry Association, *Part B of the 2014 ECSEL MARSIA*, 2013.

[10] A. Koubaa, B. Andersson, “A Vision of Cyber-Physical Internet,” *Proceedings of the 8th International Workshop on Real-Time Networks*, Dublin, Ireland, 2009.

[11] S. Amin, G. Schwartcz, A. Hussain, “*In Quest of Benchmarking Security Risks to Cyber-Physical Systems,” IEEE Network*. Jan./Feb. 2013, pp. 19–24. http://dx.doi.org/10.1109/MNET.2013.6423187

[12] “Networking and Information Technology Research and Development Program,” *High-Confidence Medical Devices: Cyber-Physical Systmes for 21st Century Health Care.* NTRD, 2009.

[13] G. Schirner, D. Erdogmus, K. Chowdhury, T. Padir, “The Future of Human-in-the-Loop Cyber-Physical Systems,” *Computer*, IEEE computer Society Digital Library, 2013, pp. 36–45. http://doi.ieeecomputersociety.org/10.1109/MC.2012.428

[14] S. A. Haque, S. M. Aziz, M. Rahman, “Review of Cyber-Physical System in Healthcare,” *International Journal of Distributed Sensor Networks*, Hindawi Publishing Corporation, vol. 2014, p.20, 2014. http://dx.doi.org/10.1155/2014/217415

[15] E. Lee, S. Seshia, *Introduction to Embedded Systems, A Cyber-Physical Systems Approach*. 2014.

[16] Eiropas Savienības terminu vārdnīca. – R., UNDP, 2004.

Alyona Skorobogatjko, *B. sc. ing.*, is a Master’s Student at the Department of Information Technology Management, Riga Technical University (Latvia). She received the Bachelor Degree in Information Technology from Riga Technical University in 2012. Her Bachelor Thesis on SCADA network security received special support from the Latvian local energy production company and was among laureates of the best Latvian theses in the field of Information Technology in 2012. She has experience in software development, and currently she is a Project Manager at an international company. Her professional interests include project management, software and systems, particularly healthcare systems, design, modeling and development. She has participated in a number of international scientific conferences and multiple projects.
E-mail: alona.skorobogatjko@rtu.lv.

Andrejs Romanovs, *Dr. sc. ing*., is an Associate Professor and Lead Researcher at the Information Technology Institute, Riga Technical University. He has 25 years of professional experience teaching post-graduate courses at RTU and developing more than 50 industrial and management information systems. His professional interests include modeling and design of management information systems, IT governance, IT security and risk management, integrated information technologies, as well as education in these areas. A. Romanovs is a senior member of the IEEE, LSS; the author of more than 50 papers in scientific journals and conference proceedings in the field of Information Technology.
E-mail: andrejs.romanovs@rtu.lv,

Nadezhda Kunicina, *Dr. sc. ing.* Since 2005 she has been an Associate Professor with RTU. Her fields of scientific interest are electrical engineering, embedded systems, sustainable transport systems. The research interest is related to the improvement of electric energy effectiveness in industrial electronics and electric transport. She is a Scientific Project Manager of FP7 – ARTEMIS – 2012 called Arrowhead project. The aim of project is to address the technical and applicative challenges associated with cooperative automation.
E-mail: nadezda.kunicina@rtu.lv.

Aļona Skorobogatjko, Andrejs Romanovs, Nadežda Kunicina. Veselības aizsardzības kiberfizikālo sistēmu apskats
Jau vairākus gadus dažādu nozaru speciālisti visā pasaulē interesējas par virtuālās un fiziskās pasaules mijiedarbības iespēju izmantošanu. Kiberfizikālo sistēmu pielietošanas mērķis ir integrēt reālus fiziskus procesus ar virtuāliem skaitļošanas procesiem. Pētījuma tēmas aktualitāte ir neapšaubāma un balstās uz to, ka kiberfizikālās sistēmas ir daudzsološa joma, kuras attīstība virza uz priekšu medicīnu. Kiberfizikālās sistēmas ir specializētas skaitļošanas sistēmas, kurām ir fiziskas mijiedarbības līdzekļi ar kontroles un vadības objektu. Iegultās sistēmās galvenais fokuss ir skaitļošanas elements, bet kiberfizikālās sistēmās – saite starp skaitļošanas un fizisko elementu. Kibefizikālās sistēmas tiek pielietotas tādās jomās kā medicīna, transporta plūsmu vadība, automobiļu būvniecība, industriālo un tehnoloģisko procesu vadība, enerģijas ekonomija, ekoloģijas monitorings un pārvaldība, avionika un kosmiskā tehnika, industriālie roboti, tehniskās infrastruktūras pārvaldība, sadalītas robottehnikās sistēmas, sistēmas aizsardzības mērķiem. Ir slimnīcas, kur jau tagad roboti pienes pacientiem ēdienu, šķiro pastu, maina gultasveļu, kā arī transportē pacientus uz operāciju zāli ar robotizētām gultām. Taču pilnībā automatizēta veselības aizsardzības sistēma vēl nevienā medicīnas iestādē nav ieviesta. Kiberfizikālo sistēmu izstrādei ir nepieciešamas gan zināšanas par datoriem, programmatūru, tīkliem, gan arī par fiziskiem procesiem, ar kuriem tiks integrēta izstrādājamā sistēma. Kiberfizikālo sistēmu izstrāde ir iteratīvs process, kas sastāv no 3 fāzēm: modelēšanas, izstrādes un analīzes. Pirms veselības aizsardzības kiberfizikālās sistēmas izstrādes ir vērts iepazīties ar medicīnas iekārtu standartiem un nolikumiem, kā arī klīnisko pētījumu standartiem, kurus apskatot un, identificējot izstrādājamās sistēmas galvenos uzdevumus, var uzsākt prasību definēšanu atbilstoši attiecīgajiem nolikumiem un standartiem.

Алёна Скоробогатько, Андрей Романов, Надежда Куницына. Современное состояние медицинских кибер-физических систем
На протяжении последних десятилетий специалисты из разных областей заинтересованы в исследовании возможностей взаимодействия реального мира с виртуальным. Кибер-физические системы – это специализированные вычислительные системы, которые включают в себя объекты взаимодействия с реальным миром, вычислительные объекты и систему коммуникации. Тема исследования весьма актуальна, так как кибер-физические системы являются многообещающей отраслью, развитие которой способствует развитию медицины в целом. Во встроенных системах главной является вычислительная часть, а в кибер-физических системах – связь между вычислительными и физическими элементами. В современном мире кибер-физические системы используются в медицине, в том числе в телемедицине, управлении транспортом и обеспечении безопасности, автомобилестроении, в распределённых роботизированных системах, управлении производственными и технологическими процессами. Существуют больницы, в которых уже сейчас роботы разносят еду пациентам, меняют постельное бельё, с помощью роботизированной кровати пациенты транспортируются в операционные залы, но полностью автоматизированная система здравоохранения ещё не введена ни в одном медицинском учреждении. Разработка кибер-физических систем невозможна без знаний о вычислительных системах, сетях, но ещё более важными являются знания о физических процессах, интегрируемых с виртуальными процессами. Процесс разработки кибер-физических систем является итеративным процессом и состоит из трех фаз: моделирования, разработки и анализа. На данный момент не существует стандартов и регламентов, относящихся именно к медицинским кибер-физическим системам, поэтому стоит ознакомиться со стандартами и регламентами разработки медицинских систем, а также со стандартами клинических исследований. Рассмотрев вышеупомянутые регламенты и стандарты и определив главные задачи разрабатываемой системы, можно начать процесс формулирования требований к медицинской кибер-физической системе.