Security challenges in cyber systems

Safdar, Ghazanfar A.; Kalsoom, Tahera; Ramzan, Naeem

Published in:
2020 International Conference on UK-China Emerging Technologies (UCET)

DOI:
10.1109/UCET51115.2020.9205388

Published: 29/09/2020

Document Version
Peer reviewed version

Safdar, G. A., Kalsoom, T., & Ramzan, N. (2020). Security challenges in cyber systems. In *2020 International Conference on UK-China Emerging Technologies (UCET)* IEEE. https://doi.org/10.1109/UCET51115.2020.9205388

Security Challenges in Cyber Systems

Ghazanfar A. Safdar
School of Computer Science & Technology
University of Bedfordshire
Luton, United Kingdom
ghazanfar.safdar@beds.ac.uk

Tahera Kalsoom
School of Computing, Engineering and Physical Sciences
University of the West of Scotland
Glasgow, United Kingdom
tahera.kalsoom@uws.ac.uk

Naeem Ramzan
School of Computing, Engineering and Physical Sciences
University of the West of Scotland
Glasgow, United Kingdom
naeem.ramzan@uws.ac.uk

***Abstract*— CPS (Cyber-Physical Systems) is proposed by the NSF (National Scientific Foundation) to describe a type of necessities which conglomerates hardware and software components and being the next step in development of embedded systems. CPS includes a wide range of research topics from signal processing to data analysis. This paper contains a brief review of the basic infrastructure for CPS including smart objects and network aspects in relation to TCP/IP stack. As CPS reflect the processes of the physical environment onto the cyber space, virtualisation as important tool for abstraction plays crucial role in CPS. In this context paper presents the challenges associated with mobility and vritualisation; accordingly, three main types of virtualisation, namely network, devices and applications virtualisation are presented in the paper. The main focus of the paper is made on security. Different threats, attack types and possible consequences are discussed as well as analysis of various approaches to cope with existing threats is introduced. Furthermore, needs and requirements for safety-critical CPS are reviewed.**

Keywords— **CPS, Systems, Security, Safety, Virtualisation**

I. INTRODUCTION

CPS is a concept focusing on bridging physical and cyber worlds. Firstly, the term of CPS was proposed by NSF, where CPS are described as complex engineered systems devoted to integration of cyber and physical components to extend capabilities of recent embedded systems [1]. This definition states clearly that CPS is the next evolution stage of Embedded Systems. CPS while compared to embedded systems are not limited by just one device, it is more an ecosystem of devices operating in the physical environment and being controlled by computational elements. Another similarity to CPS concept is Internet of Things (IoT) defined as global infrastructure connecting various physical and virtual entities called 'things' in order to provide advanced services [2].

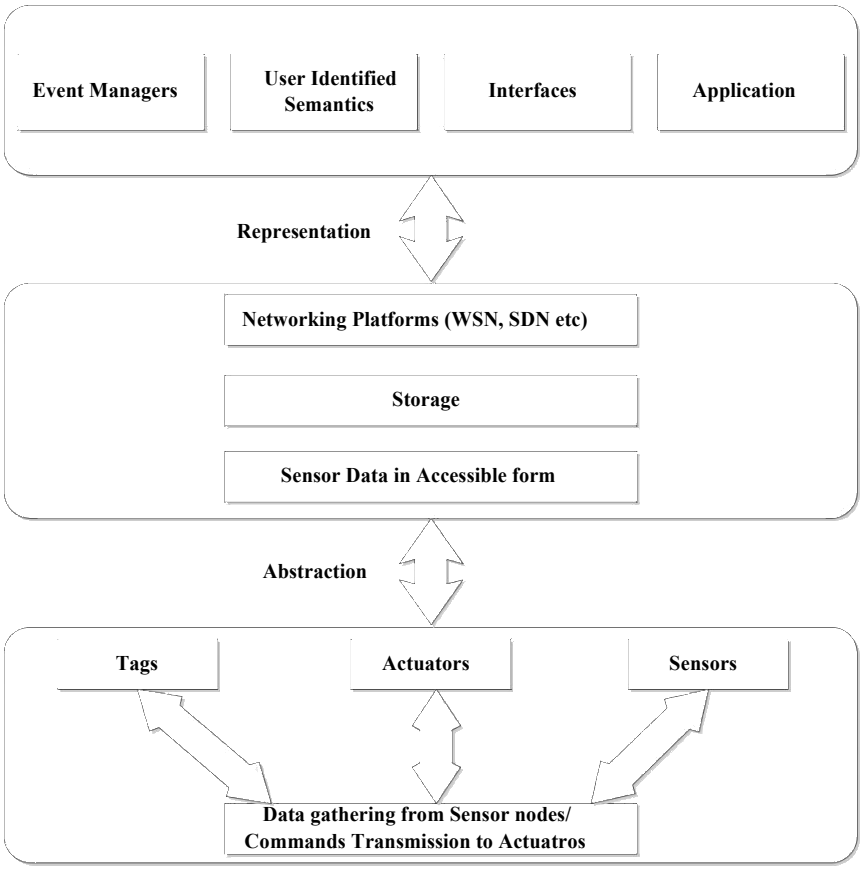
In many areas of human activities, CPS has gained more and more attention, especially in the capacities where physical processes and physical equipment needed to be controlled, orchestrated and coordinated with humans, systems, or subsystems. The emerging trends like Industry 4.0 [3] or Industry Internet [4] are the key indicators of CPS importance; transition to these concepts will involve increasing automation, autonomy and complete new understanding of production processes. Major incentive, which forces CPS development is a need of convergence for physical processes and computational capabilities, where high degree of communication between components and abstraction of the processes occurring in the physical environment is needed. The scaling of the CPS systems, small and large scale respectively, is distinguished by number of involved components [5]. Small-scale CPS have just a little number of physical as well as cyber components while large-scale systems have hundreds or even thousands of components. Both of them can be geographically distributed, which may require convergence with global networks, such as Internet [6].

There were several efforts to develop a general model for CPS in order to give a clear idea of the main components of a CPS regardless of application domains. In [7], CPS is represented through three main layers: the first layer consists of sensors and actuators which observe changing physical environment; the second layer aims at communication and abstraction of the real-world processes and the third deals with computational capabilities. Another work in [8] describes an approach for CPS design consisting of three layers, namely physical layer, platform layer, and computation/ communication layer, where the last two layers are in fact cyber layers. To establish a comparison among the design concepts, there are common similarities such as the same number of design layers and similar functions performed by the layers. Thus, first layer in both concepts [7, 8] is focused on physical components operating in physical environment, whereas the second layer is aimed at interconnection of the lower and higher levels, storage and service composition with particular attention being paid to abstraction mechanisms and the last one serves to high level functions such as computational algorithms, processing, etc. However, there is some research work which purely focuses on architectures for specific application domains. As in [9], the four-layer architecture for CPS in healthcare domain is represented. General view of main layers and components of CPS can be represented as in Fig. 1.

The rest of the paper is organised as follows. Infrastructure of Cyber physical systems is presented in section II whereas importance of security in the presence of existing threats is highlighted in section III. Finally, paper is concluded in section IV.

II. INFRASTRUCTURE FOR CYBER PHYSICAL SYSTEMS

Infrastructure plays a crucial role in deployment of every system; the same applies to Cyber-Physical Systems (CPS). In line with Fig. 1, the main components of CPS can be considered as sensors / actuators, controllers, communication networks [10]. However, some CPS solutions additionally employ gateways [11]. Importantly, CPS can be both open-loop or closed loop systems. By the analogy with Internet of Things (IoT), open-loop CPS can have access to the global networks, and in this case such paradigms as Cloud Computing, BigData etc. can be added into the notion of CPS infrastructure. Cyber Physical systems can consist of large extent of heterogeneous devices, including sensors, actuators, etc.



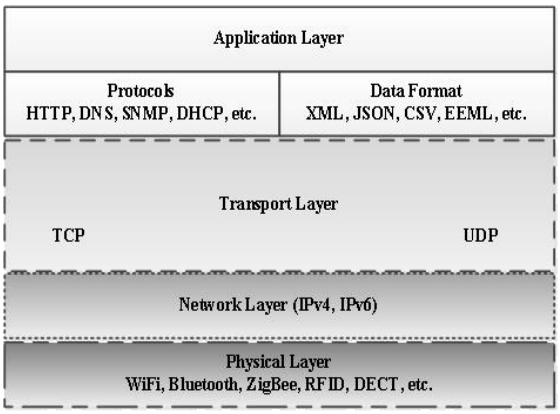


Fig. 2. TCP/IP enabled CPS Integration model.

Five level CPS architecture has been proposed in [12] with layers functionality described as: (i) Smart connection level, (ii) Data-to-information conversion level, (iii) Cyber level, (iv) Cognition level, and (v) Configuration level. Crucial role by different architectural solutions plays the point of view on the system, for example in [13], CPS architecture is proposed from the service oriented point of view and consists of 4 levels as follows: (i) Perceive tier, (ii) Data tier, (iii) Service tier, and (iv) Execution tier. Since CPSs are the part of ICT area, it is important to find interrelations between Open Systems Interconnection Model (OSI), architectures and models developed for CPS. An adapted OSI model for CPS involves Middleware and System Infrastructure model. However, if CPS needs to be integrated with global networks such as Internet, TCP/IP model can be the best contender, where two lowest layers, Physical and Data, accordingly, are represented by just one level. Application, Transport and Network layers respectively form part of the other three layers. Fig. 2 represents some technologies and protocols belonging to each of the layers.

However, this model raises the issues of choice of transport protocol to be the best candidate for Cyber Physical Systems. The need for design of new transport protocol for CPS systems has been highlighted in [6]. The main argument behind the design of the new transport protocol was increased reliability without any requirement of acknowledgements. However, challenging task to build the new transport protocol for CPS can face several difficulties, one of these is that there are many devices which support TCP/IP or UDP/IP stacks, accordingly issues of standardization and compatibility become extremely important for the design of new transport protocol. Equally, it is very difficult to decide about transport protocol independently of the underlying medium which is being used [14]. Despite the stated need, existing protocols such as connection-oriented TCP and connectionless UDP can offer wide functionality. Therefore, considerable level of reliability can be achieved by combining TCP and UDP, depending on messages types and data types to be transmitted [15]. Importantly, while making a choice of transport protocols for CPS, the objectives of designed system need to be considered and strongly met. In general, when loss tolerant real-time data have to be transmitted, UDP is preferred over TCP [16]. Since there is a need to monitor the actual state of physical environment, data gathered from sensors can be very sensitive to delays. To be able to deal with near real time transmission and to account for heterogeneous wireless

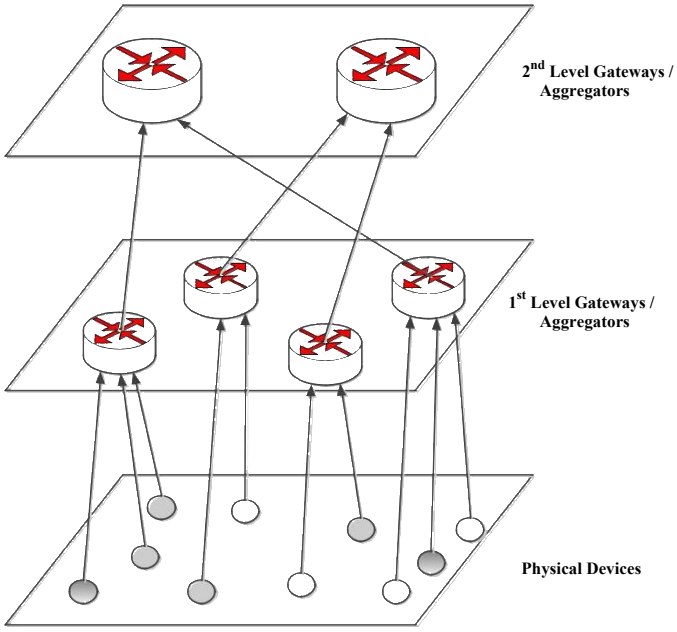


Fig. 3. CPS-layered gateway structure.

technologies, a gateway approach is proposed [17]. Gateways bring in the fact that there will be no more end-to-end transmission, but through some mediator between sensing devices and target nodes [18].

Gateway structure can be very complex and is usually represented through layered model showing different gateway roles. Having said that, depending upon the role, certain gateways not only aggregate data from sensor nodes but from other gateways too. Such a layered gateway structure is represented in Fig. 3.

III. Security in Cyber Physical Systems

Since potential threats can affect both the cyber and physical environments, thus security provision in CPS is extremely important at all stages, namely design, deployment and operation [16,17]. Moreover, as CPS are used on many objects of critical infrastructure, issues for protecting them have become extremely relevant. A system to protect a hydroelectric dam with particular focus on conflict resolution for internal policy management is discussed in [16]. The work discusses analysis of unauthorized network usage and proposes corresponding countermeasures which include reconfiguration of devices as well as measures ensuring integrity of critical data storage. The objects and people are represented as assets and agents respectively in Socio-CPS (SCPS). Though the issues related to SCPS security are discussed in [19], however the work presented lacks in attack prediction. Modern cyber physical systems require components- or subsystems-centric security approach to evaluate the possible consequences for the whole system, even when one of the components is compromised [20]. Considerable research work discusses the possibility of attacks on control systems in order to gain access to the physical part of CPS [19, 20]. As a consequence, SCADA systems, even though based on web technologies, are designed with the viewpoint to minimize the external access to critical infrastructure. However, convergence of SCADA systems with corporate and global networks have introduced new security threats, such as non-secure remote connections, knowledge availability, etc. [20]. Centralised administration has been proposed to tackle the issue of insecurity in remote connections as well as unauthorised privileges.

A. *Types of Existing Attacks*

Fig. 4 describes common attack types and their sub-types in Cyber Physical Systems. The intruder aims to take control of entire system by launching control hijacking attack, whereas code injection exploits system vulnerabilities by systematic injection of rogue piece of code to change the execution of the entire program. Malware attacks employ special software to hamper normal functioning of a system. Traffic sniffing or interception is practiced in case of eavesdropping attack, whereas the intruder impersonates itself in spoofing attack [19]. All attack types can be extended by Denial of service attacks (DoS) which is aimed at flooding the system in order to disable the actual services provided by the system [18,19].

Based on the above mentioned attack types several attack subtypes can be highlighted as follows.

1) Spoofing Subtypes: GPS spoofing is based on broadcasting of incorrect signals of higher strength than received from satellites in order to deceive the victim [20]. Intruder explores the IP addresses of the victim nodes and then sends ARP responses to node X and node Y, with IP address of corresponding node and its own MAC address in ARP spoofing. Thus all packets between X and Y will then pass through the intruder node. IP spoofing is another subtype of spoofing attack aimed at using another IP address to pass through security system. This type of attack can be used on the first stage of complex intrusion in conjunction with reflected attack.

2) Code Injection Subtypes: SQL injection attack involves insertion of malicious SQL statement in the queries, thus leading towards failure of the input data. Cross site

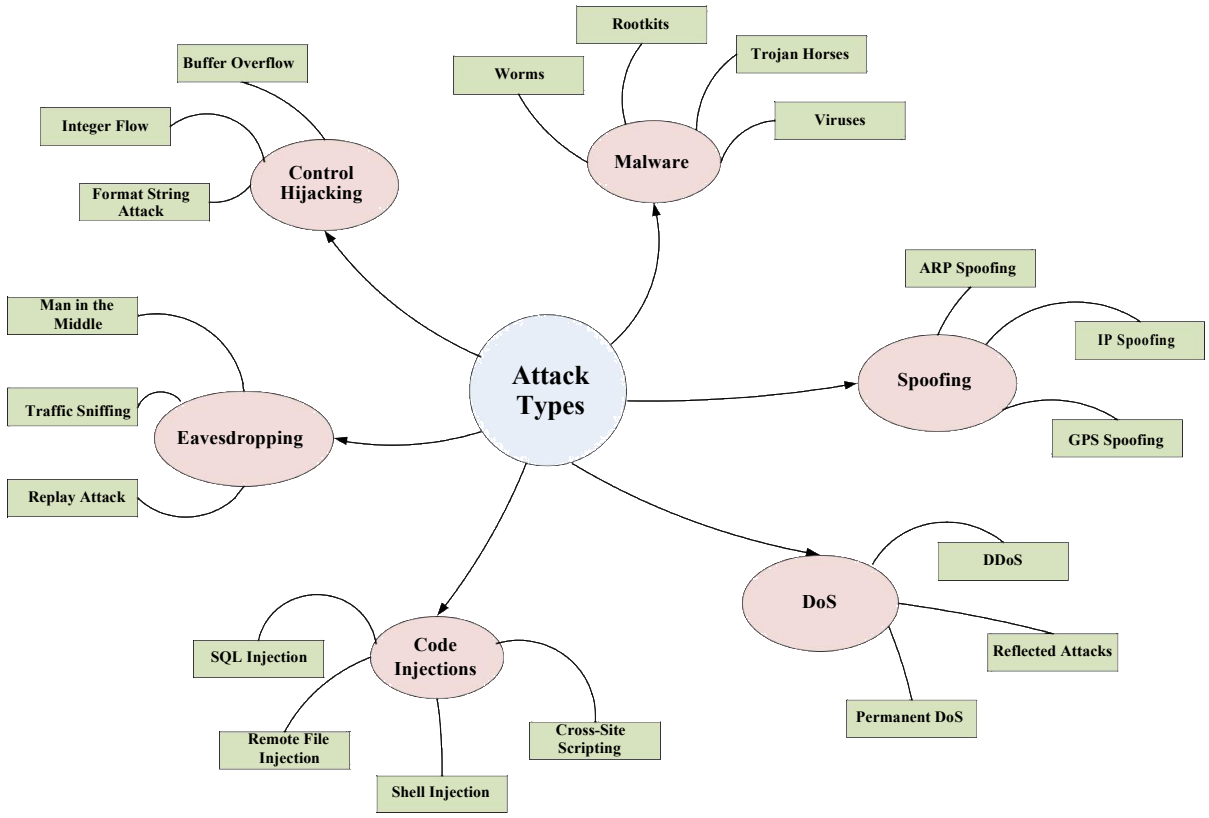


Fig. 4. Common attack types and their subtypes.

scripting exploits open scripting vulnerabilities and adds malicious code in to web application leading towards execution. Remote file injection extends itself on the serve side of web applications where the file with malicious code is downloaded and is executed on the server. Shell injection attack is implemented through inclusion of malicious shell code into the code string for further interpretation by the shell [20].

3) Eavesdropping Subtypes: Man-in-the-Middle is an active type of attack and occurs when intruder intervenes between communicating entities trying to intercept the packets. Traffic sniffing is a passive type of eavesdropping aimed at traffic analysis using special device or program. Relay attacks are aimed at interception of authentication related information.

4) Malware Subtypes: Worm is a type of Malware software with ability of making copies of itself thus resulting into wastage of network bandwidth. Virus is also able to replicate itself as worm, but comparatively infects files and programs in the system. Trojan horse intrudes in the system under the guise of legitimate software, whereas Rootkit is a set of software; such as scripts, executable files, configuration files, etc; with ability to hide itself and other malicious software.

5) Control Hijacking Subtypes: Buffer overflow is a phenomenon when a program is writing data outside of the given buffer, often it is the consequence of the wrong processing of input data. Integer overflow is an error occurred due to inability to represent the numeric value within given storage space, whereas Format string is an intrusion during which the input string is executed as a command. Important, all attack types can be divided into either passive/active or invasive/non-invasive respectively [19]. Passive attacks, such as traffic sniffing, have the purpose to intercept the sensitive data without causing any destruction to the operation of the entire system. Whereas active attacks, like DoS/DDoS, code injections etc, are aimed at causing direct damage or to gain the control of the system or infrastructure [18].

For active attacks, main purpose is to destroy or damage the system. Depending on the above-mentioned attack groups, accordingly different protection strategies need to be implemented.

B. Attack Vectors

Threats eventually translate into attack vectors. Hardware based attack vectors for smart devices namely, device identity theft and cryptographic keys theft have been identified in [21, 22]. Importantly, attack vectors can vary depending upon CPS application domain. Work presented in [21] considers medical implants related attacks with the purpose, either to steal the information, change the therapy, or render the device useless by exhaustion of its energy sources. In an energy management domain, for example smart homes, an intruder can manipulate energy consumption measurements resulting into energy theft [22]. Considerable research work has been done towards automatic identification of attack vectors, such as data disclosure and resources disruption etc. [21]. Knowledge based attack vector presented in [22] assumes that the intruder may not possess the necessary knowledge about physical processes and ways to take control of the system. However, the attacker implements five steps of intrusion: access,

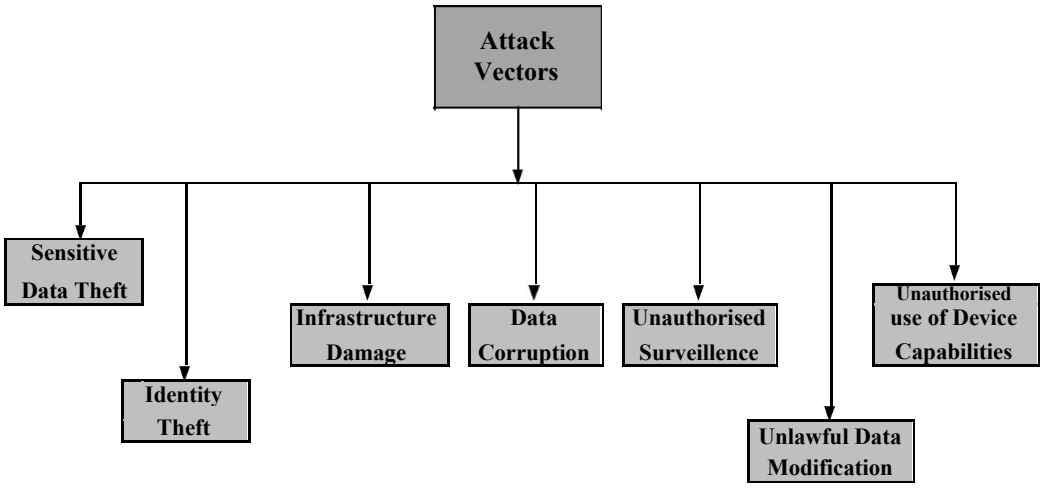


Fig. 5. Attack vectors in Cyber Physical Systems.

discovery, control, damage and cleanup accordingly, to gain full control of the system in direct or indirect way and to hide any traces of any caused intrusion. Fig. 5 presents the main attack vectors in Cyber Physical Systems.

IV. Conclusion

Cyber-Physical Systems are complex systems based on convergence of physical or hardware and cyber or software components. CPS has large variety of application areas: among others are transport, healthcare, wearable's, home automation etc. The number of deployed CPS steadily increase, which causes several challenges related to security and safety. Importance of new complex approaches in the area of Security and Privacy for CPS considering the influence of single components and subsystems threats on the whole system is discussed. Some salient threats and attack vectors were reviewed and debated. More discussion is needed towards threats modelling, which is very important on design stage to develop security mechanisms as well as to evaluate possible damage to the systems under different circumstances. Necessity of joint security and safety consideration in order to identify the most complete set of potential threats also needs to be highlighted as future work in the paper.

References

[1] National Science Foundation (NSF), Cyber-Physical Systems, USA, 2015 [Online], Available: http://www.nsf.gov/pubs/2015/nsf15541/nsf15541.pdf

[2] ITU-T, "Overview of the Internet of Things", Recommendation ITU-T Y.2060, 2012.

[3] M. Hermann, T. Pentek, B. Otto, Design Principles for Industrie 4.0 Scenarios: A Literature Review, Working Paper, Technical University of Dortmund, Dortmund, Germany, 2015.

[4] P.C. Evans, M. Annunziata, Industrial Internet: Pushing the Boundaries of Minds and Machines, General Electric [Online], Available: http://www.ge.com/docs/chapters/Industrial_Internet.pdf

[5] D.C. Schmidt, J. White, C.D. Gill, "Elastic Infrastructure to Support Computing Clouds for Large-scale Cyber-Physical Systems", in Proc. *IEEE ISORC Symp.*, 2014, pp. 56-63.

[6] A. Koubaa, A. Björn, "A Vision of Cyber-Physical Internet", in Proc. *8th International Workshop of Real Time Networks (RTN)*, 2009, pp. 1-6.

[7] Y. Tan, S. Goddard, L.C. Pérez, "A prototype architecture for cyber-physical systems", *ACM SIGBED Review*, vol. 5, issue 1, Jan. 2008.

[8] J. Sztipanovits, X. Koutsoukos, G. Karsai, N. Kottenstette, P. Antsaklis, V. Gupta, B. Goodwine, J. Baras, S. Wang, "Toward a science of cyber–physical system integration", in *Proc. IEEE*, vol. 100, issue 1, pp. 29-44, Jan 2012.

[9] O. Kocabas, T. Soyata, M.K. Aktas, "Emerging Security Mechanisms for Medical Cyber Physical Systems", *IEEE/ACM Transactions on Computational Biology and Bioinformatics*, vol. 13, issue 3, pp. 401-416, 2016.

[10] H. Li, A. Dimitrovski, J.B. Song, Z. Han, L. Qian, "Communication Infrastructure Design in Cyber Physical Systems with Applications in Smart Grids: A Hybrid System Framework", *IEEE Communications Surveys & Tutorials*, vol. 16, issue 3, pp. 1689-1708, 2014.

[11] M. Szczodrak, Y. Yang, D. Cavalcanti, L.P. Carloni, "An open framework to deploy heterogeneous wireless testbeds for Cyber-Physical Systems", in *Proc. 8th IEEE International Symposium on Industrial Embedded Systems (SIES)*, 2013, pp. 215-224.

[12] J. Lee, B. Bagheri, H-A. Kao, "A Cyber-Physical Systems architecture for Industry 4.0-based manufacturing systems", *Manufacturing Letters*, vol. 3, pp. 18-23, 2015.

[13] L. Hu, N. Xie, Z. Kuang, K. Zhao, „Review of Cyber-Physical System Architecture", in Proc. *15th IEEE International Symposium on Object/Component/Service-Oriented Real-Time Distributed Computing Workshops*, 2012, pp. 25-30.

[14] J-P. Vasseur, A. Dunkels, *Interconnecting Smart Objects with IP*. Morgan Kaufman Publishers Inc., San Francisco, USA, 2010.

[15] S. Bae, D. Jang, K.S. Park, „Why Is HTTP Adaptive Streaming So Hard?", in *Proc. 6th Asia-Pacific Workshop on Systems*, 2015, No. 12, http://dx.doi.org/10.1145/2797022.2797031

[16] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, (2015). "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications", *IEEE Communications Surveys & Tutorials*, vol. 17, issue 4, pp. 2347-2376, 2015.

[17] H. Wang, J. Li, H. Gao, (2015). „Dynamic Resource Allocation of Gateways for Packet Transmission in Cyber-Physical Systems", in *Proc. IEEE International Conference on Mobile Ad-hoc and Sensor Networks (MSN)*, 2015, pp. 150-157.

[18] J. Valente, C. Barreto, A.A. Cardenas, (2014). "Cyber-Physical Systems Attestation", in *Proc. 10th IEEE International Conference on Distributed Computing in Sensor Systems*, 2014, pp. 354-357.

[19] M.E. Perez Hernandez, S. Reiff-Marganiec, "Autonomous and self-controlling smart objects for the future internet", in *Proc. 3rd International Conference on Future Internet of Things and Cloud (FiCloud)*, 2015, pp. 301-308.

[20] G. Kortuem, F. Kawsar, V. Sundramoorthy, D. Fitton, "Smart Objects as Building Blocks for the Internet of Things", *IEEE Internet Computing*, vol. 14, issue 1, pp. 44-51, 2010.

[21] M. Sabou, "Smart Objects: Challenges for Semantic Web Research", *Semantic Web Journal*, vol. 1, isuue 1,2, pp. 127-130, 2010.

[22] S.N. Han, I. Khan, G.M. Lee, N. Crespi, R.H. Glitho, "Service composition for IP smart object using realtime Web protocols: Concept and research challenges", *Computer Standards & Interfaces*, vol. 43, pp. 79-90, 20