Smart city cyber-physical security

Ana-Maria TUDOR
Marketing department, BEIA Consult International, Bucharest, Romania

ana.tudor@beia.ro

George SUCIU
R&D department, BEIA Consult International, Bucharest, Romania

george@beia.ro

George Valentin IORDACHE
R&D department, BEIA Consult International, Bucharest, Romania

george.iordache@beia.ro

Gabriela BUCUR
Marketing department, BEIA Consult International, Bucharest, Romania

gabriela.bucur@beia.ro

Hussain IJAZ
R&D department, BEIA Consult International, Bucharest, Romania

ijaz@beia.ro

Marius VOCHIN
R&D department, BEIA Consult International, Bucharest, Romania

marius.vochin@upb.ro

Abstract

Recently, the number of Internet users has increased enormously, this becoming the main way in which states and non-states actors increase their economic and diplomatic capacity through strategic and targeted manipulation with the help of web content that they transmit to citizens. Brilliant urban areas have a bleeding edge obligation to guarantee a protected and safe physical and advanced environment advancing durable and feasible metropolitan improvement for the prosperity of EU residents. S4AllCities incorporates progressed mechanical and authoritative arrangements in a market situated brought together Cyber – Physical Security Management structure, targeting raising the strength of urban communities' frameworks, administrations, ICT frameworks, IoT and cultivating insight and data sharing among city's security partners. A smart city is made up mainly of information and communication technologies (ICT) to develop, implement and promote the practice of sustainable development to address the growing challenges of urbanization. Mostly, ICT is a smart network of objects and machines that are connected and transmit data using both wireless technology and the cloud. IoT-based and cloud-based applications receive, analyze, and manage data in real time to make a good decision about quality of life. People use Smartphones, mobile devices, cars and smart homes for smart city ecosystems. Communities can improve energy distribution, streamline garbage collection, reduce traffic congestion, and even improve IoT air quality. This paper fills a gap in the literature dealing with attacks on critical infrastructure in smart cities and presents envisioned pilots for 3 cities in Europe, as well as experiments in follower cities, one of them being Buzau in Romania.

Keywords: *ICT, wireless technology, urbanization, IoT, CPS, city safety.*

1. Introduction

The notion of smart city is considered a massive one, covering the administration and integrity of the entire configuration with the help of built-in technology. In this situation, surveillance is performed by cyber security, bringing together all components of the configuration, including administration, governance, citizens, healthcare, society, the education system and the environment, using ICT. [7] Cyber security is often described as digital or ICT technologies, which are used by a smart city to improve features and services to make costs more efficient and used resources. [6]

Increased advances in ICT must lead to improved management, operations, and the environment in several ways. As a result, issues related to advanced smart cities are becoming increasingly difficult. This is due to the rate of change which is quite high. This leads to the need for up-to-date technologies and intense web research to bring about organizational change. To gather personal details about people, you can use applications and social networks. [27]

In 2013, it was estimated that in 2020, the global market for smart city solutions will reach $408 billion, according to The Department for Business

Innovation & Skills of the UK, which means that smart cities will represent approximately 24% of the global market. In 2020, the real amount reached $410.8 billion and is estimated to grow to $820.7 billion by 2025 in just 5 years. [12, 31]

As common platforms with services and tools are absent, this prevents the efficient development of the associated ecosystem. A platform has been developed, Smart Citizen Service, which classifies the market into integrated video surveillance, in-vehicle cameras, intelligent healthcare, security and threat management, and intelligent education.

Due to the growth of the urban population, new market opportunities are generated for those in the industry who want to meet the requirements of the Smart City market. A major growth factor in the smart city market is the manifestation of governments' interests for platform providers over independent smart solutions. Some of the major players in this market use their own platform to provide this type of service, Smart City services. Some of these platforms are: CityIQ by Current; Cisco Kinetic by CISCO; OceanConnect by Huawei; Hitachi Vantara by Hitachi; CityNext by Microsoft; IMPACT IoT platform by Nokia; City Intelligent Platform by Siemens.

Technological developments have increased the complexity of the relationship between the cyber domain and the physical domain in many application domains, i.e. manufacturing, healthcare, transport, automobiles, etc. [2]. This complex interaction requirement leads to efficient integration of the cyber domain and the physical domain by Cyber-Physical Systems (CPS) [23]. CPS is a deeply connected communication network in which, as seen in Fig. 1, many embedded computing devices, smart controllers, physical environments, and humans communicate systematically with each other [24, 28].

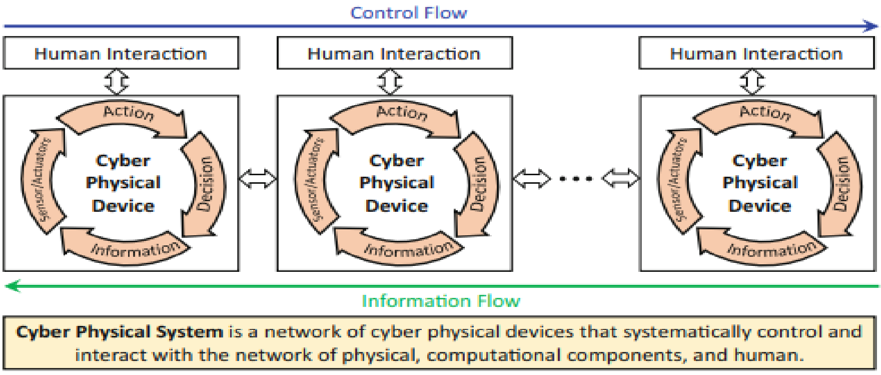


Fig. 1. Key features of a CPS
Source: *[11]*

Usually, by sharing the information and communicating the appropriate control commands, CPS systems communicate with each other. CPS uses sensors to collect data from the physical domain and analyze it by controllers to issue the control commands required to guide/control the physical domain via actuators. The complex and massive integration with humans of networked computing equipment, sensors and actuators in CPS plays an important role in the growth of the Internet of

Things (IoT), in which various cyber and physical (sub)-systems are connected over the Internet [11, 15]. IoT has revolutionized many application fields, such as smart traffic control, healthcare, transport networks, industrial automation, smart grids, autonomous vehicles, and smart homes/buildings due to their ability to manage such complex interactions (as shown in Fig. 2).

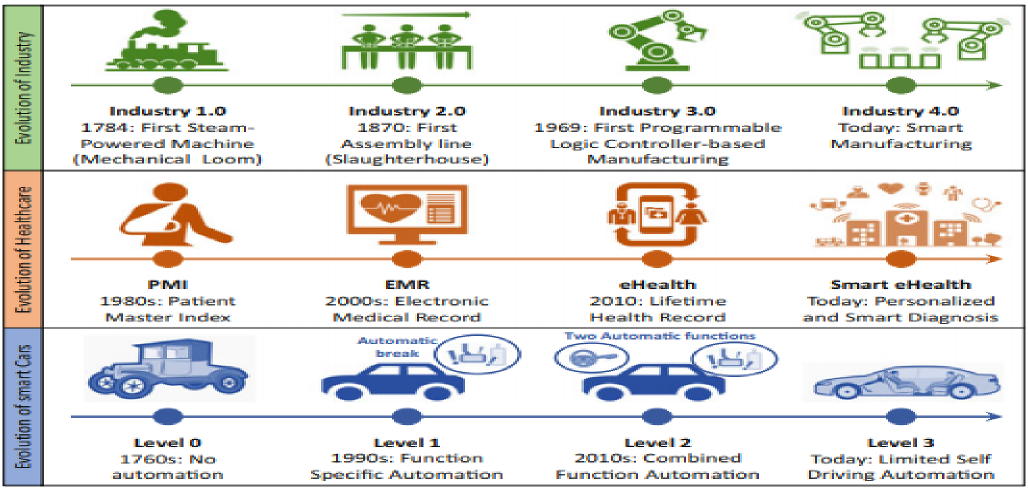

Evolution of Industry
Industry 1.0
1784: First Steam-Powered Machine (Mechanical Loom)
Industry 2.0
1870: First Assembly line (Slaughterhouse)
Industry 3.0
1969: First Programmable Logic Controller-based Manufacturing
Industry 4.0
Today: Smart Manufacturing
Evolution of Healthcare
PMI
1980s: Patient Master Index
EMR
2000s: Electronic Medical Record
eHealth
2010: Lifetime Health Record
Smart eHealth
Today: Personalized and Smart Diagnosis
Evolution of smart Cars
Automatic break
Two Automatic functions
Level 0
1760s: No automation
Level 1
1990s: Function Specific Automation
Level 2
2010s: Combined Function Automation
Level 3
Today: Limited Self Driving Automation

Fig. 2. Timeline of the technological advancements in different applications
Source: *[15]*

In relation to its use in the corresponding industries, the scope and use/opportunities of IoT differ (as shown in Fig. 3). For example, many application fields, such as multimedia, manufacturing, financial firms, etc., used the IoT in several of their applications in 2017, primarily in protection and surveillance, resources, and asset management [21] (as shown in Fig. 3).

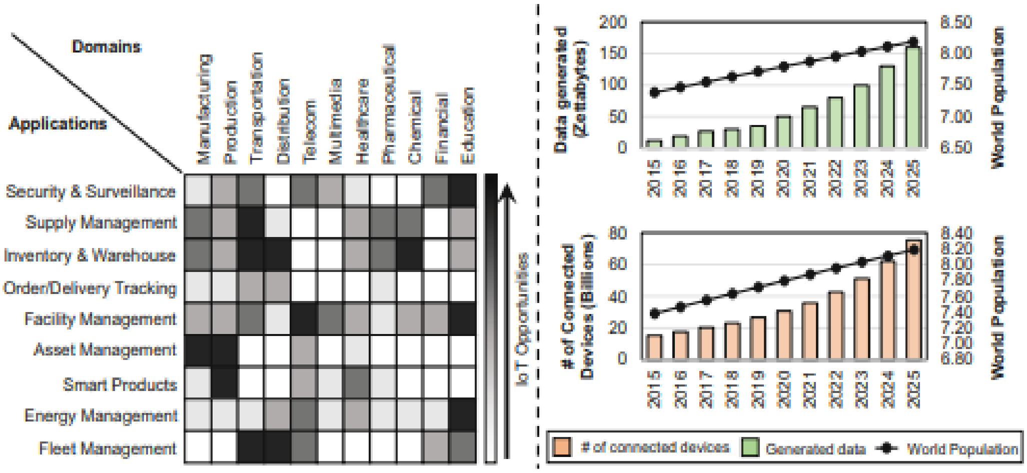


Fig. 3. On the left, a heat map shows the opportunities and scope of the IoT for different applications
Source: *[21].*

The following challenges are coming with the extensive use of IoT in industries, especially in safety-critical applications:

1. One of the main challenges is dealing with the enormous amount of data generated that needs to be stored and processed. An analytical survey by the ”Statista” group for example, indicates that by 2025, almost 75.42 billion connected devices will be used, producing approximately 180 zettabytes of measured data [33], as shown in Fig. 3.
2. CPS is vulnerable to multiple security threats due to the dynamic convergence of the cyber domain (i.e. networked computing devices), physical domain (i.e. actuators) and humans [18, 25]. Therefore many real-world security incidents have been documented. Blocking the city water pipeline [4, 32, 34], hacking the pacemaker [3, 13], anti-lock braking system [29], wheel speed sensor spoofing in smart cars [20, 30], relay attacks (to disable lights)[9] and other industrial attacks [1, 19, 22] are some of the prominent incidents. These incidents allow researchers to answer the following main research questions:
   - How to ensure secure data acquisition from sensors?
   - How to ensure the security of the controllers and corresponding control signals over different CPS layers?
   - How to ensure secure inter-layer, intra-layer, and stack communication of data and control signals?

Researchers have suggested multiple security measures to answer these research concerns, i.e. online identification of anomalies [16, 35], anonymization [11], trusted computing (attestation) [10, 26], data and control signal encryption [8] and verifiable computation. However, the growing number of connected devices and the corresponding data, and resource constraints, make it very difficult to develop safety measures, especially in CPS battery-operated devices. Therefore in order to cope with volatile operating environments over a lifetime, protection measures in the CPS need to be energy efficient yet adaptive and sustainable. In addition, these security mechanisms need to be sufficiently intelligent to adjust to the unexpected attack surface for sustainable stable CPS.

2. Smart city

The goal of this work is to recognize the key trends in scientific literature characterizing smart urban mobility. "Smart city" is currently the most "in vogue" term among academics and administrative/governmental representatives from all over the world that has been discussed and examined. This multidimensional concept is focused primarily on smart technology structured around a few main elements: smart mobility, smart environment, smart governance, smart living, and all that targets the well-being of people. Due to its major effect on the environment through emissions as well as living by needing intelligent transport systems, this work focuses on a hot subject: mobility. A significant topic of modern cities is addressed, namely smart mobility, presenting the key problems and potential solutions, as well as the stakeholders involved and responsible for their implementation.

In recent years, the idea of a smart city, especially smart mobility and intelligent transport systems, has become very common. The authors began verifying the number of publications available in the Web of Science and Scopus databases to examine current research trends among publications dealing with urban smart mobility or the Intelligent Transport System (ITS) (Fig. 4). A study of the number of publications after 2000 was carried out by the scientists, when the number of publications surpassed seven in the Scopus database and two in the WoS database.

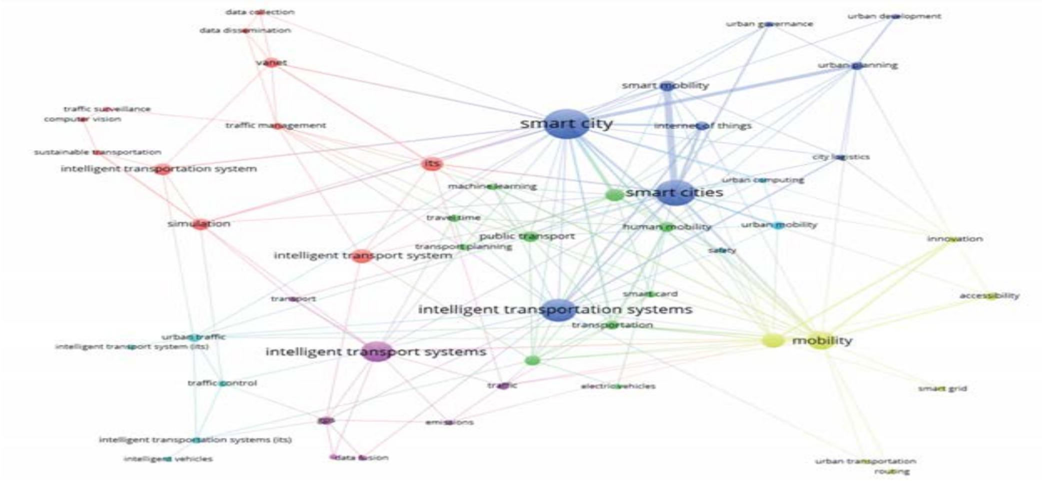


Fig. 4. urban smart mobility or intelligent transport system
***Source:** [12]*

3. PS security

A conventional security framework tests the conduct of adventure contact and other side-channel constraints. Nevertheless, these procedures do not apply to cyber-physical systems (CPS) for intricate interdependencies on different layers, exclusively reservations in physical layers [28, 14]. For example, Table 1 illustrates some of the real-world cyber-physical systems (CPS) attacks that exploit the weaknesses at different cyber physical systems (CPS) layers. Subsequently, old-style definitions for threats and consistent threat models cannot be used to examine and progress security measures in cyber physical systems (CPS) [17]. Hence, here in the chapter, we elaborate security exposures in cyber-physical systems (CPS) at different layers of CPS, particular payloads, and linked threat models.

3.1 Security attacks in CPS

The security attacks in CPS differ from traditional cyber attacks to cyber-physical attacks that exploit the vulnerabilities at different CPS layers [5, 28, 36]. Characteristically, these vulnerabilities are characterized based on the cyber-physical systems (CPS) layers. Figure 4 shows different security attacks for CPS with respect to various cyber-physical systems (CPS) layers.

Table 1. Examples of the real-world security attacks on different layers of CPS

CPS layer	Applications	Attacks	Description
Sensors/Actuators	Smart grids	False data injection	Interrupt the data acquisition by feeding false data to sensors
Network	Smart grids	Cyber extortion	Hack and exploit the CPS component that can connect to Internet [37]
Sensors/Actuators	Control system	False data/Signal injection	Corrupting the sensor data (sensors) or control commands (actuators) [38, 39]
Network	Control system	Replay attacks	Hack the network to delay or corrupt control commands [40]
Network or physical	Smart grids	Aurora experiment	Maliciously interrupt brakes [41, 42]
Network	Smart healthcare	False data injection	Corrupt the patient record [43]
Physical	Smart healthcare	Unauthorized injection	Remotely send the false commands to insulin injection pump [43]
Network	Smart cars	Denial of service	Disable the communication with brakes [44, 45]

Source: *[5]*

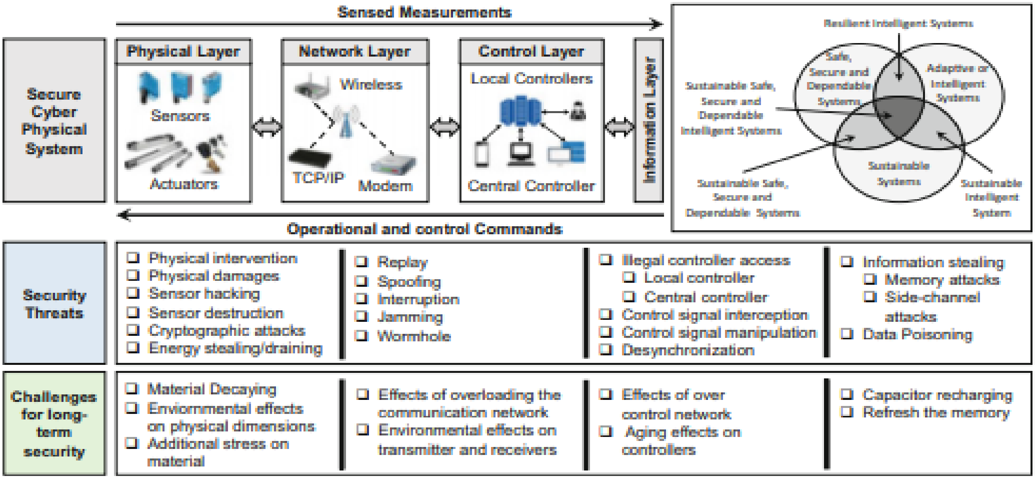
4. Designing a secure CPS

The above-mentioned security vulnerabilities increase thoughtful alarms over the usage of cyber-physical systems (CPS) in safety-critical applications, like smart home appliances, autonomous vehicles, smart healthcare, industry 4.0. Consequently, there is a compulsory need to develop security measures that are adaptive to unanticipated attacks and bearable enough to deal with long-term influence of environmental changes and technological developments [24].

In short, to design sustainable and secure cyber-physical systems (CPS), the mentioned research challenges must be resolved:

Inclusion of the security in design constraints: Multiple security measures for cyber-physical systems are being put forward so far, but security is not contained within the design constraint in cyber-physical systems design cycle. Consequently, it is domineering to integrate security constrictions into traditional design constraints.

Resource-efficient adaptive design: The complex interaction and integration of physical-domain and cyber-domain make cyber-physical systems extremely vulnerable to unexpected attack surfaces. Furthermore, the restricted resources (in battery-operated CPS) also limit the runtime security measures. So, it is domineering to develop such security measures that are adaptive and also accomplish the energy budget and resources constraints.


Sensed Measurements
Secure Cyber Physical System
Physical Layer
Sensors
Actuators
Network Layer
Wireless
TCP/IP
Modem
Control Layer
Local Controllers
Central Controller
Information Layer
Operational and control Commands
Resilient Intelligent Systems
Safe, Secure and Dependable Systems
Adaptive or Intelligent Systems
Sustainable Safe, Secure and Dependable Intelligent Systems
Sustainable Systems
Sustainable Safe, Secure and Dependable Systems
Sustainable Intelligent System

Security Threats	□ Physical intervention □ Physical damages □ Sensor hacking □ Sensor destruction □ Cryptographic attacks □ Energy stealing/draining	□ Replay □ Spoofing □ Interruption □ Jamming □ Wormhole	□ Illegal controller access □ Local controller □ Central controller □ Control signal interception □ Control signal manipulation □ Desynchronization	□ Information stealing □ Memory attacks □ Side-channel attacks □ Data Poisoning
Challenges for long-term security	□ Material Decaying □ Enviornmental effects on physical dimensions □ Additional stress on material	□ Effects of overloading the communication network □ Environmental effects on transmitter and receivers	□ Effects of over control network □ Aging effects on controllers	□ Capacitor recharging □ Refresh the memory

Fig. 4. Security attacks for CPS with respect to several CPS layers and associated challenges for long-term and sustainable security measures for CPS

Source: *[24]*

Secure communication: To design a secure cyber-physical system, it is imperative to guarantee the secure interaction and integration of numerous heterogeneous cyber-physical devices.

Data confidentiality: Information and control signals are an integral part of cyber-physical systems. Thus, it is imperative to ensure the protected communication and storage of the information and control signals.

5. Conclusion

The paper focused on smart cities, how they have developed in recent years, estimates in this area and how it will develop in the future. Most smart cities are made with the help of ICT, without whose help one could not develop, implement and promote. For the related work part, the security of the CPS was taken, a conventional security framework; described security attacks and how they differ from traditional cyber attacks. Also for the related work part, there was talk about designing such a secure CPS.

Acknowledgements

This paper was partially supported by UEFISCDI Romania and MCI through Eureka ITEA projects PARFAIT and SOLOMON, and funded in part by European Union's Horizon 2020 research and innovation program under grant agreements No. 872698 (HUBCAP) and No. 883522 (S4AllCities).

References

[1] Antonioli, D. et al. (2018), *Taking control: design and implementation of botnets for cyber-physical attacks with CPSBot*. Preprint. arXiv:1802.00152

[2] Babiceanu, R.F. et al. (2016), *Big data and virtualization for manufacturing cyber-physical systems: a survey of the current status and future outlook.* Comput. Ind. 81, 128–137

[3] Beavers, J.L. et al. (2019), *Hacking NHS pacemakers: a feasibility study*, in IEEE ICGS3, pp. 206–212

[4] Cerrudo, C. (2015), *An emerging us (and world) threat: cities wide open to cyber attacks. Secur. Smart Cities,* No. 17, 137–151

[5] Chhetri, S.R. et al. (2017), *Cross-domain security of cyber-physical systems*, in IEEE ASP-DAC, pp. 200–205

[6] Chourabi, H., Nam, T., Walker, S., Gil-Garcia, J. R., Mellouli, S., Nahon, K., Pardo, T. A., & Scholl, H. J. (2012), *Understanding smart cities: An integrative framework*. In Proceedings of the 45th Annual Hawaii International Conference on System Sciences, HICSS-45 (pp. 2289-2297). (Proceedings of the Annual Hawaii International Conference on System Sciences). IEEE Computer Society. https://doi.org/10.1109/HICSS.2012.615)

[7] Dong, Z. (2014), *Smart grid cybersecurity.* In: Proceedings of the 2014 13th International Conference on Control Automation Robotics and Vision. pp. 1-2 .

[8] Essa, A. et al. (2018), *Cyber physical sensors system security: threats, vulnerabilities, and solutions*, in IEEE ICSGSC, pp. 62–67

[9] Francillon, A., Danev, B., Capkun, S. (2011), *Relay attacks on passive keyless entry and start systems in modern cars*, in NDSS,

[10] Ghaeini, H.R. et al. (2019), *Patt: physics-based attestation of control systems*, in RAID, pp. 165–180

[11] Giraldo, J. et al. (2017), *Security and privacy in cyber-physical systems: a survey of surveys*. IEEE Des. Test 34(4), 7–17

[12] GOV.UK. 2020. *Smart City Market: UK Opportunities*. [online] Available at: <https://www.gov.uk/government/publications/smart-city-market-uk-opportunities> [Accessed 26 November 2020].

[13] Groeneveld, S.A., Jongejan, N., Fiolet, A.T.L. et al. (2019), *Hacking into a pacemaker; risks of smart healthcare devices*. Nederlands tijdschrift voor geneeskunde 163

[14] Han, S. et al. (2014), *Intrusion detection in cyber-physical systems: techniques and challenges*. IEEE Syst. J. 8(4), 1052–1062

[15] Humayedet, A. al. (2017), *Cyber-physical systems security—a survey*. IEEE Internet Things J. 4(6), 1802–1831

[16] Jin, S. et al. (2018), *Changepoint-based anomaly detection for prognostic diagnosis in a core router system*, in IEEE TCAD

[17] Konstantinou, C. et al. (2015), *Cyber-physical systems: a security perspective,* in IEEE ETS, pp. 1–8

[18] Kriebel, F. et al.(2018), *Robustness for smart cyber physical systems and internet-of-things: from adaptive robustness methods to reliability and security for machine learning*, in IEEE ISVLSI, pp. 581–586

[19] Lin, C.-T. et al. (2017), *Cyber attack and defense on industry control systems*, in IEEE Conference on Dependable and Secure Computing, pp. 524–526

[20] Narayanan, S.N. et al. (2019), *Security in smart cyber-physical systems: a case study on smart grids and smart cars*, in Smart Cities Cybersecurity and Privacy (Elsevier, Amsterdam), pp. 147–163

[21] Pelino, M. et al. (2017), *The Internet of Things Heat Map*

[22] Preuveneers, D. et al. (2017), *The intelligent industry of the future: a survey on emerging trends, research challenges and opportunities in industry 4.0*. J. Ambient Intell. Smart Environ. 9(3), 287–298

[23] Rajkumar, R. et al. (2010), *Cyber-physical systems: the next computing revolution*, in IEEE DAC, pp. 731–736

[24] Ratasich, D. et al. (2019), *A roadmap toward the resilient internet of things for cyber-physical systems*. IEEE Access 7, 13260–13283

[25] Rehman, S. et al. (2018), *Hardware and software techniques for heterogeneous fault-tolerance*, in IEEE IOLTS, pp. 115–118

[26] Roth, T. et al. (2013), *Physical attestation of cyber processes in the smart grid*, in Springer ICIIS, pp. 96–107

[27] Sengan, S., Subramaniyaswamy, V., Nair, S. K., Indragandhi, V., Manikandan, J., & Ravi, L. (2020), *Enhancing cyber–physical systems with hybrid smart city cyber security architecture for secure public data-smart network*. Future Generation Computer Systems, 112, pp. 724-737.

[28] Shafique, M. et al. (2018), *Intelligent security measures for smart cyber physical systems*, in Euromicro/IEEE DSD, pp. 280–287

[29] Shoukry, Y. et al. (2013), *Non-invasive spoofing attacks for anti-lock braking systems*, in International Workshop on Cryptographic Hardware and Embedded Systems (Springer, Berlin), pp. 55–72

[30] Shoukry, Y. et al. (2015), *Pycra: physical challenge-response authentication for active sensors under spoofing attacks*, in AM CCS, pp. 1004–1015

[31] Smart Cities Market Report 2020 - Global Forecast to 2025: *Market Size is Expected to Grow from $410.8 Billion in 2020 to $820.7 Billion* https://www.globenewswire.com/news-release/2020/10/05/2103315/0/en/Smart-Cities-Market-Report-2020-Global-Forecast-to-2025-Market-Size-is-Expected-to-Grow-from-410-8-Billion-in-2020-to-820-7-Billion.html , date: 26.11.2020

[32] Sowby, R. B. (2016), *Hydroterrorism: a threat to water resources*. Wasatch Water Rev. 1–4

[33] Statista. *Internet of things (IoT) connected devices installed base worldwide from 2015 to 2025* (in billions) (2019). https://www.statista.com/statistics/471264/iot-number-of-connecteddevices-worldwide/. Accessed 04 Nov 2019

[34] Timashev, S.A. (2019), *Cyber reliability, resilience, and safety of physical infrastructures*, in IOP Conference Series: Materials Science and Engineering, vol. 481, p. 012009

[35] Wang, P. et al. (2019), *Cyber-physical anomaly detection for power grid with machine learning*, in Industrial Control Systems Security and Resiliency (Springer, Berlin), pp. 31–49

[36] Wurm, J. et al. (2016), *Introduction to cyber-physical system security: a cross-layer perspective*. IEEE Trans. Multi-Scale Comput. Syst. 3(3), 215–227

[37] Nakashima, E. et al., Hackers have attacked foreign utilities, CIA analyst says. Washington Post, 19, 2008

[38] Fawzi, H. et al., Secure estimation and control for cyber-physical systems under adversarial attacks. IEEE Trans. Autom. Control 59(6), 1454–1467 (2014)

[39] Pasqualetti, F. et al., Attack detection and identification in cyber-physical systems. IEEE Trans. Autom. Control 58(11), 2715–2729 (2013)

[40] Mo, Y. et al., Detecting integrity attacks on SCADA systems. IEEE Trans. Control Syst. Technol. 22(4), 1396–1407 (2013)

[41] Zeller, M., Myth or reality—does the aurora vulnerability pose a risk to my generator?, in IEEE Conference for Protective Relay Engineers (2011), pp. 130–136

[42] Islam, S. et al., Physical layer security for the smart grid: vulnerabilities, threats and countermeasures. IEEE Trans. Ind. Inform. 15, 6522–6530 (2019)

[43] Li, C. et al., Hijacking an insulin pump: security attacks and defenses for a diabetes therapy system, in IEEE International Conference on e-Health Networking, Applications and Services (2011), pp. 150–156 22 F. Khalid et al.

[44] Koscher, K. et al., Experimental security analysis of a modern automobile, in IEEE Symposium on Security and Privacy (2010), pp. 447–462

[45] Hoppe, T. et al., Security threats to automotive can networks—practical examples and selected short-term countermeasures. Reliab. Eng. Syst. Saf. 96(1), 11–25 (2011)

[46] Suciu, G., Necula, L.-A., Jelea, V., Cristea, D.-S., Rusu, C.-C., Istodie, L.-R. and Ivanov, M., (2019). Smart City platform based on citizen reporting services