Smart Factory Environment: Review of Security Threats and Risks

Petra Zorić[1(✉)], Mario Musa[2], and Tibor Mijo Kuljanić[3]

[1] Faculty of Transport and Traffic Sciences, University of Zagreb, Vukelićeva 4, 10000 Zagreb, Croatia
petra.zoric@fpz.unizg.hr
[2] Hrvatska Lutrija D.O.O., Ulica grada Vukovara 72, 10000 Zagreb, Croatia
mario.musa@lutrija.hr
[3] HEP ODS D.O.O., Ulica grada Vukovara 37, 10000 Zagreb, Croatia

Abstract. The Industry 4.0 concept represents a new way of managing production processes. With its application, connections between people, systems, and objects become more complex, creating a dynamic and real-time optimized network. With the establishment of such a network, a smart factory is created. In a smart factory environment, each process must be precisely planned into a connected functional unit in order for the production process to run smoothly. A factory designed in this way has a complex information and communication infrastructure, and thus potentially more significant security threats and risks that it faces than a factory that operates traditionally. The technologies found in the smart factory environment have been evolving for some time. However, their integration with industrial systems poses new security challenges. The smart factory environment's rapid development imposes the need to ensure safe interaction between the production system elements. This paper provides an insight into the environment of a smart factory and the information and communication technologies that enable its operation. The paper provides an overview of security threats and risks that such an environment faces based on the acquired knowledge.

Keywords: Industry 4.0 · Information and communication technology · Manufacturing system

1 Introduction

The fourth industrial revolution era represents an era of the enormous potential for the development of innovation and companies' growth in the market. Production is becoming increasingly digital as the industry adopts automation. The digital transformation of the production process and the creation of added value of the services that manufacturing companies provide to end users are the Industry 4.0 environment's main features. With the Industry 4.0 concept introduction, there are changes in company strategies, business models, value chains, production processes, services, and relationships with stakeholders who participate in one production process.

D. Perakovic and L. Knapcikova (Eds.): FABULOUS 2021, LNICST 382, pp. 203–214, 2021.
https://doi.org/10.1007/978-3-030-78459-1_15

One of the crucial components of Industry 4.0 development is a smart factory created by establishing a real-time dynamic, and optimized network. As part of this network, smart sensors, implemented in factories and workplaces, are the drivers of Industry 4.0 and the Internet of Things (IoT). It is possible to achieve new ways of data analysis, which results in adaptable production processes that ensure and improve performance in the industrial sector using sensors.

Failure of certain parts of the industrial facility can endanger the safety and quality of the product and lead to serious personal injuries and cause material damage. The combination of smart sensors with specific technology implemented in a smart factory environment, such as artificial intelligence, leads to self-testing, monitoring, and improving the sensor's performance, thus reducing the number of damaged data.

Despite the many opportunities provided to all stakeholders in the smart factory environment, new vulnerabilities have been created that must be managed to have a positive impact on both business and society as a whole. Complex and precise systems, such as a smart factory, bring with them certain risks and challenges in security.

Terms such as Industry 4.0 or smart factory have seen an exponential increase in the number of published scientific and professional papers in recent years. The topic of security in such an environment is still insufficiently researched and represented in the currently available scientific and professional literature. For this reason, this paper deals with the presentation of security threats and challenges that are possible in a smart factory environment. This paper aims to provide insight into the most critical information and communication technologies in a smart factory environment and present the security risks and threats possible in a smart factory environment.

2 Smart Factory Environment

Smart factories (Fig. 1) are production systems that respond in real-time to meet the changing requirements and needs of end-users and the factory's conditions and supply network. The goal of such a system is to optimize production processes fully. In one highly digitized production plant like a smart factory, all systems are interconnected and participate in the exchange of data of every aspect of production in real-time. The communication between different systems in such an environment takes place without significant interference and completely imperceptibly, and the entire production process takes place automatically without human interference.

Data is a crucial aspect of smart factories. When transferring data through systems to connect all production operations, the entire facility in which the smart factory environment is implemented can learn and adapt to the business's changing needs. This concludes that smart factories are intelligent production systems that can dynamically adapt to changes that occur due to their ability to learn on the go.

This achievement of a high level of automation of production processes and efficiency is enabled by using many currently available technologies, some of the most critical IoT, artificial intelligence (AI), and Machine-to-Machine communication (M2M). Above mentioned creates specific products ordered by end-users and creates entire related value chains [2]. Increasing productivity and reducing labor costs by adopting smart factories

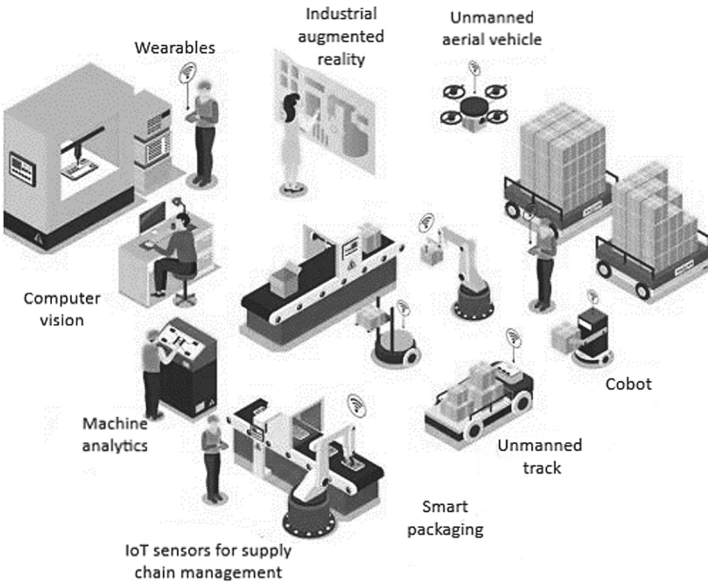

Fig. 1. Smart factory concept [1]

powered by innovative technologies can be significant. For example, by 2025, the adoption of smart factories launched by AI could increase productivity by 30%, while labor costs would decrease by 18–33% [3].

New business models are accelerating the manufacturing industry's transformation, changing the current business methods and market structure, and establishing digital supply networks (Fig. 2) [4].

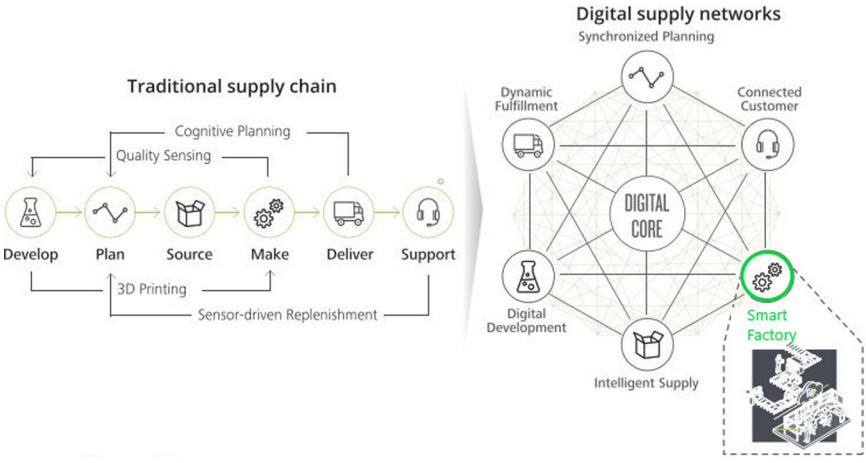

Fig. 2. The transition from a traditional supply chain to a digital supply network [4]

In the model shown in Fig. 2, it can be seen that traditional supply chains are linear. Today's supply chains are transformed into a dynamic system in which all the links are interconnected - the digital supply network. This network integrates information from many different sources and from various locations to initiate the physical act of production and distribution of the service, i.e., the end product of a smart factory. This method allows for a greater connection between areas that did not even exist before. Communication between different network parts is multidirectional, creating a link between traditionally unconnected links in the supply chain.

2.1 The Main Features of a Smart Factory

Smart factories can significantly help the manufacturing industry mostly because the development and application of digital technology can offer greater efficiency at all manufacturing processes, better quality products with fewer errors, and greater flexibility of the manufacturing processes themselves. There are five main features through which a smart factory can be described: connectivity, optimization, transparency, proactivity, and agility [5]. All of these features individually can play a significant role in enabling more informed decisions and improving the production process. Given that each production process is specific and that for this reason, the two smart factories are unlikely to look the same, manufacturers decide which of the features are relevant to meet their production needs.

Connectivity is one of the most crucial features of any smart factory. Linking core processes and materials to create data crucial for real-time decision making is one of the main requirements of a smart factory environment. Smart sensors equipped with the asset allow the systems to update the data continuously. Together with information coming from the market, they provide insight into supply chain processes, thus ensuring the supply network's greater efficiency.

Optimization enables the execution of operations in the production process with minimal manual interventions and high reliability. Optimized energy consumption with workflow automation leads to increased revenue and quality of work and decreased costs and waste.

The transparency of data collected in a smart factory environment allows for greater visibility of production processes based on the cloud's available data. The transparent network enables more excellent monitoring of the facility in monitoring the execution of the process in real-time.

As a smart factory feature, proactivity provides the system with anticipation and action before specific challenges arise. This feature may include identifying anomalies, identifying and predicting the resolution of quality problems, and monitoring safety and maintenance concerns. This can improve the time frame of a process, quality but also prevent security problems.

Agility allows smart factories to adapt to changes in production with minimal intervention. Independent configuration of equipment and material flow depending on the type of product and the impact of changes on the product in real-time reduces downtime and increases profits.

These features allow manufacturers greater visibility of their assets and system and cope with some of the challenges faced by more traditional factory structures. This

improves productivity in the production process itself and more significant responses to fluctuations in suppliers and customers' conditions.

2.2 Advantages of a Smart Factory

Asset efficiency is one of the most prominent advantages of a smart factory. Continuous analysis of large amounts of data reveals asset performance issues that may require some corrective optimization. This kind of self-correction distinguishes a smart factory from traditional automation leading to greater overall asset efficiency. Smart factories optimize different assets and help the organization get the most out of them. It also helps an organization take advantage of all these resources' synergy to gain a significant advantage in productivity and revenue.

The maintenance problems characteristic of traditional factories does not occur in smart factories that overcome this problem with proactive, predictive maintenance capabilities. In this way, downtime or losses in business are eliminated. The scalable infrastructure of a smart factory environment is cost-effective because it can be easily expanded to meet the manufacturing process's growing needs [6].

A smart factory's self-optimization characteristic can predict and detect trends in machine quality failures in the manufacturing process. A more optimized quality process could lead to a higher quality product with fewer defects and recalls in production. Such a process has traditionally led to more cost-effective processes. A better process could also mean an integrated view of the supply network with fast, non-delayed responses.

It is also important to note a smart factory's self-sustainability that can replace specific roles that require repetitive and tedious activities. However, the human worker's role in a smart factory environment can take on a higher level of judgment and discretion on the spot, which can lead to greater job satisfaction and reduced traffic. Also, in terms of safety, greater process autonomy may provide less human error potential, including industrial accidents that cause injuries [4].

It is also important to emphasize that governments worldwide have recognized the importance of the new generation of production and have become active in investment in infrastructure, sponsorships, tax breaks, and the like to facilitate its implementation in companies [7].

3 The Most Crucial Information and Communication Technologies in a Smart Factory Environment

Equipment located in a smart factory environment generates a large amount of data during the execution of specific actions in the production process. Such data are not structured and are usually unused. However, with the advent of IoT and Big Data technologies, such data analysis takes place with ease. Equipment should be ready to collect data and transfer it to a platform that can analyze it. To be able to do this, it must be equipped with sensors. It can support industry-standard protocols such as TCP/IP, SECS (SEMI Equipment Communications Standard)/GEM (Generic Equipment Model) or OPC (Open Platform Communications) [8].

Smart sensors have become devices with detection and self-awareness capabilities. They are designed as IoT components that convert real-time information into digital data transmitted to the gateway. They can predict and monitor scenarios in real-time and take corrective action in an instant [1].

Nowadays, millions of such embedded devices are used in security-critical applications such as critical infrastructure or industrial control systems. Examples include necessary technology such as RFID (Radio-Frequency Identification) to identify and track products in supply chain scenarios to smartphones and wearable equipment that have significant computing capabilities and Internet connections. Such a network enables new services in the industrial sector and is known as IoT [9].

Industrial IoT (Fig. 3) is a collective name for automation, intelligent computer systems, and classical manufacturing engineering [10]. It consists of vertical and horizontal connections of people, object machines, and information and communication technology systems in real-time, enabling dynamic control of complex systems [11].

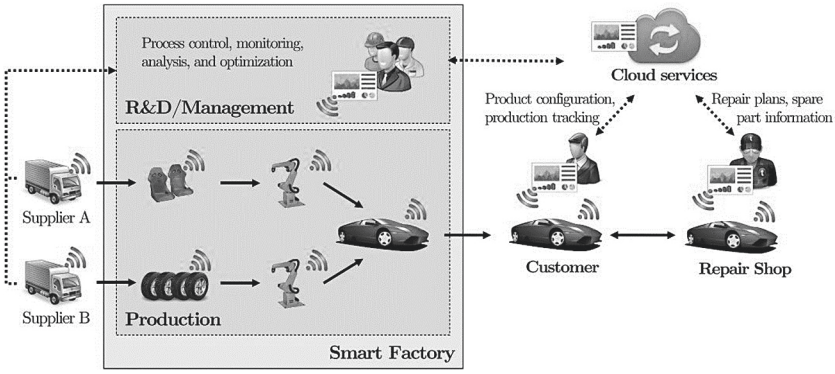

Fig. 3. Industrial IoT in smart factory environment [10]

Programmable logic controllers characteristic of classic factories have been replaced by more advanced cyber physical systems (CPS) whose prominent roles are to meet agile and dynamic production requirements and improve the industry's efficiency as a whole. CPS is the foundation of industrial IoT and represents computer platforms that monitor and control production's physical processes. Such systems typically communicate via closed industrial communication networks via IoT but are often connected to the Internet [12–15]. CPS can be facilities, products, devices, buildings, production facilities, or logistics components that contain embedded systems [16].

In addition to the above, Fig. 4 shows the various technologies present in the smart factory environment needed to achieve innovation and improve production processes' capacity. M2M communication in such an environment is direct and intensive and refers to a technology that facilitates direct communication between devices in a network without human assistance. Advanced industrial robots are designed for complex tasks and can learn from their mistakes and improve their performance.

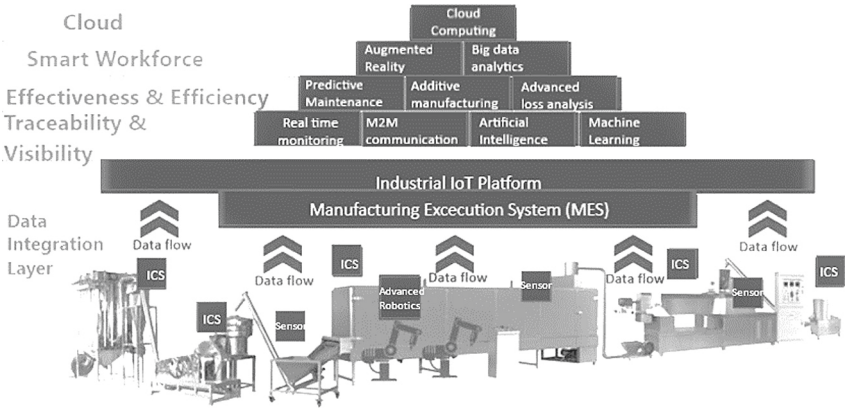

Fig. 4. Technologies within smart factory environment [18]

The evolution of big data presents challenges for data management itself. Traditional data tools, procedures, and infrastructures are not designed to manage diverse and large amounts of data. For this reason, a new immense data management discipline has been developed. Techniques have been developed to address storage, contextualization, integration, and access to extensive data to support data processing and learning. In a smart factory environment, big data analytics is necessary to test vast amounts of different types of data sets generated by smart sensors or devices in real-time [17].

AI and Machine Learning (ML) have revolutionized numerous industries in recent years. AI algorithms allow computers and digital machines to perform tasks accurately related to intelligent human beings. ML algorithms, on the other hand, allow computers to operate and improve their prediction capabilities without explicit programming. The most significant difference is visible in the requirement of human action with these technologies. In AI, the human aspect is useless, while in ML, a minimal level of human involvement in the production process is required [3].

Predictive solutions in a smart factory environment monitor the equipment's condition and predict the time of occurrence of a particular equipment failure with the aim of efficient maintenance. Real-time monitoring includes technologies that serve to collect and aggregate security data from system components and monitor and analyze events taking place online. Advanced loss analysis includes methods of analysis of different types of losses to eliminate and/or reduce them.

Additive manufacturing technologies, such as 3D printing, allow creating objects of different geometric shapes by adding materials. Augmented Reality in a smart factory environment is used to improve the efficiency of manual assembly tasks. Cloud Computing solutions provide access to shared sets of resources, such as networks, servers, and applications [18].

The 5G network has the potential to revolutionize IoT and industrial IoT. From a security perspective, 5G adds an essential new functionality to EAP-TLS (Extensible Authentication Protocol Transport Layer Security) authentication that allows non-SIM-based credentials such as certificates [19].

4 Security Threats and Risks

In the traditional production process, the security of production was achieved with physical isolation carried out based on strict access rights management. The smart factory is connected by nature, and the essential part of the factory networks is connected to wireless networks and more expansive corporate systems. Devices involved in the manufacturing process become accessible to unauthorized attacks. For this reason, the risk of cybersecurity poses more significant concern in such an environment than in a traditional manufacturing facility environment. Such concerns need to be addressed within the overall smart factory architecture [4].

Each information and communication system is most often defined through three fundamental principles, known as the CIA triad: confidentiality, accessibility, and integrity [20]. Confidentiality is related to ensuring the protection of property inspections from unauthorized entities. Integrity is focused on protecting assets from unauthorized alterations, while availability is a feature related to allowing access to assets to authorized entities at any time allowed. Availability and integrity are of paramount importance in the production system because data gaps and false data can lead to significant changes in the processes themselves or production [21].

Many attacks are motivated by political reasons, but they can also be motivated by financial reasons [22]. Cyber-attacks on a smart factory often pursue one of the following three goals [23]:

- Theft of personal data of end customers - criminals use a unique integrated CRM (Customer Relationship Management) system, for example, access to the operating system through heating and air conditioning suppliers,
- Interruption of the entire system - can cause dramatic losses associated with hacker attacks,
- Industrial espionage and sabotage - technology vulnerabilities can be exploited to steal intellectual property and gain a significant competitive advantage over competitors.

Although production systems in a smart factory environment are designed and set up in such a way as to be isolated, and there is great confidence in such systems, minimal integrity checks are performed to prevent malicious activity. Systems and machines that are potentially weak links in the security chain and can be maliciously used to damage manufactured goods or cause failures are MES (Manufacturing Execution System), HMI (Human Machine Interfaces), and industrial IoT devices. An experiment [24] was also conducted to check how and to what extent malicious attacks can affect the insufficiently protected information and communication system of the production environment. The feasibility of several attacks was tested under different assumptions of the attacker model, and five attacks were analyzed (Fig. 5).

Due to the high level of interconnection of production and IT components and integration based on information technology, the physical production process's operation depends on the smooth operation of information and communication services that lead to them. For this reason, smart factory networks face new threats to information and

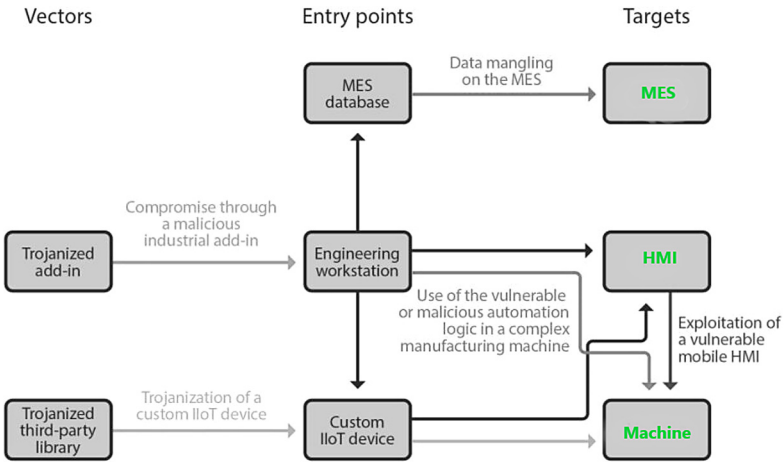

Fig. 5. Overview of possible attacks in the smart factory environment [24]

communication security concerning four dimensions: availability, access, accuracy, and accountability. Consequently, smart factory security threats arise from four channels [25]:

- Software errors and hardware malfunctions,
- Open Internet protocols used in such an environment and standard networks,
- Numerous parties involved in the execution of the production process and
- A large number of devices that can be accessed.

Technologies that are located within a smart factory environment enable its operation to carry with them specific safety requirements. Due to the different requirements that such technologies have and are essential for their proper implementation, new risk categories are generated because vulnerabilities and threats increase throughout the smart factory environment. All components found in such a dynamic system become security-critical as industrial surveillance systems become the target of malicious cyber-attacks [26, 27]. The protection of personal data is also an essential aspect of the smart factory environment's security. The BYOD (Bring Your Own Device) approach carries with it many threats [28]. Confidential data stored on connected devices, which can be accessed in more ways than ever before, offers a way for infiltrators to infiltrate the network, increasing industrial espionage risk.

Threats can come from various sources, such as worker activity in such an environment or hacker attacks. They can cause various damages in the business process itself and even interrupt the business [29]. One of the most critical threats in the smart factory environment is the unusability of the on-demand service. Given the growing dependence of production infrastructure on the reliable functioning of information and communication services, data and access to them are crucial.

DDoS (Distributed Denial of Service) attacks are among the most significant threats in the modern production environment [30]. This attack seeks to prohibit legitimate users

from accessing a property in a production environment. They use multiple vulnerable systems infected with malware, and such a threat is difficult to protect for any externally accessible interface [21, 28].

It is imperative to invest in preventive measures and active defense against attacks to ensure connected production systems. These include cryptographic countermeasures, intrusion detection systems, proactive staff training, and good incident management. However, there is still insufficient awareness of the importance of cybersecurity in the manufacturing industry. Given the investments in digital technology significant every year, 34% of manufacturers do not include cybersecurity in their risk register, which is a devastating and worrying statistic [31].

5 Conclusion

The constant progress of information and communication technologies applied in the manufacturing industry promises excellent potential for developing production processes, which leads to a paradigm shift in production. Emerging production systems enable automated and flexible production facilities and can economically create personalized products.

However, such systems' interconnectedness in a smart factory environment causes its vulnerability to increase and makes it risky. Today's production systems are still not sufficiently sophisticated in terms of defense against malicious threats. This applies to attacks on CPS that can cause physical damage and endanger human life. Given the many threats to which the smart factory environment is exposed, companies are forced to implement extensive security and protection measures for information and communication systems that allow a large flow of data to optimize the entire production process.

This paper is a platform to develop security tools that can be used to protect the smart factory environment maximally. Future work will also address a proposal to design security mechanisms to protect the CPS in this environment.

References

1. Kalsoom, T., Ramzan, N., Ahmed, S., Ur-Rehman, M.: Advances in sensor technologies in the era of smart factory and industry 4.0. Sensors **20**, 6783 (2020). https://doi.org/10.3390/s20236783
2. Grabowska, S.: Smart factories in the age of industry 4.0. Manag. Syst. Prod. Eng. **28**, 90–96 (2020). https://doi.org/10.2478/mspe-2020-0014
3. Gisler, A.: Smart factories (2019). https://digital-library.theiet.org/content/journals/10.1049/et.2012.0610
4. Burke, R., Mussomeli, A., Stephen, L., Marty, H., Brenna, S.: The smart factory (2017)
5. Ilanković, N., Zelić, A., Gubán, M., Szabó, L.: Smart factories – the product of Industry 4.0. Prosperitas **7**, 19–31 (2020). https://doi.org/10.31570/Prosp_2020_01_2
6. Rathnam, L.: Industry 4.0: building the 'smart factory' of tomorrow—today. http://techgenix.com/smart-factory/. Accessed 09 Nov 2020
7. Büchi, G., Cugno, M., Castagnoli, R.: Smart factory performance and industry 4.0. Technol. Forecast. Soc. Change **150**, 119790 (2020). https://doi.org/10.1016/j.techfore.2019.119790

8. Illa, P.K., Padhi, N.: Practical guide to smart factory transition using IoT, big data and edge analytics. IEEE Access **6**, 55162–55170 (2018). https://doi.org/10.1109/ACCESS.2018.2872799
9. Peraković, D., Periša, M., Cvitić, I., Zorić, P.: Information and communication technologies for the society 5.0 environment. In: Zbornik radova trideset osmog simpozijuma o novim tehnologijama u poštanskom i telekomunikacionom saobraćaju – POSTEL 2020, pp. 203–212. University of Belgrade, Faculty of Transport and Traffic Engineering, Belgrade (2020). https://doi.org/10.37528/FTTE/9788673954318/POSTEL.2020.020
10. Virat, M.S., Bindu, S.M., Aishwarya, B., Dhanush, B.N., Kounte, M.R.: Security and privacy challenges in internet of things. In: Proceedings of the 2nd International Conference on Trends in Electronics and Informatics, ICOEI 2018, pp. 454–460. Institute of Electrical and Electronics Engineers Inc. (2018). https://doi.org/10.1109/ICOEI.2018.8553919
11. Arnold, C., Kiel, D., Voigt, K.I.: Innovative business models for the industrial internet of things. In: 26th International Association for Management of Technology Conference, IAMOT 2017, pp. 1379–1396 (2020). https://doi.org/10.1007/s00501-017-0667-7
12. Lu, Y.: Industry 4.0: a survey on technologies, applications and open research issues (2017). https://doi.org/10.1016/j.jii.2017.04.005
13. Zheng, P., et al.: Smart manufacturing systems for industry 4.0: conceptual framework, scenarios, and future perspectives. Front. Mech. Eng. **13**(2), 137–150 (2018). https://doi.org/10.1007/s11465-018-0499-5
14. Rao, S.K., Prasad, R.: Impact of 5G technologies on industry 4.0. Wirel. Pers. Commun. **100**(1), 145–159 (2018). https://doi.org/10.1007/s11277-018-5615-7
15. Alcácer, V., Cruz-Machado, V.: Scanning the industry 4.0: a literature review on technologies for manufacturing systems (2019). https://doi.org/10.1016/j.jestch.2019.01.006
16. Mabkhot, M., Al-Ahmari, A., Salah, B., Alkhalefah, H.: Requirements of the smart factory system: a survey and perspective. Machines **6**, 23 (2018). https://doi.org/10.3390/machines6020023
17. Gao, R.X., Wang, L., Helu, M., Teti, R.: Big data analytics for smart factories of the future. CIRP Ann. **69**, 668–692 (2020). https://doi.org/10.1016/j.cirp.2020.05.002
18. ENISA: Good practices for security of internet of things in the context of smart manufacturing. In: European Union Agency for Network and Information Security (ENISA), Attiki, Greece (2018)
19. Small, M.: 5G and identity. https://www.kuppingercole.com/blog/small/5g-and-identity. Accessed 15 Oct 2020
20. Ahmad, A., Bosua, R., Scheepers, R.: Protecting organizational competitive advantage: a knowledge leakage perspective. Comput. Secur. **42**, 27–39 (2014). https://doi.org/10.1016/j.cose.2014.01.001
21. Tuptuk, N., Hailes, S.: Security of smart manufacturing systems. J. Manuf. Syst. **47**, 93–106 (2018). https://doi.org/10.1016/j.jmsy.2018.04.007
22. Walker-Roberts, S., Hammoudeh, M., Aldabbas, O., Aydin, M., Dehghantanha, A.: Threats on the horizon: understanding security threats in the era of cyber-physical systems. J. Supercomput. **76**(4), 2643–2664 (2019). https://doi.org/10.1007/s11227-019-03028-9
23. FPT Software: 5 Ways to Mitigate Cybersecurity Risks in Smart Manufacturing. https://www.fpt-software.com/5-ways-to-mitigate-cybersecurity-risks-in-smart-manufacturing/. Accessed 10 Dec 2020
24. Trend Micro: Threats and Consequences A Security Analysis of Smart Manufacturing Systems. https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/threats-and-consequences-a-security-analysis-of-smart-manufacturing-systems. Accessed 11 Oct 2020
25. Häckel, B., Hänsch, F., Hertel, M., Übelhör, J.: Assessing IT availability risks in smart factory networks. Bus. Res. **12**(2), 523–558 (2018). https://doi.org/10.1007/s40685-018-0071-5

26. Tupa, J., Simota, J., Steiner, F.: Aspects of risk management implementation for industry 4.0. Procedia Manuf. **11**, 1223–1230 (2017). https://doi.org/10.1016/j.promfg.2017.07.248
27. Ervural, B.C., Ervural, B.: Overview of cyber security in the industry 4.0 era. In: Ervural, B.C., Ervural, B. (eds.) Industry 4.0: Managing the Digital Transformation. SSAM, pp. 267–284. Springer, Cham (2018). https://doi.org/10.1007/978-3-319-57870-5_16
28. Herrmann, F.: The smart factory and its risks. Systems **6**, 38 (2018). https://doi.org/10.3390/systems6040038
29. Cavusoglu, H., Cavusoglu, H., Son, J.Y., Benbasat, I.: Institutional pressures in security management: direct and indirect influences on organizational investment in information security control resources. Inf. Manag. **52**, 385–400 (2015). https://doi.org/10.1016/j.im.2014.12.004
30. Cvitić, I., Peraković, D., Periša, M., Botica, M.: Novel approach for detection of IoT generated DDoS traffic. Wirel. Netw. **27**(3), 1573–1586 (2019). https://doi.org/10.1007/s11276-019-02043-1
31. Swivel Secure: Industry 4.0 and the cybersecurity risks to the future of manufacturing. https://swivelsecure.com/solutions/manufacturing/manufacturing-is-at-risk-from-cybercrime/. Accessed 15 Nov 2020