MANAGEMENT OF CYBER SECURITY THREATS IN THE FACTORIES OF THE FUTURE SUPPLY CHAINS

Jukka Hemilä
Business ecosystems renewal, VTT Technical Research Centre of Finland Ltd,
Vuorimiehentie 3, 02044 Espoo, Finland, E-mail: jukka.hemila@vtt.fi

Markku Mikkola
Business ecosystems renewal, VTT Technical Research Centre of Finland Ltd,
Vuorimiehentie 3, 02044 Espoo, Finland, E-mail: markku.mikkola@vtt.fi

Jarno Salonen
Cyber security, VTT Technical Research Centre of Finland Ltd,
Visiokatu 4, 33720 Tampere, Finland, E-mail: jarno.salonen@vtt.fi

ABSTRACT

Today there are numerous Factories of the Future initiatives delivering different Industry 4.0 applications to manufacturing industry supply chains. However, in the future, Factory of the Future is not going to be a simple manufacturing asset, nor a sum of isolated assets. Instead, it will comprise a network of factories, which is considered in a System of Systems approach. The current challenge is to propose novel architectures, technologies and methodologies to optimize the level of efficiency and security of this System of Systems in a context where every step towards digitization exposes the manufacturing process to a widening array of cyber threats. This paper discusses about the management of cyber threats in System of Systems operations and supply chains. The next generation System of Systems are using different technologies with the combination of human aspects from workers, managers, entrepreneurs and decision makers. In addition, economically there are limitations on how much to invest on different technologies and human aspects. In addition, monetary and financial flows are under the burden of cyber risks. This study will therefore embrace the technical, economic and human dimensions at once. This study is based on a European-wide multi-national research project, the aim of which is to define - through different use-cases - the preventive and reactive capabilities to address cyber and physical threats and safety concerns in System of Systems. The study indicates different cyber challenges related to the future manufacturing business and operational models, with a special attention on "as-a-service" business model. The paper also indicates initial managerial and practical views on the management of cyber threats in future business models.

Keywords: cyber threats, business models, Factories of the Future, System of Systems

1. INTRODUCTION

Digitalization and Internet of Things (IoT) are global trends in many industries. IoT is defined as an infrastructure of interconnected objects, people, systems, and information resources that allow them to process information of the physical and the virtual world and react. By 2020, the number of connected devices is expected to be over 26 billion devices (Omitola & Wills, 2018). In the manufacturing industry, a global revolution in manufacturing systems is ongoing and leading companies around the world have invested in the development of smart manufacturing

systems that are able to respond in real time to changes in customer demands, as well as the conditions in their supply chains (Tuptuk & Hailes, 2018). Applying Industry 4.0 in practice has been a continuously increasing trend in the manufacturing industry. Industry 4.0 creates a bridge between the digital and physical world through different IoT technologies such as the use of cloud systems, data analytics and machine learning. The connection between digital and physical environments is usually referred to as Cyber-Physical Systems (CPS). This connection provides the ability to create and update real-time virtual representations of physical assets to populate a digital twin (Sharpe et al, 2019). Cyber based products and services are acquired through supply chains that typically involve numerous suppliers of hardware, firmware and software components and services sourced globally (Windelberg, 2015). Actually, in manufacturing companies, this means numerous technologies from the supply side, including robotics and automation manufacturers, IIOT (Industrial IoT) and M2M (Machine-to-Machine) communication suppliers as well as SCADA (Supervisory Control And Data Acquisition), ERP (Enterprise Resource Planning) and Supply Chain management tool providers. In the future, integrated factories will operate as a System of Systems through intelligent machines, human factors integration, and integrated supply chains (Nahavandi et al, 2015). All this aforementioned development has made manufacturing supply chains more complex and at the same time more vulnerable towards different cyber risks. However, in the Industry 4.0 approach, networking of companies, which increases network complexity, seems to provide competitive edge, but at the same time increases vulnerability. There is a definite need for operations, where cyber risks are managed, but operations are optimized. Reported cyber-attacks from recent years targeting industrial and manufacturing systems demonstrate that the cyber threat is real, and that the consequences of these attacks can be severe (Tuptuk & Hailes, 2018).

So far, the literature lacks a holistic overview and framework to describe the Industry 4.0 risks (Schneider, 2018). This paper focuses on cyber security threats, related to modern manufacturing industry supply chains. Cyber security threats are related to humans, machines, interactions and exist practically everywhere in the organization and collaboration processes. As the complexity in supply chains increases, the amount of information and integration is also increased. Whenever some object (human or machine) communicates and shares information and data, there is a risk of cyber-attacks. However, manufacturing companies have not yet fully protected themselves from threats related to cyber security. The paper indicates the research approach (Chapter 2), our findings (Chapter 3) and concluding discussion (Chapter 4).

2. RESEARCH APPROACH

The entire industrial ecosystem is changing as digitalization and cyber-physical systems are characterizing the Fourth Industrial Revolution and Industry 4.0 initiatives can be seen globally. Because of the ongoing radical change, the purpose of the study is to discuss about the cyber security risks related to Industry 4.0 applications and operations. This conceptual paper is based on a European research project with the aim of defining - through different use-cases - the preventive and reactive measures and capabilities to address cyber and physical threats and safety concerns in System of Systems. Our focus is on the as-a-service operation model, where production line is offered as a service to the customer site (Figure 1).

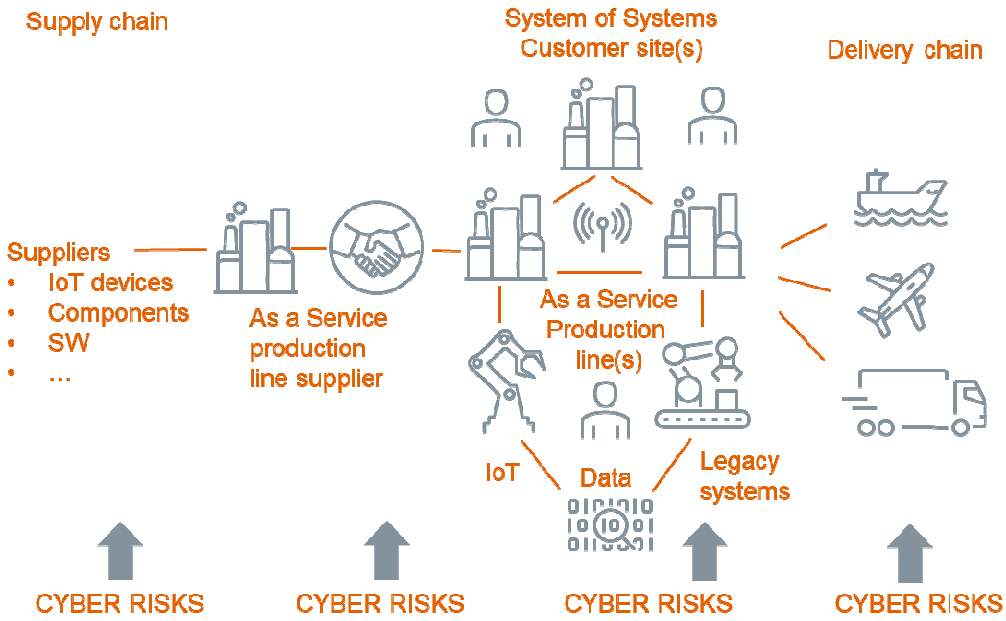

Figure 1. Research context - Cyber risks in System of Systems operations

The use-cases represent very different sized companies, from SMEs to globally operating multi-national and multi-site companies. We have collected the initial ideas for cyber threat management within workshops and collaborative teleconferences. The workshop and teleconference participants represent practitioners from the use case companies, academic researchers and software providers' experts. All participants are representing consortium member organizations. Additionally, initial findings have been enriched with literature findings. Later, external expert interviews and workshops will be organized for getting broader views on the topic. The research is still ongoing, and this paper indicates only the first findings. The final aim is to develop a management model for the cyber security threats in manufacturing industries and this paper comprises the first cyber risk management model for Industry 4.0 operations. The final management model will be developed with the project use cases by combining expert interviews, workshop results and literature findings. Project will demonstrate cyber-security solutions, which experiences will be taken in account to final management model. Practical demos will demonstrate cyber threats management with systematic data-analysis. These experiences will be part of management model as well.

3. FINDINGS

Currently there is a huge hype around the CPS and Industry 4.0, and many leading manufacturers have already invested on latest connectivity technologies. However, Sharpe et al. (2019) have argued that most manufacturers still exist in a world of data silos and unconnected resources, and there is a lack of research demonstrating the key benefits of CPS to manufacturers. Security has been documented as a major challenge in CPS, it is a concern of many industrialists and therefore it must be a fundamental consideration in any type of CPS (Sharpe et al, 2019). Cyber criminals have moved from focusing primarily on organizations rich in sensitive personal data, such as financial or healthcare institutions to targeting any organization with IT weaknesses (Sikich, 2019). Almost any connected device, whether on the shop floor in an automated system or remotely located at a third-party contract manufacturer, should be considered as a potential target for cyber-attacks. This increased risk and dramatically expanded threat surface requires a

fundamental change in how security is viewed within the Industry 4.0 driven manufacturing. There are examples already on how cyber criminals have attacked with malware to milking machines and heating or cooling systems, where the control system is accessible from the Internet, with a weak malware protection or completely without protection. In response to this growing threat, manufacturing executives must define security a core corporate priority and push forward the implementation of preventative measures in their organizations (ibid). Despite the risk being identified, there is still too little reporting of cyber incidents related to the manufacturing industry and the majority of examples are ones that have caused the most significant damage (Tuptuk and Hailes, 2018). According to the Sikich report (2019), the confidence of manufacturing firms in their ability to withstand cyber-attacks is high; 54% rate themselves "very" or even "extremely" confident in their ability to weather the effects of a data breach. Still almost half of companies do not have confidence against cyber-attacks. A bit over one third (38%) of smaller companies perform cyber audits and just over 30% have somehow prepared themselves for attacks (Sikich, 2019). Actually, our findings from practice are quite similar, as most of the small and medium sized manufacturers have not yet focused on cyber threats. Email and web servers are generally protected, but the operational processes and connected devices are usually not usually. At the same time, most competitive manufacturers have invested in advanced manufacturing technologies and equipment (Sikich, 2019). In the end, the manufacturing industry might face a dilemma that even though the CPS and digitalization advantages are increasing due to the investments on latest manufacturing technologies, the security issues are seen too large a barrier for the implementation.

In our ongoing research, the challenge is to propose novel architectures, technologies and methodologies to optimize the level of efficiency and security of SoS in the context where every step towards digitization exposes the manufacturing process to a widening array of cyber threats. We intend to solve more than just the technological challenges of Industry 4.0. The project will embrace technical, economic and human dimensions at once, which are combined under the future System of Systems management model. Our study focuses on the customer-centric plant, which provides customized production lines for dairy product customers. In the future direction of our case study, automated robots will be introduced and one production line can easily manage many different final products. Today, one production line produces only one final product, so the future model results into a more efficient operation for the end customer. Today these production lines are ordered and delivered according to customer needs, and customers generally operate their own production. We have identified an opportunity for "as-a-service" type of operation model, where the supplier offers a specific production capacity and customer billing is based on the usage of the production line or on the output of the line. The service business model lowers the investment risk of the customer, while the supplier should take more risk when offering such a capacity rather than the basic production line. The "as-a-service" model means real time connectivity from supplier to the customer site, ensuring the availability of sufficient capacity and the overall process performance. That introduces new challenges for cyber security, as most of the critical processes are controlled over a remote connection using the internet, which increases the threat of cyber-attacks. Therefore, IP protection is the key security challenge. In other words, the growing integration of value chain and full-life-cycle management increases cyber threats into a new level. This results in an immediate need of new types of management and tools in the modern manufacturing industry that faces a growing amount of cyber threats. Traditionally, the IT components used within the manufacturing systems domain are heterogeneous, with a high number of legacy systems and devices that can have a lifetime up to 20 years (Tuptuk & Hailes, 2018). These systems have complex interactions with physical processes, and IT failures can also affect physical processes. In the networked environment of Industry 4.0, Schneider (2018) have

argued that various reference architectures and platform models enable companies to reduce development and deployment costs for software, share IT resources and access dedicated manufacturing software applications that facilitate (joint product and process) innovations. There is a cost for additional collaboration processes, but advantages for resource sharing can be bigger than costs. Beyond the traditional approaches to architectures for industrial control systems, our research has indicated a set of key focus areas that can be considered the main areas for daily management against cyber threats. These key focus areas are split into three categories: 1) Modelling and Simulation, 2) Production optimization, 3) Cyber risk management. These categories are constructed over three organizational dimensions: 1) Technical, 2) Economical, 3) Human. Together these categories and dimensions are framing our proposed cyber threat management framework, which is called the SoS Management Model.

Firstly, when looking deeper into the dimensions, the Technical dimension includes cyber-physical system digital twins, real-time tracking, as well as human-machine transaction management. In a modern manufacturing system, especially when operating in as-a-service model, the supplier should have clear picture of the manufacturing line at customer site. Here the modelling and the customer site comprehensive digital twin create great advantages for the as-a-service operation model. In the production optimization point of view, real-time tracking of production line is needed for getting real-time data from the actual statuses. Then digital twin will then be updated according the data from the real system. There is a continuous loop between the real life and digital twin, and data is continuously shared. From the cyber risk management point of view, the last management topics for technical dimension are the Human-Machine Cyber-security tools, where managers should understand which kind of tools are needed for detecting and preventing cyber-attacks within the human-to-machine interaction in the production line and operations. The stakeholders related to operations include workers, managers and decision makers, who all need different technologies to support their daily work. Actually, we can say that all software today is connected to internet and therefore create a potential for a cyber-attack. Also human errors related to e.g. how to use the software increase this risk, but that view has been included in the later human dimension.

Secondly, the Economical dimension deals with the Supply chain and Ecosystem modelling, Data exploitation for economical studies and Transaction flow control. There the factory supply chains and related ecosystems should be modeled in order to understand the supply chain responsibilities and flows. The factory ecosystem is a natural expansion to the manufacturing plant simulation models and digital twins. Production line digital twins can be integrated with the supply chain models in such a way that overall physical system can be defined and modelled digitally. Data exploitation for economical studies means enabling to build new business opportunities based on big data analytics over the manufacturing data but also understanding traditional economic and monetary flows in the operations. Requirement for data exploitation is the real time tracking of production line, which generates data for analysis purposes. In the economical dimension, Transaction flow control is needed to detect, investigate, respond and prevent cyber risks in human-machine interactions.

The third dimension is the Human dimension, where the key focus areas are Human-Machine interaction modelling, Optimization of human-machine interaction and cyber risk management of Human-Machine interaction. The human dimension is still an important part of the modern manufacturing line, despite the high automation level in many cases. Manufacturing operations and support functions cannot operate without humans, and the human operator is always a cyber security risk. The increase of automation will change the workplace of the future and demand new skills and competences from employees. In the future, companies will depend on

not fewer, but on differently qualified employees. Hence, advanced concepts of work organization improving the development of decision-making and competences could generate a higher quality of life because of better working conditions. The understanding of the cyber threat environment from the human factors point of view is important, because there are several hazards that can cause severe and long-term damages to the company. There are typically many organizational levels taking part in the supply chain operations from the factory floor level to managers and decision makers. Actually, the diversity within the organizations has increased lately after the increase of complexity in operations. Here in Human dimension, the first focus area is the Human-Machine interaction modelling, which is done based on the digital twin of the production line and in the ecosystem model. Here the aim is to model all transactions that humans are doing within the operations. By modeling the transactions, companies can generate an overview on who is doing what in each operation. Secondly, the optimization can be done when all transactions are understood and processes defined. Thirdly, the Human-Machine interaction cyber risk management is used especially for cyber risk control, i.e. when cyber tools are in use and transaction flows are managed well. This means that companies should identify the software being used as well as the cyber security tools needed for ensuring cyber protection. One example is email, as there is a constant cyber risk related to email sharing. There are examples how cyber criminals have used company look-a-like invoice emails, that the recipients have believed and paid money based on the forged information.

The SoS Management Model is arising from the previous three dimensions. The Modelling and simulation category focus areas are combined to SoS Simulation Model that consists of the following categories: SoS Simulation Model, Optimized Distributed Manufacturing Model, and Cyber Risk Management Model. In the modelling and simulation category, the final aim is the SoS Simulation Model, which is used for production optimization, where clusters of technology developments enable the increase in productivity and efficiency in the entire supply chain. In the production optimization category, the aim is to ensure distributed manufacturing capability, which enables the optimization of the distribution of production load over a network of factories in real time. Schneider (2018) have argued that especially SMEs with limited resources can minimize their investment and implementation risks, when they fully exploit the networking effects of Industry 4.0 and even better fulfill customer requirements with jointly developed services. We have also found that collaboration and jointly developed offerings can bring additional competitive edge for SMEs. The as-a-service operation model in SoS requires a lot of collaboration, but also additional transactions. The final aim in cyber risk management category is the Cyber Risk Management Model, which is a combination of technologies enabling to secure smart manufacturing systems against cyber threats. The following Figure (Figure 2) presents our proposed framework for cyber security threat management.

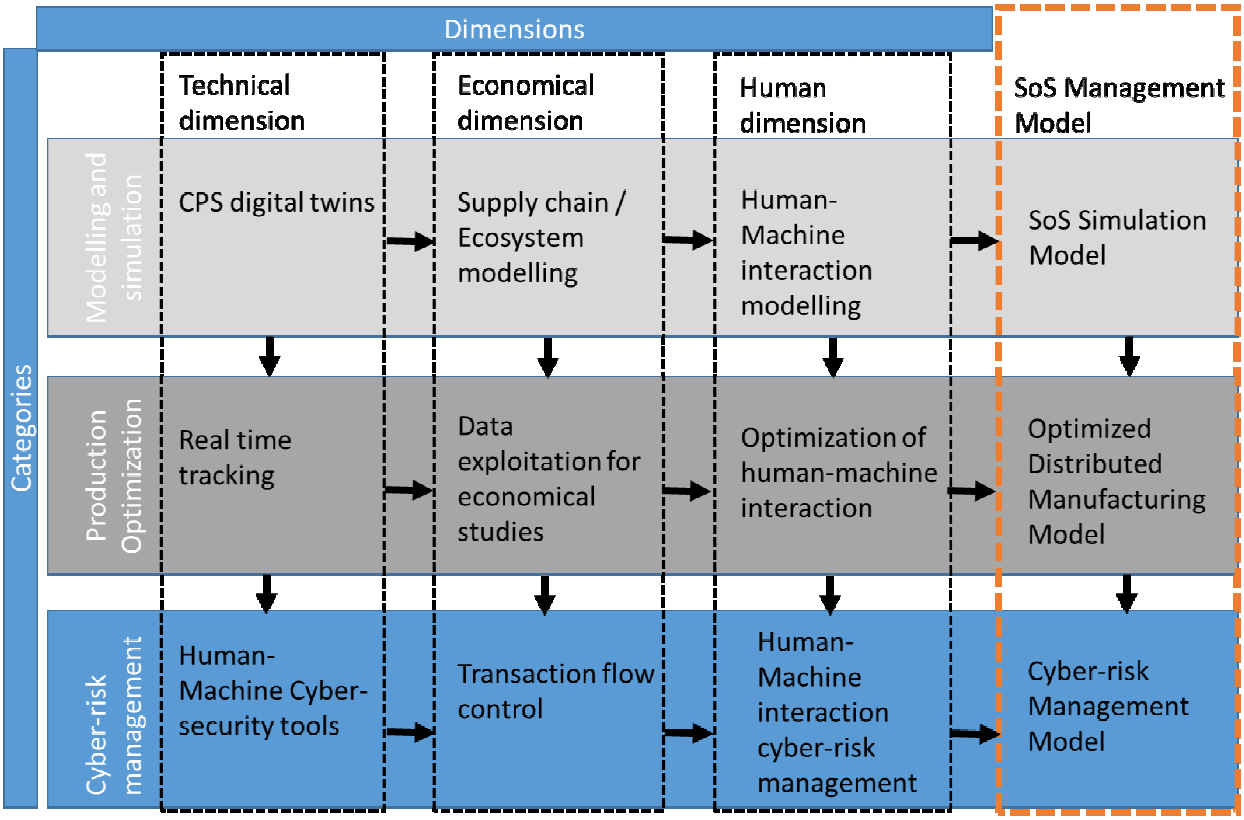

Figure 2. Proposed framework for cyber security threat management

There will definitely be cyber risks and threats in all levels of operations and supply chains. In our proposed framework, all key focus areas should be managed well with the technologies and improved processes. There are many transactions in manufacturing operations, like monetary flows, information flows, material flows, where cyber risks are taking place. Especially the human risk exists everywhere, despite the high automation level in modern production. All transactions should be defined and understood before identifying the related cyber risks and vulnerabilities. Relevant technologies should be implemented for managing the aforementioned risks. Large and complex as-a-service based operation models need comprehensive cyber risk management tools and processes.

4. DISCUSSION AND CONCLUSION

All connected devices are today facing the risk of cyber-attacks. Every process can comprise a potential attack-vector for cyber criminals. Even though more known global organizations might be a more attractive target for cyber criminals, criminals also see the potential of smaller companies because of their lack of protection mechanisms and systems. To understand the likely avenues of a cyber-attack, companies need to understand the vulnerabilities of their entire system, but only few studies has explored this for smart manufacturing systems (Tuptuk & Hailes, 2018). An increasing complexity and connectivity in ecosystems require a higher need for cyber security (Voigt et al, 2019). Windelberg (2019) have argued that to ensure the secure, reliable and safe operation of information and communications and operational technology systems that are integral to critical infrastructures, organizations must effectively manage risk factors that arise in supply chains for cyber based products and services. Our study indicates similar findings as Windelberg, and the ecosystem stakeholders must clearly understand the cyber

risks of the supply chain, and effectively try to implement the applicable tools to manage the risks and vulnerabilities. To minimize cyber risks, companies need to implement and use an effective and comprehensive IT security management system (Tuptuk & Hailes, 2018). The overall cyber protection is dependent on the legacy systems and interactions in use, and there is no generic advice on which kind of cyber security solution will give the optimal protection. This is why we have proposed the framework with capabilities to be managed well. Resource sharing within the ecosystem, or sub-part supply chains, might be the answer to increased cyber threats. Especially SMEs can invest in latest technologies for protecting their operations. Software as a Service (SaaS) model is another approach for lowering the investments, i.e. where companies are just paying for the use of cyber tools.

Actually, our conceptual paper has defined the SoS Management model, without practical validation of the model. That is surely one main limitation of the study. In practice, there are many more academics who would be interested in the security challenges of smart manufacturing than there are academics with access to testbeds or real plant on which to conduct experiments (Tuptuk & Hailes, 2018). The future research will focus on the practical development of these key areas, so that the model can be evaluated in practice. In the supply side, robotics and automation manufacturers, IIOT and M2M communication suppliers, SCADA, ERP and other Supply Chain IT-providers need to improve their cyber risk management features in their products. Tuptuk and Hailes (2018) have argued that to develop effective security solutions, the research and industry communities need to work together and focus on efficient, robust, reliable, low-cost security solutions that can cope with the deployment and runtime requirements of the current and future manufacturing systems. In our future studies, we will conduct research within the case study on which kind of practical cyber risk management tools there are available within the different technologies. According to the findings by Voigt et al. (2019), challenges and risks of Industry 4.0 can be divided into five categories: Human factor, IT security, organization and implementation, data analysis and legal issues and standards. Here, the human factor is discussed mostly and featured as the most important aspect according the literature survey by Voigt et al (2019). Our study also highlights the human aspect and its vulnerabilities as a part of overall cyber threat management. Finally, our proposed SoS Management model with three dimensions and three categories introduces a comprehensive model for modern production management.

5. ACKNOWLEDGEMENTS

This article is based on research results from the European project “17032 CyberFactory#1” under the ITEA3 program with the objective of designing, developing, integrating and demonstrating a set of key enabling capabilities to foster optimization and resilience of the Factories of the Future (FoF). The project started in 2018, ends in 2022 and it comprises more than 30 partners from eight countries. (https://www.cyberfactory-1.org/).

6. REFERENCES

Nahavandi S., Creighton D., Le V.T., Johnstone M., Zhang J. (2015). *Future Integrated Factories: A System of Systems Engineering Perspective*. In: Fathi M. (eds) Integrated Systems: Innovations and Applications. Springer, Cham.

Omitola, T., Wills, G. (2018). Towards Mapping the Security Challenges of the Internet of Things (IoT) Supply Chain. *Procedia Computer Science*, 126, 441-450.

Schneider, P. (2018). Managerial challenges of Industry 4.0: an empirically backed research agenda for a nascent field. *Review of Managerial Science*, Springer, 12(3), 803-848.

Sharpe, R., van Lopik, K., Neal, A., Goodall, P., Conway, P., West, A. (2019). An industrial evaluation of an Industry 4.0 reference architecture demonstrating the need for the inclusion of security and human components. *Computers in Industry*, 108, 37-44.

Sikich. (2019). *2019* Manufacturing and Distribution Report. *Consultancy company Sikich report series 2019.*

Tuptuk, N., Hailes, S. (2018). Security of smart manufacturing systems. *Journal of Manufacturing Systems*, 47, 93-106.

Windelberg, M. (2016). Objectives for managing cyber supply chain risk. *International Journal of Critical Infrastructure Protection*, 12, 4-11.

Voigt, K-I., Hartmann, E., Rücker, M., Veile, J. Birkel, H. (2019). Risks of Industry 4.0 for Logistics – A Systematic Literature Review. *Proceedings of the 24th International Symposium on Logistics (ISL 2019)*, Würzburg, Germany 14th – 17th July 2019.