Fraunhofer
IPT

FRAUNHOFER INSTITUTE FOR PRODUCTION TECHNOLOGY IPT

WHITE PAPER **CYBERSECURITY IN NETWORKED PRODUCTION**

CONTENTS DIRECTORY

INTRODUCTION

Digitalization and networking bring with them an enormous growth potential for companies and will gain more importance for Germany as a business location in the coming years [1, 2]. The management and strategy consultancy McKinsey & Company estimates that German companies will be able to generate an additional € 126 billion in added value by 2025 through consistent digitalization [3]. Viewed in this overall context, the manufacturing sector generated more than a quarter of Germany's total gross domestic product in 2018 [4]. Despite the large growth potential, the digitalization rate in the production of large German companies is only just under 30 percent – with small and medium-sized companies even only at 20 percent [5]. And one of the biggest obstacles to networking is cybersecurity [6]: whereas the focus used to be primarily on the functional safety of production facilities, cybersecurity – due to the shift from closed to open cyber-physical systems – is now increasingly coming to the fore [7]. However, long life cycles mean that updates are no longer offered for plants, patch policies become outdated and thus inadequate, and the available network protocols are no longer secure [8].

Moreover, due to worldwide networking, cybercrime is not only a local, but a global problem for all industrialized nations. Especially attacks on industrial automation systems and the number of publicized cyber incidents are increasing rapidly [9, 10]. Cybercrime examples ranges from severe extortion of car manufacturers by means of ransomware to physical damage of a blast furnace in a German steel plant [11, 12].

The Fraunhofer Institute for Production Technology IPT has therefore developed a holistic Production Security Readiness Check (PSRC) based on current norms, standards and guidelines, which shows manufacturing companies what security level they are currently at and what risks they are exposed to. Based on the company security level, the PSRC shows options for action that companies can use to close the gap between the security level already achieved and the desired level.

WHAT NEEDS TO BE PROTECTED?

Digital information is an asset that must be protected. To ensure the necessary protection, certain requirements are placed on IT systems. These requirements are referred to as the protection goals of IT security [13, 14]. The goal is therefore to prevent confidential information from reaching non-authorized persons (confidentiality) or from being modified by unauthorized third parties (integrity) [15,16]. In parallel, access to information should, in the best case, be permanently guaranteed (availability) [17]. Based on these requirements, there are three central goals that need to be protected: Confidentiality, integrity and availability of both data and systems [12, 16]. In addition to these central goals, other protection goals exist, including authenticity, accountability, transparency, and contingency [18]. The requirements for IT systems in the form of protection goals are either determined by the company, for example if critical manufacturing data is to be stored and processed confidentially, or they are defined in laws and standards.

There is currently no coherent and generally applicable IT security law in Germany. Rather, legal requirements relating to IT security are spread across a large number of different laws [19]. The entry into force of the IT Security Act in 2015 was intended to contribute more specifically to improving the security of IT systems in companies [20]. The main addressees of the law also include operators of critical infrastructure and telecommunication and telemedia providers [19, 21]. German industrial production and the associated value chains are not explicitly mentioned as addressees. There are no legal foundations for this sector outside of the regulations for critical infrastructures that affect IT security [12]. In IT, there are a large number of different standards and norms from various bodies that affect security [12]. Figure 1 depicts the most important laws, standards and bodies promoting IT security.

World	ITU	ISO	IEC	ISA
	ITU-T X.xx	ISO 270xx	IEC 62433-x-x	ISA 99.xx.yy
Europe	ENISA	ETSI	CEN/CENELEC	
	Reports/Studies	TS 102 xxx	Guides	
		TR 103 xxx	EN Standards	
Germany	BSI	TeleTrust	DKE	Platform I4.0 AG3
	Grundschutz (200-x)	Guides	VDI/VDE / DIN	BDEW, BMWi, BMBF
	Technical guidelines	Handouts	VDI/VDE 2182	Guides
	Application notes and interpretations		DIN SPEC 27070	Result/Discussion Paper

Overview of the most important international and national IT security laws, standards and bodies [27]

INDUSTRIAL PRODUCTION FROM THE IT PERSPECTIVE

Today's industrial production aims to increase its productivity and at the same time reduce costs. To achieve this goal, automated production systems are used within an operational context. The individual areas of today's industrial automation are illustrated by the so-called automation pyramid (cf. Figure 2, left) [23].

The automation pyramid describes six different levels in the company that have interfaces with each other. The advancing networking of production means that IT (Information Technology) and OT (Operational Technology) networks are slowly converging. A complete air gap, the physical separation of systems between the supervisory and planning levels, is de facto continuously decreasing in today's production. Production equipment that used to operate in isolation with proprietary protocols in the IACS (Industrial Automation and Control Systems) environment, for example, is now adopting open network protocols from IT networks [26]. Threats against production plants were previously considered manageable, since these plants – seen from an IT perspective – formed islands that could only be attacked from the outside to a limited extent [12]. With reference to the automation pyramid, the Industry 4.0 approach now ensures that all system components are networked horizontally and vertically throughout. However, this means that the classic hierarchical automation pyramid is dissolving and an automation network is created (cf. Figure 2, right). For sensors and actuators at the field level, this means that they not only exchange data exclusively with the control level (PLC/SCADA), but across levels [27]. Field devices are then directly connected to the automation network. From the point of view of IT security, this means that field devices can now be accessed directly from the Internet via Ethernet/WLAN and are therefore also vulnerable to attack. Protective layers from PLC or SCADA systems no longer exist. Interfaces to mobile data carriers offer additional potential for attack [28]. Risks and challenges for production can be derived from both the automation pyramid and the automation network shown.

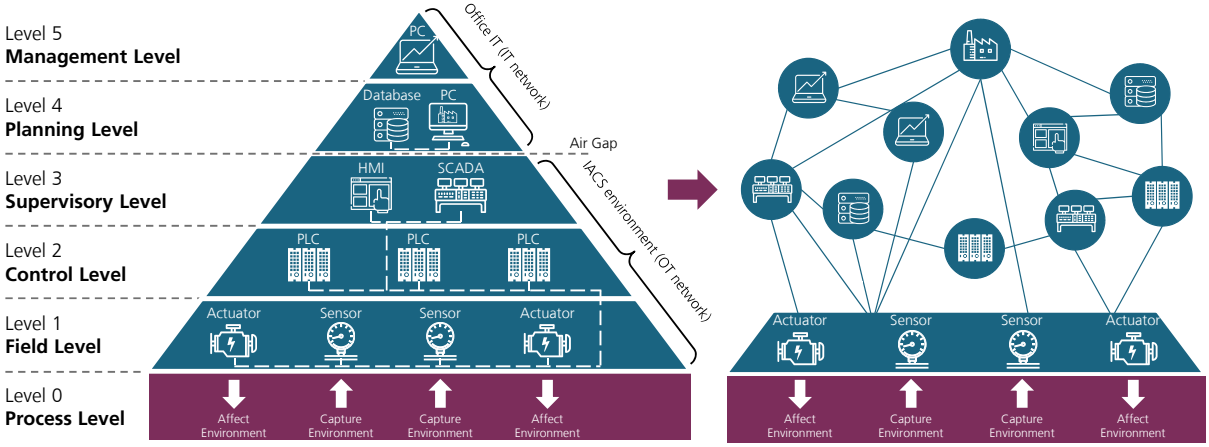

Figure 2: Automation pyramid and network in the production [23] [24]

Risks and Challenges in Production

The risks and challenges in production can be defined into three categories: literature distinguishes between the operational, the technical and the management domain [8]. Thus, it is necessary to achieve a large number of operational goals, for example, ensuring functional capability, while at the same time maintaining a high level of availability of the production facilities. On the technical side, the risks and challenges are based in the use of embedded systems and insecure network protocols, but also in the requirement to guarantee real-time performance. In most cases, an IACS must operate in real time to manage the production process. Communication latency and jitter are the critical factors for real-time communication of the OT network. The requirement for low latency makes it difficult to implement resource-hungry security mechanisms such as encryption. From a management perspective, low user and operator awareness, inadequate regulation of IT

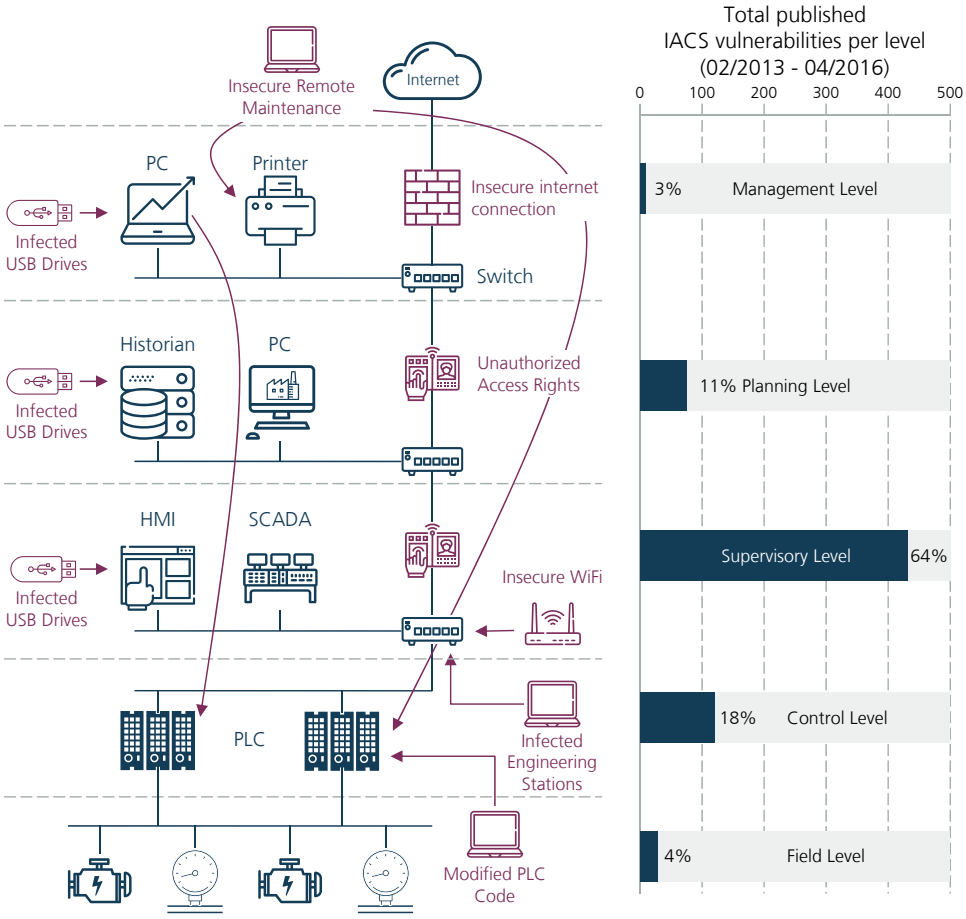

Figure 3: Cumulative number and representation of possible weak points in the automation pyramid [30] [31]

security in production, and long equipment lifecycles pose additional risks [8]. Procuring a new industrial plant entails higher investment: the plant must be operated for several decades in order to pay off the investment costs. A plant life of up to 30 years is not uncommon [29]. These long life cycles lead to two problems in terms of cybersecurity: There is hardly any protection against the new threats and at the same time security mostly depends on unsupported (operational) systems [8]. If companies do not consistently address these described risks and challenges, vulnerabilities in production can arise.

Vulnerabilities in the Production Environment

Vulnerabilities exist in every single level of the automation pyramid: The left part of Figure 3 shows examples of vulnerabilities for each individual level. The right part shows the cumulative number of published IACS-related vulnerabilities from 2013 to 2016. This number is based on public reports as well as the ICS-CERT database. With 465 out of 724 cases, more than half of the published vulnerabilities concern the supervisory level [30, 31].

IT security experts see several reasons as to why many vulnerabilities are discovered at this level in particular. Possible causes are [30]:

1. The industrial hardware and software used is similar to office hardware and software (e.g. HMI) and is therefore familiar to vulnerability researchers.
2. The software used can be easily and cheaply obtained from researchers in the form of demo versions.
3. The supervisory level is critical in nature, meaning that access to the supervisory level automatically grants access to the connected control level and physical process. The search for weak points within the control and field levels becomes not necessary.
4. Non-authenticated protocols allow direct access to the OT network.

Attack Methods and Means

To implement security measures, it is necessary to understand the attackers' methods. They are no different from security experts that test a system. Different types of attacks are shown in Figure 4.

Regardless of the type of attacks, they follow a similar pattern [34]:

1. Spying out vulnerabilities of the system
2. Infiltration of the system by exploiting its vulnerability
3. Execution of the malware

The description is based on expert interviews conducted by the ENISA ICS Security Stakeholder Group (EICS) and the European SCADA and Control Systems Information Exchange (EuroSCSIE) as part of an ENISA study. Other experts from industry, academia and politics were interviewed [32].

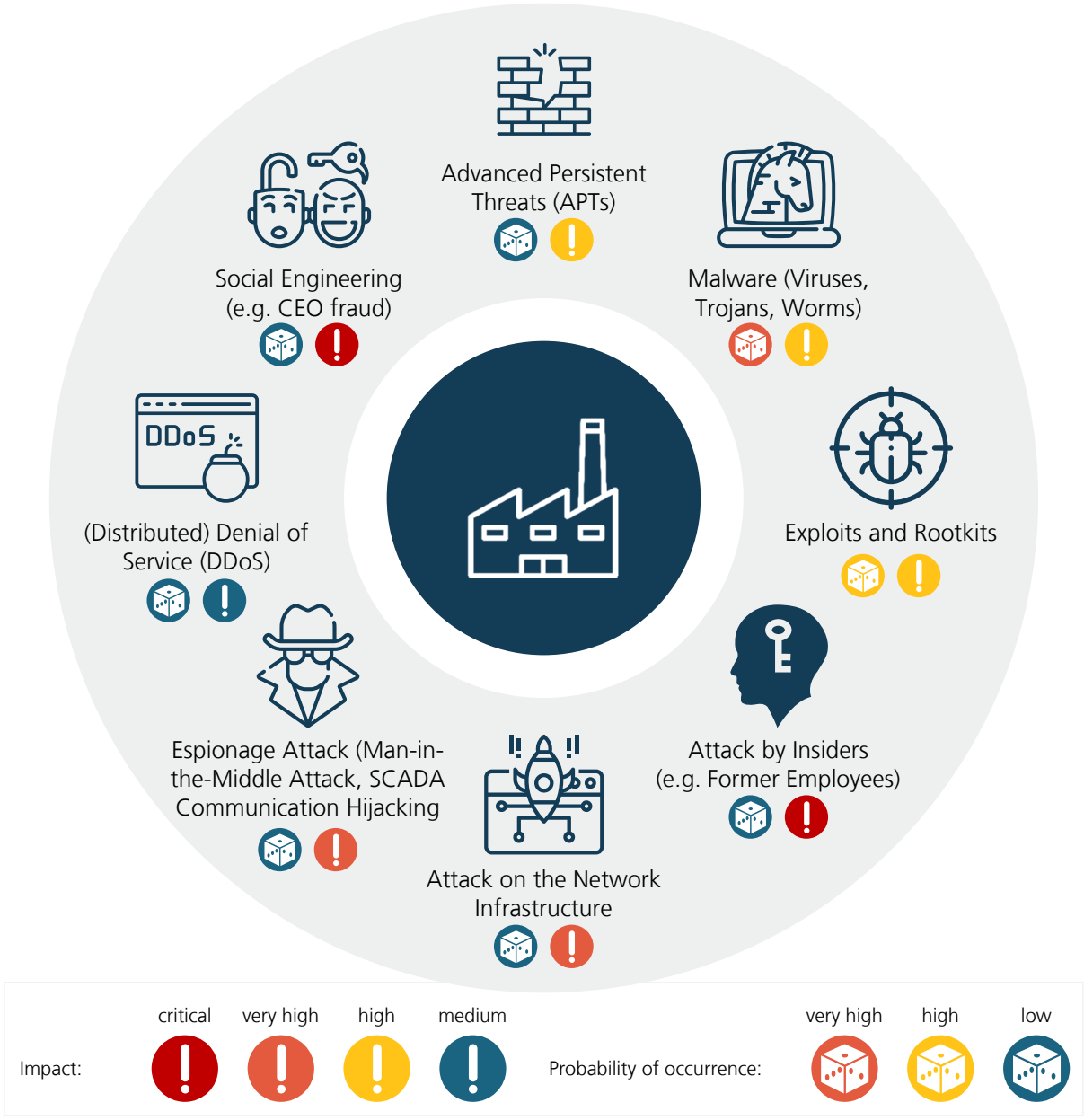

Figure 4: Common methods and means of attacking industrial production facilities [32][33][34]

STUDY DESIGN

To determine the current security level of companies, the Fraunhofer IPT has developed the Production Security Readiness Check (PSRC). The PSRC is a model for self-assessment of the cybersecurity status of manufacturing companies and helps them to evaluate and improve their cybersecurity planning. Specifically, the PSRC focuses on the implementation and management of cybersecurity practices related to information technology (IT) assets, operational technology (OT) assets, as well as environments in which they operate. The PSRC model has been mapped in the form of an Excel spreadsheet.

The Production Security Readiness Check helps manufacturing companies in achieving the following goals:
1. Assessing and strengthening cybersecurity measures in production.
2. Identification of risk vectors in the company and in production

Prioritization of Actions and Investments in Cybersecurity

The PSRC was developed to be used by manufacturing companies of any industry, structure, and size [35]. The tool is primarily based on the Cybersecurity Capability Maturity Model (C2M2) and a combination of common cybersecurity standards such as ISO 27001, IEC 62443, NIST CSF, and BSI IT-Grundschutz. The application of existing security norms and standards is essential in the IT and OT domains to ensure a holistic approach to security [36][37][38]. The PSRC consists of nine domains that map those topics that must be considered for a holistic security approach. These are illustrated in Figure 5 [35].

Figure 5: The nine domains of the PSRC

Sample and Survey Method

The sample selection was based on the Classification of Economic Activities, 2008 Edition (WZ 2008) of the German Federal Statistical Office. The economic sector C Manufacturing Industry was particularly relevant for this study. To address the companies, the Creditreform database was used with the help of the business information service provider Nexis. Companies with a minimum number of employees of 20 from the manufacturing sector were selected, which also had an e-mail contact address.

From the given pool of companies, 28 companies from different industrial sectors finally participated in the detailed study. Their allocation to the respective industry sectors can be seen in Figure 6. In the first step, these companies assessed their security status using PSRC. The time needed for the self-assessment was designed at a minimum of three hours per company. Based on the completed results, the second step was to conduct telephone interviews with selected companies, each lasting 30-60 minutes. The aim of the interviews was to verify the results obtained and to qualitatively explore the reasons for a possibly low level of implementation.

Evaluation Method

In order to better compare the previously defined domains with each other, the evaluation was carried out identically for each domain: The evaluation always began in general terms and ended in a detailed examination. In order to be able to represent the described cybersecurity practices – which form the basis of the PSRC – at an appropriate level of abstraction, these were mapped in the Excel sheet as independent, clearly differentiable building blocks. For this purpose, these building blocks each refer to a question that is as fine-grained as possible and, although they have identical nomenclature, their

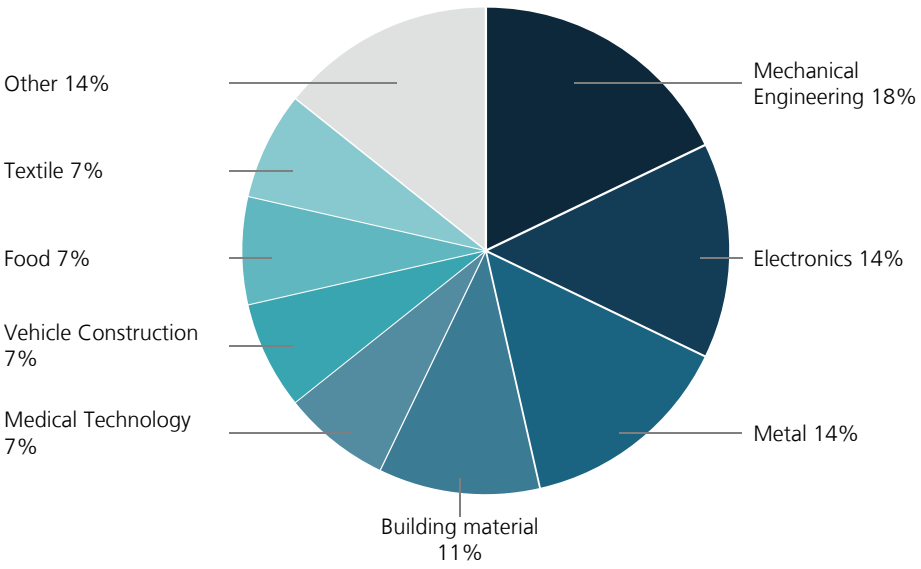

Figure 6: Industry sectors involved in the IT security study

content differs across domains. For example, in the asset, change and configuration management (ACCM) domain, the company evaluates on a four-level scale whether it has not implemented, partially implemented, largely implemented or fully implemented the building block "ACCM-1.1a: There is an inventory of OT and IT assets relevant to production" [35]. Based on the individual scores of the respective building blocks, the summarized implementation status of all practices in a domain for the participating small and medium-sized enterprises (SMEs) and large enterprises is presented in the form of a boxplot diagram. Specifically, it means that across all practices, the mean value of the implementation status was determined for each individual company. The individual mean values for the companies were then plotted on the boxplot diagram. As additional information, the boxplot diagram includes the median – which is robust against outliers – as well as the mean value of the previously calculated individual values. The advantages of the boxplot diagram lie in the clear presentation of the distribution and the range of the results.

In the next step, a detailed examination of the method and management objectives within the domain also took place in the form of a boxplot diagram. The method and management goals serve as categories for the individual cybersecurity practices (e.g., ACCM-1.1b: There is an inventory of information assets relevant to production etc.) into higher-level goals such as Goal: 1. Manage the Asset Inventory of the ACCM domain [35]. This is shown in Figure 7.

In the detailed analysis, the actual and target implementation status of the individual modules within a domain of SMEs and large companies was compared in a network diagram. For this purpose, the actual implementation average was determined for each individual module for all SMEs and large companies and compared with the recommended target implementation status. This representation makes it possible to identify the need for optimization of each individual module.

Asset, Change and Configuration Management (ACCM)

Goal: 1. Manage the Asset Inventory	Module	Actual	Target	GAP
ACCM-1.1a: There is an inventory of OT and IT assets relevant to production	ACCM-1.1a	3	3	
ACCM-1.1b: There is an inventory of information assets relevant to production	ACCM-1.1b	2	2	
ACCM-1.2c: The inventory contains additional information to support the enterprise c	ACCM-1.2c	1	2	Moderate
ACCM-1.2d: Inventoried assets are prioritized based on their importance to productic	ACCM-1.2d	1	2	Moderate
ACCM-1.3e: The inventory describes (physical and logical) connections, communica	ACCM-1.3e	1	2	Low
ACCM-1.3f: The asset inventory is reviewed and updated at a specified frequency	ACCM-1.3f	1	2	Low
Goal: 2. Manage Asset Configuration	**Module**	**Actual**	**Target**	**GAP**
ACCM-2.1a: Base configurations are set for inventoried assets to ensure that multipl	ACCM-2.1a	2	3	Critical
ACCM-2.1b: Base configurations are used to configure assets before commissionin	ACCM-2.1b	2	3	Critical

Figure 7: An excerpt from the ACCM domain [35]

FINDINGS

Across domains, the implementation status of all cybersecurity practices of the SMEs and large enterprises surveyed is shown in Figure 8.

On average, the large enterprises surveyed have a higher cybersecurity implementation status than SMEs. This is particularly noticeable in the median (GU: 0.98; SME: 0.66). These data show that the topic of cybersecurity is less present overall among the SMEs surveyed than among the large enterprises. Both boxplots show large spreads and thus a high variance in the implementation of cybersecurity practices.

Detailed Consideration Using the Example of the Asset, Change and Configuration Management Domain

The asset, change and configuration management domain describes the management, configuration and modification of IT and OT assets. Assets are understood to be all assets of a company, including all hardware and software in production [35]. In the asset, change, and configuration management domain, the following results are summarized and can be seen in Figure 9: Compared to the risk management domain, the ACCM domain shows a higher level of implementation – on average and median for both the participating SMEs (mean:

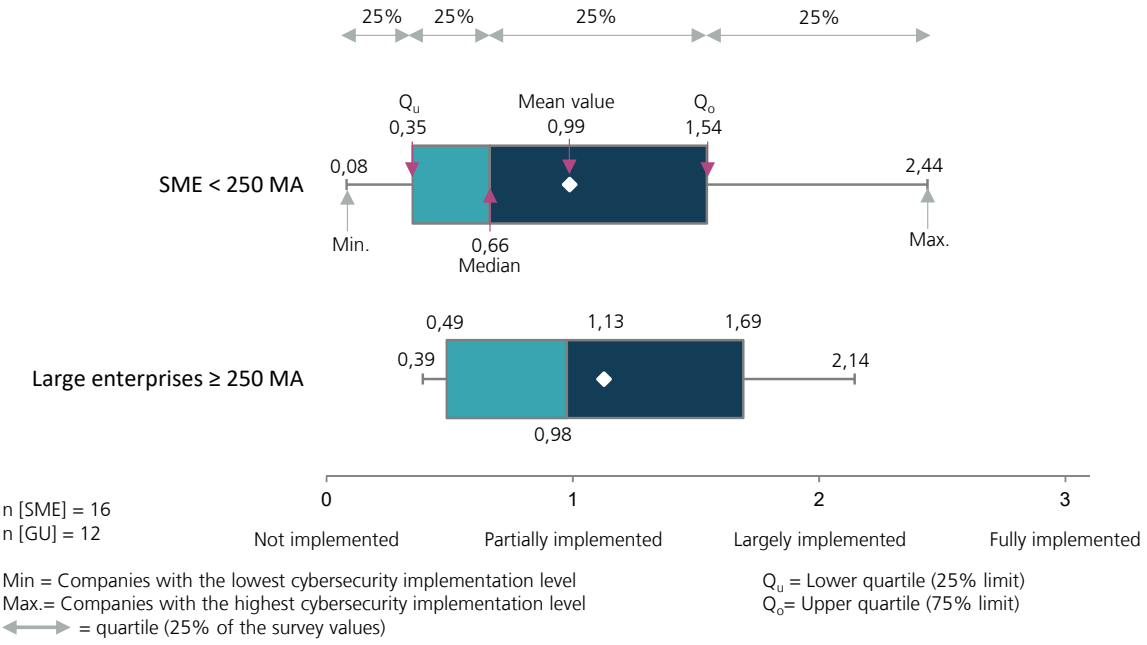

Figure 8: Implementation status of all cybersecurity practices across all domains

1.13; median: 0.98) and the large enterprises (mean: 1.47; median: 1.55). This can be explained by the fact that the management of corporate assets – irrespective of IT security – is a common process, particularly in large companies.

One company from the print media industry has used the GDPR introduced in May 2018 as an opportunity to voluntarily improve asset documentation not only in the IT network but also in the OT network, thus raising the level of security. However, the large companies surveyed see the intrusion of legislation into non-critical sectors such as manufacturing as problematic. They fear overregulation through legislation.

In a detailed representation (Figure 10), we can see that the participating companies certainly have a basic inventory of IT and OT assets that are relevant for production. All other additional information supporting the inventory, such as the mapping of physical and logical connections between assets, is either not implemented – in SMEs – or only partially implemented – in the large companies – which is reflected in the respective mean value. In the case of mapping, one company example shows a historical growth of connections within the company, coupled with poor documentation. As a result, not all connections can be clearly tracked.

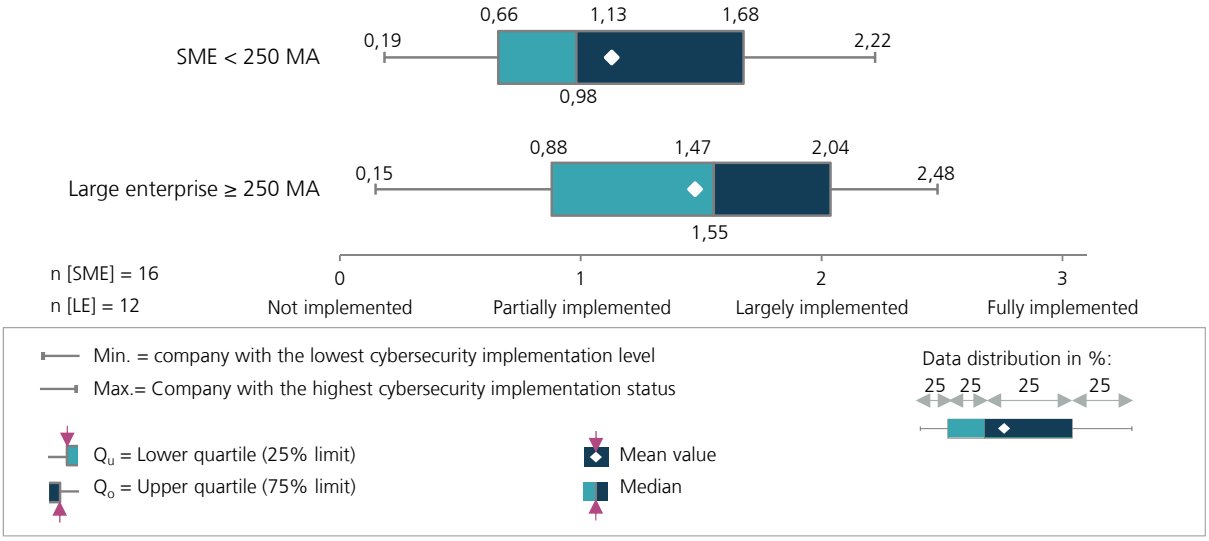

Figure 9: Implementation status of all cybersecurity practices in the ACCM domain

Especially an institutionalization of the activities, i.e. their consolidation in the first three methodological objectives, was not implemented by more than half of the participating SMEs. Viewed in the network diagram (Figure 11), neither the participating SMEs nor the large companies were able to fully achieve the recommended level of implementation. The large enterprises performed better than the SMEs in most building blocks. Base configurations for inventoried assets are partially (SMEs: 1.75) and largely (large enterprises: 2.25) in place to ensure the same configuration for identical assets (see building block ACCM-2.1a). When importing basic configurations to production facilities, IT protection goals are only partially considered. Production facilities from third-party companies act like a kind of black box for companies: i.e. a company must trust what the manufacturer has preconfigured and pre-installed. However, the manufacturers of production facilities often inadequately document the set parameters.

If parameter changes are made to production facilities, companies document these changes regularly, but do not test them with regard to the protection goals (confidentiality, integrity and availability), but only estimate them in a best-practice procedure (cf. modules ACCM-3.1a-3.3g). The reason for this procedure is to avoid production downtime. Another

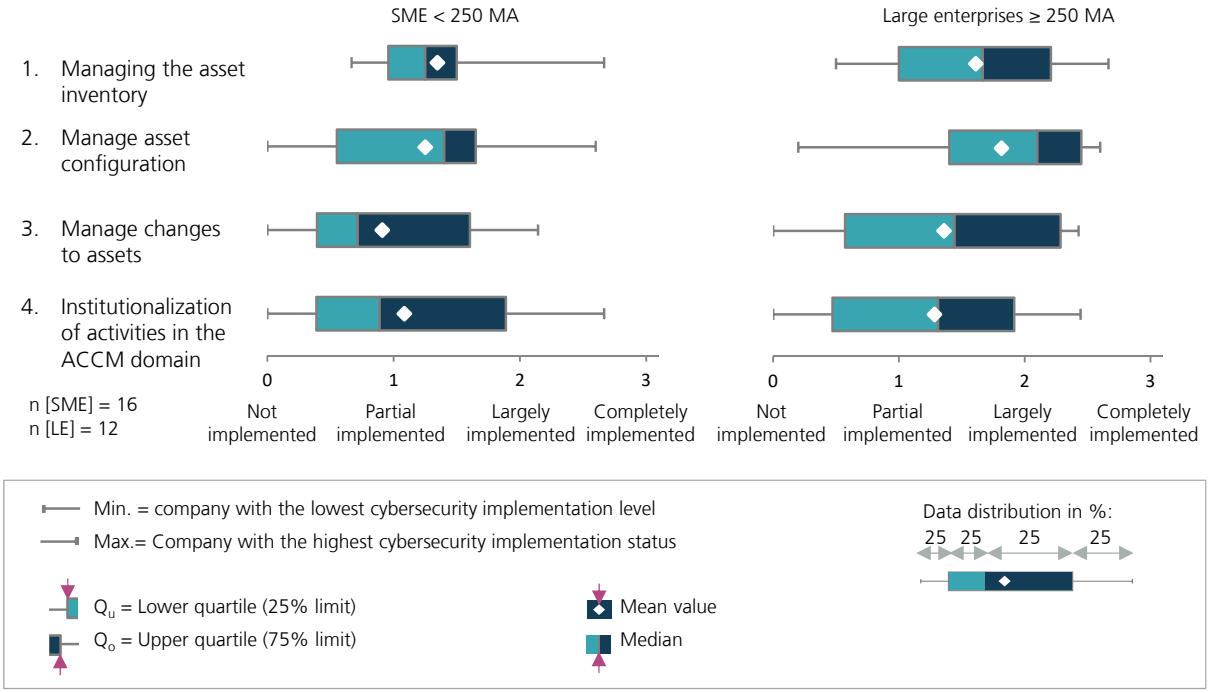

Figure 10: Implementation status of method and management goals in the ACCM domain [35]

reason for the lack of testing of changes is that the choice for plants in production is made according to the best-in-breed principle. This means that individual solutions are identified for each area of application and integrated into the existing infrastructure. This creates a very heterogeneous machine picture, which does not allow the development of a separate test environment (sandbox) with each machine manufacturer. Likewise, the benefit of focusing solely on the availability of a plant is critically evaluated by an expert from a participating mechanical engineering company.

The segmentation and isolation of IT and OT networks and their assets is well known to all companies surveyed, but is not consistently applied, especially by SMEs. In many cases, they do not yet see the need for this because their production does not have a direct connection to the Internet and therefore does not need to be segmented separately. Establishing vertical, cross-level access in the automation pyramid in both directions – while at the same time separating the production systems – is a challenge for SMEs in particular.

Summary of the Results of the Other IT Security Domains

Large companies, especially those listed on the stock exchange, have a general risk management system with well-documented manuals. Within risk management, cybersecurity is predominantly actively addressed in the office network. In production, the risk from cyberattacks is recognized, but only actively targeted in a few cases. The situation is similar among the participating SMEs, although the

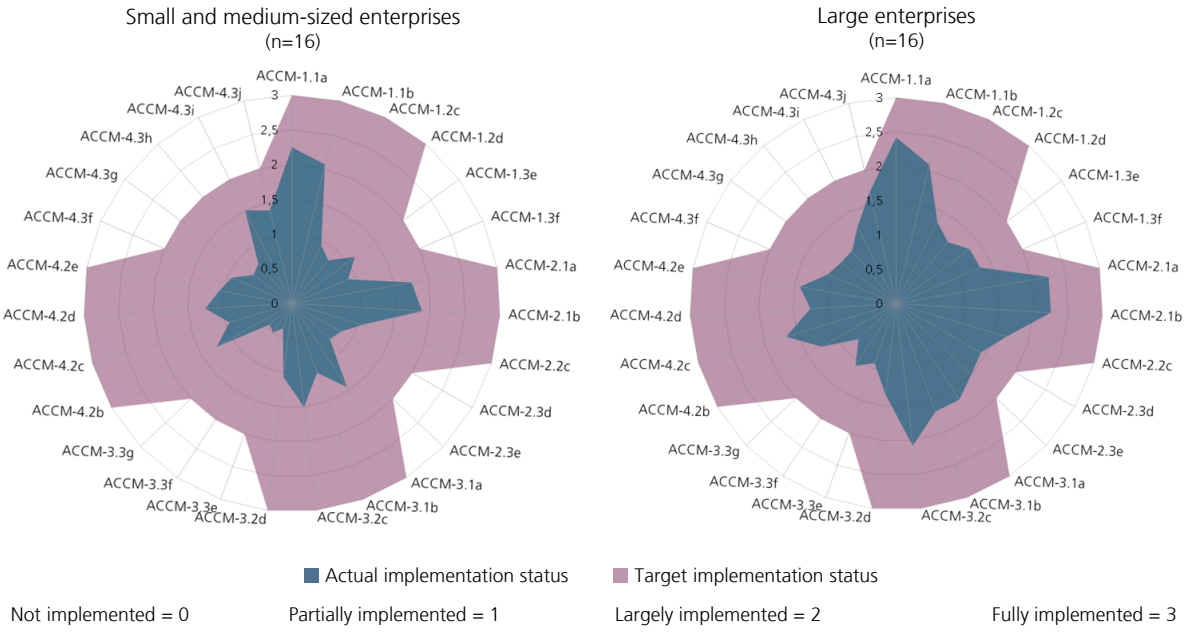

Figure 11: Actual and target implementation status of the individual modules in the ACCM domain

implementation of security measures is even lower on average here. Both the large enterprises and SMEs have difficulty holistically grasping the threat landscape posed by cyberattacks. Quote from one respondent: "You can start anywhere, so to speak." – There is a reluctance to invest in an initial effort. Dealing with the risk of cyberattacks finds a reactive rather than a proactive nature.

Compared to all other domains, the identity and access management domain achieved the highest level of implementation among both SMEs and large enterprises. In this domain, mature directory services such as Windows Active Directory (AD) and off-the-shelf software such as SAP already exist to help enterprises manage the entire lifecycle – from creation to deactivation – of logical and physical access. Similar to the ACCM domain and asset management, processes for managing access and identities have become established in enterprises. A few companies additionally apply the need-to-know principle for access allocation. One large enterprise revealed problems with the allocation of access at production sites outside Germany or Europe. Due to the lack of awareness of security – especially in the Asian and Arabic regions – security risks are incorrectly assessed for poorly administered access, according to the IT administrator. In his opinion, the understanding of security is at a similar level in Europe, the USA and also in India.

Another challenge is the balancing act between security and the user-friendliness of the IT network infrastructure. In concrete terms, this already means regulating the use of USB sticks, for example. On the one hand, a general ban on all USB sticks in the company would drastically reduce user-friendliness; on the other hand, allowing the uncontrolled use of USB sticks would significantly compromise security.

The results of the threat and vulnerability management domain are similar to those of the risk management domain: while large enterprises have a structured approach to eliminating vulnerabilities and threats, SMEs apply these in an ad hoc manner. However, both are overwhelmed by the acceleration of asset update cycles. There are huge differences in how vulnerabilities are handled on different components: while Windows components are subjected to active patch management, companies do not de facto actively patch PLC controllers. If testing is nevertheless carried out, large companies in particular make use of support from the respective manufacturers at the time of patching. However, the exact effects of a patch on a plant cannot be predicted. This is due to the difficulty already described in the ACCM domain, namely that companies do not have test systems and devices on-site in multiple versions.

In the situational awareness domain, companies had to evaluate their activities around logging and monitoring. Logging and monitoring are performed, but not in a comprehensive or goal-oriented framework: production is not considered separately, but logging is done company-wide in the IT and OT network. Large enterprises in particular use so-called security information and event management systems to support the company in their monitoring. SMEs choose an alternative route due to their limited resources: they outsource some of the logging and monitoring activities to service providers who periodically evaluate the logged data. Large enterprises with a high volume of data use common log file analysis tools, but have difficulty configuring thresholds for alerts and warnings to protect the enterprise from cyberattacks. Defining the normal behavior of a network and distinguishing false alarms from true alarms must be done largely by hand. Many manufacturers of production equipment do not clearly communicate to the operating companies what they must, should or can monitor.

The exchange of information and communication regarding cybersecurity topics can be described as inadequate overall: this domain has the second lowest level of implementation of all domains and holds particular potential for improvement. Most of the participating companies, both large enterprises and SMEs, rely exclusively on their own resources and obtain information independently without being active in an exchange network.

Responses to cyber events and incidents, as well as activities around continuity of production, are also not sufficiently implemented. Due to sophisticated attack methods, participating companies fear that they will not detect a large number of attacks. Forward thinking to prevent incidents in general is slow to establish itself. Preventive measures to ensure continuous production are increasingly being developed at large companies with the help of business continuity management. Although this is being demanded by more and more customers of large companies, cybersecurity events play a subordinate role in this. Pro forma contingency plans do exist, but these are rarely tested with a view to an emergency. In the event of a cyberattack or incident, companies prefer to communicate openly internally. For example, a CEO fraud attack is communicated internally via email. IT leaders motivate employees to report any suspicious event. The companies strive to establish a no-blame culture to reduce employees' fear of possible consequences.

Neither the SMEs nor the large companies surveyed are familiar with cybersecurity practices in relation to the entire supply chain. When procuring new equipment, it is rare security requirements are listed in the specifications. The IT department is also rarely involved in procurement processes. Responsibilities as to who is responsible for the security of the system after delivery are inadequately defined between the manufacturer and the operator of a system. In addition, plant operators currently rely on the manufacturer's promises that the delivered plant is secure. No security-related acceptance tests or security audits are carried out. The large companies surveyed have the lowest level of implementation of all domains here.

Despite the low level of implementation of the human risk factor domain, cybersecurity training is an issue at the companies surveyed. However, there is often a lack of consistent implementation: the existence of malware is merely pointed out on the intranet, but active, repetitive training either does not take place at all or at best rarely. Many employees are lulled into a deceptive sense of security that the IT department will protect them against risks. When new employees are hired, the large companies surveyed in particular have written instructions for IT that must be signed by the employees. However, security is only mentioned in passing in these instructions, if at all. A particular challenge is that when technical security measures are introduced, organizational measures in the form of training should not be neglected. Otherwise, there is a very high probability that employees will not understand the meaning of a newly introduced technical measure and will therefore not accept it or even circumvent it.

Figure 12 shows a summary of the remaining domains in quantitative terms.

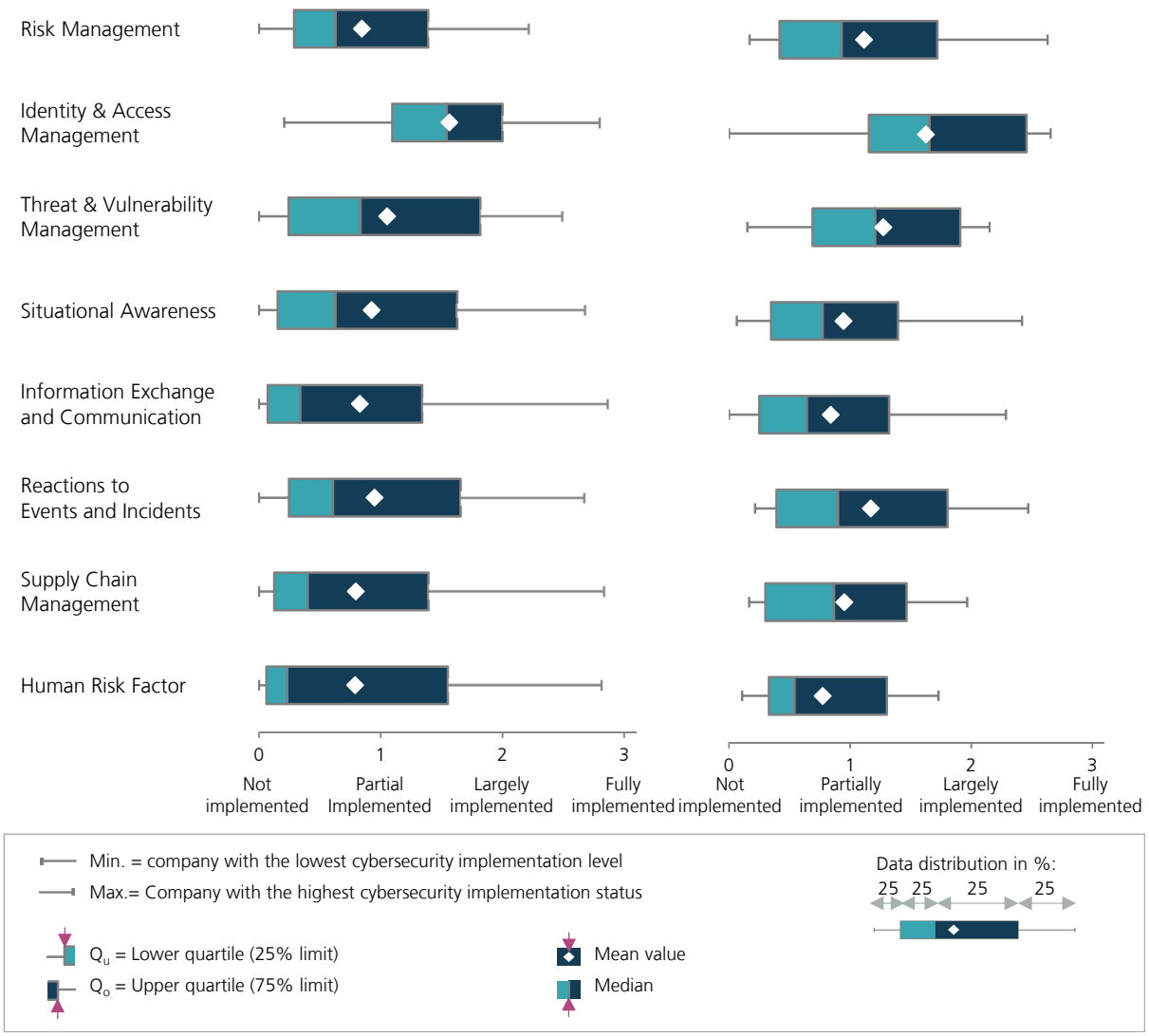

Figure 12: Implementation status of the other domains

OUTLOOK

The study showed that the Production Security Readiness Check can be used to record the security level of individual companies in the manufacturing sector in detail. By revealing its own weak points, the PSRC can thus contribute to improving the security level. With regard to the evaluation, we can confirm that the implementation status of cybersecurity activities does not meet the required level either in SMEs or in large enterprises. In this respect, there is an enormous need for action across all industries – although some companies are already working intensively on this topic in certain domains.

In the interviews, the PSRC received consistently positive feedback. The companies particularly liked the division into different domains, as this makes it clear which security areas they should pay particular attention to in the future. One SME would like to use the PSRC to communicate to management what measures should be defined for expanding cybersecurity in the company. However, the high level of detail in the readiness check sometimes led to difficulties in answering the questions for SMEs without their own IT department. For this target group, both scope and complexity should be reduced. Another option is to adapt the Readiness Check to different industry sectors and their specific requirements. The selected data collection method in the form of a self-assessment proved to be suitable in principle.

In the future, companies can use the one-time documented ACTUAL implementation status as a benchmark reference for the further implementation of cybersecurity practices. The Readiness Check can be consulted as a working aid at regular intervals, as it can document the progress in establishing and improving one's own cybersecurity practices when updated. It enables companies to query their current security level at any time and to identify the vulnerabilities that continue to exist.

In particular, the transformation of the classic automation pyramid into an automation network and, beyond that, into a cyber-physical system will result in further challenges for new technologies. For example, the properties of the new mobile communications standard 5G – high data rates, low latency – will be of great importance and offer new possibilities for wirelessly connecting field devices from critical infrastructures. In this context, cybersecurity will become even more important [39]. It will then become clear to what extent the PSRC can continue to be used in a supporting role.

Overall, the Production Security Readiness Check can already make an important contribution to a more secure IT and OT environment in companies today – especially in the course of increasing digitalization and the growing importance of cybersecurity as a result.

AUTHORS

Raphael Kiesel, M.Sc. M.Sc.
Group manager, Production Quality Department

Alexander Kies, M.Sc.
Research fellow, Production Quality Department

Alexander Kreppein, M.Sc.
Research fellow, Production Quality Department

Timo Heutmann, M.Eng.
Research fellow, Production Quality Department

Jan Dering, M.Sc.
Master thesis researcher, Production Quality Department

Dr.-Ing. Dipl.-Wirt.-Ing. Thomas Vollmer
Head of Production Quality Department

Prof. Dr.-Ing. Robert H. Schmitt
Head of the Chair of Metrology and Quality Management and member of the board of directors for the Laboratory for Machine Tools and Production Engineering WZL of the RWTH Aachen University and member of the board of directors of the Fraunhofer IPT

Acknowledgement

We would like to express our particular thanks to Prof. Dr. Thomas Russack of the FOM University of Applied Sciences for his support in the preparation of the study results.

REFERENCES

[1] Vereinigung der Bayerischen Wirtschaft e. V. (Ed.): Studie – Digitalisierung als Rahmenbedingung für Wachstum. 2017. URL: https://www.baymevbm.de/Redaktion/Frei-zugaengliche-Medien/Abteilungen-GS/Volkswirtschaft/2017/Downloads/FINALE_2018-05-29_Studie-Digitalisierung-als-Rahmenbedingung-f%C3%BCr-Wachstum_2017.pdf [Accessed: 19.03.2021].

[2] Presse- und Informationsamt der Bundesregierung (Ed.): Digitalisierung gestalten – Umsetzungsstrategie der Bundesregierung. 2018. URL: https://www.bundesfinanzministerium.de/Content/DE/Downloads/Digitalisierung/2018-11-15-Digitalisierung-gestalten.pdf?__blob=publicationFile&v=2 [Accessed: 19.11.2020].

[3] McKinsey & Company (Ed.): Digitalisierung im Mittelstand erhöht Wachstum in Deutschland um 0,3 Prozentpunkte pro Jahr. 2017. URL: https://www.mckinsey.com/de/news/presse/digitalisierung-im-mittelstand-erhoht-wachstum-in-deutschland-um-03-prozentpunkte-pro-jahr [Accessed: 15.01.2019].

[4] Statistisches Bundesamt (Ed.): Bruttoinlandsprodukt 2018 für Deutschland. Begleitmaterial zur Pressekonferenz am 15. Januar 2019 in Berlin. 2019. URL: https://www.destatis.de/DE/Presse/Pressekonferenzen/2019/BIP2018/pressebroschuere-bip.pdf?__blob=publicationFile [Accessed: 19.11.2020].

[5] Lichtblau, K.; Schleiermacher, T.; Goecke, H.; Schützdeller, P.: Digitalisierung der KMU in Deutschland. Konzeption und empirische Befunde. 2018. URL: https://www.iwconsult.de/fileadmin/user_upload/projekte/2018/Digital_Atlas/Digitalisierung_von_KMU.pdf [Accessed: 19.11.2020].

[6] Icks, A.; Schröder, C.; Brink, S.; Dienes, C.; Schneck, S.: Digitalisierungsprozesse von KMU im Verarbeitenden Gewerbe. Bonn: Institut für Mittelstandsforschung (IfM) Bonn, 2017. http://hdl.handle.net/10419/156246

[7] Deutsche Telekom AG (Ed.): Security on the Industrial Internet of Things. How companies can defend themselves against cyber attacks. 2016. URL: https://www.t-systems.com/blob/269626/1c7f8ae72c3e86714a4ffc47aeaef407/DL_WP_Security%20M2M.pdf [Accessed: 19.11.2020].

[8] Hahn, A.: Operational Technology and Information Technology in Industrial Control Systems. In: Colbert, E. J. M.; Kott, A. (Eds.): Cyber-security of SCADA and Other Industrial Control Systems. Cham: Springer International Publishing, 2016, pp. 51-68.

[9] Kaspersky Lab ICS CERT (Ed.): Threat Landscape for Industrial Automation Systems in H2 2017. 2018. URL: https://ics-cert.kaspersky.com/media/KL_ICS_REPORT_H2-2017_FINAL_EN_22032018.pdf [Accessed: 19.11.2020].

[10] Center for Strategic & International Studies (Ed.): Significant Cyber Incidents. n.d. URL: https://www.csis.org/programs/cybersecurity-and-governance/technology-policy-program/other-projects-cybersecurity [Accessed: 15.01.2019].

[11] F-Secure GmbH (Ed.): Live Security Studie 2017/2018. Eine repräsentative Untersuchung von Bitkom Research im Auftrag von F-Secure. 2018. URL: https://blog.f-secure.com/wp-content/uploads/2018/05/f-secure-live-security-studie-2017_2018.pdf [Accessed: 19.11.2020].

[12] Bundesministerium für Wirtschaft und Energie (Ed.): IT-Sicherheit für die Industrie 4.0. Produktion, Produkte, Dienste von morgen im Zeichen globalisierter Wertschöpfungsketten. Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie. Abschlussbericht. 2016. URL: https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/it-sicherheit-fuer-industrie-4-0.pdf?__blob=publicationFile&v=4 [Accessed: 19.11.2020].

[13] Stobitzer, C.: Schutzziele der Informationssicherheit. 2017. URL: http://www.kryptowissen.de/schutzziele.php [Accessed: 27.07.2018].

[14] Eckert, C.: IT-Sicherheit. Konzepte - Verfahren - Protokolle. 8th ed. Munich: De Gruyter, 2013.

[15] Holznagel, B.: Recht der IT-Sicherheit. Munich: Beck, 2003.

[16] Gadatsch, A.; Mangiapane, M.: IT-Sicherheit. Digitalisierung der Geschäftsprozesse und Informationssicherheit. Wiesbaden: Springer Vieweg, 2017.

[17] Dustdar, S.; Gall, H.; Hauswirth, M.: Software-Architekturen für Verteilte Systeme. Prinzipien, Bausteine und Standardarchitekturen für moderne Software. Berlin, Heidelberg: Springer, 2003.

[18] Bedner, M.; Ackermann, T.: Schutzziele der IT-Sicherheit. In: Data Protection and Data Security – DuD. Vol. 34, 2010, No. 5, pp. 323-328. http://doi.org/10.1007/s11623-010-0096-1

[19] Schneider, F.: IT-Sicherheit 2018: Pflichten für Unternehmen. 2018. URL: https://www.cmshs-bloggt.de/tmc/it-recht/it-sicherheit-2018-sicherheit-fuer-unternehmen/ [Accessed: 12.07.2018].

[20] TeleTrusT – Bundesverband IT-Sicherheit e.V. (Ed.): IT-Sicherheitsgesetz und Datenschutz-Grundverordnung: Handreichung zum Stand der Technik technischer und organisatorischer Maßnahmen. Revidierte und erweiterte Ausgabe 2018. 2018. URL: https://www.teletrust.de/fileadmin/docs/fachgruppen/ag-stand-der-technik/TeleTrusT-Handreichung_Stand_der_Technik_-_Ausgabe_2018.pdf [Accessed: 17.07.2018].

[21] Bundesamt für Sicherheit in der Informationstechnik – BSI (Ed.): Schutz Kritischer Infrastrukturen durch IT-Sicherheits-

gesetz und UP KRITIS. 2017. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Schutz-Kritischer-Infrastrukturen-ITSig-u-UP-KRITIS.pdf?__blob=publicationFile&v=7 [Accessed: 19.11.2020].

[22] Bundesministerium für Wirtschaft und Energie (BMWi) (Ed.): IT-Security in der Industrie 4.0. Handlungsfelder für Betreiber. Leitfaden. 2016. URL: https://www.plattform-i40.de/PI40/Redaktion/DE/Downloads/Publikation/leitfaden-it-security-i40.pdf?__blob=publicationFile [Accessed: 19.11.2020].

[23] Heinrich, B.; Linke, P.; Glöckler, M.: Grundlagen Automatisierung. Sensorik, Regelung, Steuerung. 2nd, revised and extended edition. Wiesbaden: Springer Vieweg, 2017.

[24] INAUT Automation GmbH (Ed.): Ganzheitliche Lösung. n.d. URL: http://www.invilution.com/ganzheitliche-loesung [Accessed: 12.08.2018].

[25] Wiesel, C.: Was ist wo los im Netz? Permanente und passive Analyse der Kommunikationsqualität in Profinet-Netzwerken. In: messtec drives Automation. Vol. 25, 2017, No. 10, pp. 14-16.

[26] Stouffer, K.; Pillitteri, V.; Lightman, S.; Abrams, M.; Hahn, A.: Guide to Industrial Control Systems (ICS) Security. Supervisory Control and Data Acquisition (SCADA) systems, Distributed Control Systems (DCS), and other control system configurations such as Programmable Logic Controllers (PLC). 2015. http://dx.doi.org/10.6028/NIST.SP.800-82r2

[27] Vogt, M.; Sherman, A.: 3D-Snapshot-Kameradaten in der Industrie: Wie Edge-Computing die optimale Datenbereitstellung ermöglichen kann. Sick AG Whitepaper. 2018. URL: https://cdn.sick.com/media/docs/1/41/041/Whitepaper_3D_SNAPSHOT_CAMERA_DATA_IN_INDUSTRY_de_IM0077041.PDF [Accessed: 19.11.2020].

[28] Niemann, K.-H.; Hoh, M.: Anforderungen an die IT-Sicherheit von Feldgeräten. Schutzlösungen für hoch vernetzte Produktionsanlage. In: atp edition. Vol. 59, 2017, No. 12, pp. 42-53.

[29] Khondoker, R.; Larbig, P.; Scheuermann, D.; Weber, F.; Bayarou, K.: Addressing Industry 4.0 Security by Software-Defined Networking. In: Zhu, S.; Scott-Hayward, S.; Jacquin, L.; Hill, R. (Eds.): Guide to Security in SDN and NFV. Challenges, Opportunities, and Applications. Cham: Springer International Publishing, 2017, pp. 229-251. https://doi.org/10.1007/978-3-319-64653-4_9

[30] Fireeye iSight Intelligence (Ed.): Overload. Critical lessons from 15 years of ICS Vulnerabilities. 2016 Industrial Control Systems (ICS) Vulnerability Trend Report. 2016. URL: https://www.tripwire.com/-/media/tripwiredotcom/files/solution-brief/ics-vulnerability-trend-report-final.pdf?rev=f9b8f49716224a10a1639d36582ec269 [Accessed: 19.11.2020].

[31] Kaspersky Lab ICS CERT (Ed.): Threat Landscape for Industrial Automation Systems in the second half of 2016. 2017. URL: https://ics-cert.kaspersky.com/reports/2017/03/28/threat-landscape-for-industrial-automation-systems-in-the-second-half-of-2016/ [Accessed: 19.11.2020].

[32] European Union Agency for Network and Information Security: Communication network dependencies for ICS/SCADA Systems. 2017. https://doi.org/10.2824/397676

[33] Bundesamt für Sicherheit in der Informationstechnik (BSI) (Ed.): Die Lage der IT-Sicherheit in Deutschland 2017. 2017. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?__blob=publicationFile&v=4 [Accessed: 19.11.2020].

[34] Department of Homeland Security (Ed.): Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies. Industrial Control Systems Cyber Emergency Response Team. 2016. URL: https://us-cert.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf [Accessed: 19.11.2020].

[35] U.S. Department of Energy (Ed.): Cybersecurity Capability Maturity Model (C2M2). Version 1.1. 2014. URL: https://www.energy.gov/sites/prod/files/2014/03/f13/C2M2-v1-1_cor.pdf [Accessed: 19.11.2020].

[36] Standard DIN EN ISO/IEC 27001:2017-06. Informationstechnik - Sicherheitsverfahren - Informationssicherheitsmanagementsysteme - Anforderungen. https://dx.doi.org/10.31030/2634923

[37] National Institute of Standards and Technology (Ed.): Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. 2018. https://doi.org/10.6028/NIST.CSWP.04162018

[38] Bundesamt für Sicherheit in der Informationstechnik (Ed.): BSI-Standard 200-2. IT Grundschutz-Methodik. 2017. URL: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Kompendium/standard_200_2.pdf?__blob=publicationFile&v=7 [Accessed: 19.11.2020].

[39] Ahmad, I.; Kumar, T.; Liyanage, M.; Okwuibe, J.; Ylianttila, M.; Gurtov, A.: 5G security: Analysis of threats and solutions. In: Institute of Electrical and Electronics Engineers (Ed.): 2017 IEEE Conference on Standards for Communications and Networking (CSCN). 2017 IEEE Conference on Standards for Communications and Networking (CSCN) took place 18-20 September 2017 in Helsinki, Finland. Piscataway: IEEE, 2017, pp. 193-199. https://doi.org./ 10.1109/CSCN.2017.8088621

Cybersecurity in Networked Production
White Paper Fraunhofer IPT

Authors
Raphael Kiesel, Alexander D. Kies,
Alexander Kreppein, Timo Heutmann,
Jan Dering, Thomas Vollmer,
Robert H. Schmitt

Fraunhofer Institute for
Production Technology IPT
Steinbachstrasse 17
52074 Aachen
Germany
Phone +49 241 8904-0
info@ipt.fraunhofer.de
www.ipt.fraunhofer.de

Your Contact
Jonathan Krauß, M.Sc.
Head of Production Quality Department
Phone +49 241 8904-475
jonathan.krauss@ipt.fraunhofer.de

Alexander Kreppein, M.Sc.
Research fellow, Production Quality Department
Phone +49 241 8904-289
alexander.kreppein@ipt.fraunhofer.de

ISBN 978-3-00-068591-0
DOI: 10.24406/ipt-n-633345