2nd Conference on Production Systems and Logistics

Derivation Of Counter-Measures For Industry 4.0 Environments And Cyber-Physical Production Systems Based On Their Cyber-Security Vulnerabilities

Günther Schuh[1], Jacques Engländer*[1], Lars Kaminski[1], Jan Hicking[1], Martin Bülskämper[1]

[1]*Institute for Industrial Management, FIR at RWTH Aachen University, Campus-Boulveard 55, Aachen 52074, Germany | *Corresponding author*

Abstract

The digital transformation is changing the way companies think and design their manufacturing environment. Both due to the increasing number of connections between IoT-Devices, tooling machines, and production lines and the phenomenon of the convergence of IT and OT, systems are becoming more complex than years ago. Organizational and cultural changes within manufacturing companies strengthen this trend and form Industry 4.0 environments and cyber-physical production systems (CPPS). As these systems do not longer stay alone but are connected to each other and the company's outside, the size of the potential attack surface is increasing as well. Besides that, manufacturing companies, small and medium-sized in particular, are facing complex challenges based on lack of knowledge, budget, and time to understand as well as to interpret their current situation and risk level and therefore to derive necessary counter-measures. Efficient as well as pragmatic tools and methods for these companies do not exist. This paper shows a research approach in which the company-specific set-up of Industry 4.0 environment and CPPS is characterized by its potential vulnerabilities. This enables companies to evaluate their risk potential before setting up this kind of environments and to undJo,erstand the potential consequences more precisely. By doing so, companies can derive and prioritize important counter-measures and so to strengthen their level of cyber-security efficiently. This will decrease the number of cyber-security attacks and increase the company's competitiveness.

Keywords

Cyber-Security; Industry 4.0 Environments; Manufacturing Companies; SMEs; Digital Transformation;

1. Introduction

The digital transformation of manufacturing companies is changing the way on how we think about organizational, technical, cultural, and processual relations. We see shifting paradigms in manufacturing companies through Industry 4.0 [1], which need to be addressed in several ways. These paradigms are required for so-called cyber-physical production systems (CPPS), which are formed by former standalone cyber-physical systems (CPS). Those CPS are physical systems such as machines, tools, or electrical components, enriched with cyber aspects such as software components. Therefore, they are characterized by a deep linking of physical and computational elements. On a higher enterprise level, this convergence of information technology (IT) and operational technology (OT) is called IT/OT-convergence, forming the Industrial Internet of Things (IIoT). It enables companies to now understand patterns, which had been an unknown unknown in the past, by analyzing data from former silos.

DOI: https://doi.org/10.15488/11253

The result is, that the security goals of both IT and OT are merging [2]. Due to the fact, that these IIoT-systems are complex by their nature and are becoming even more complex because of new technologies and further developments, manufacturing companies seem to be overburdened by questions such as how to manage and how to secure these systems. As cyber- and information-security have always been an important aspect to take into account, its importance is continuously growing due to the convergence of different domains. It is no longer acceptable just to secure single components, the realization of cyber-security needs to happen on an entire system level [3]. Therefore, the trustworthiness of IIoT-systems is becoming an important success factor for manufacturing companies. While many companies understand the need, they face significant challenges in implementing it. Lots of existing regulations, standards, and frameworks are too extensive to be applicable by SMEs. Furthermore, they are characterized by a lack of brownfield approaches, because the large number is not taking existing frame conditions into account. The fact that SMEs are suffering from limited resources, budget, know-how, and time complicates their situation [4]. Therefore, we focus on the following three aspects in this paper:

- Modeling of Industry 4.0 environments based on existing but adopted frameworks
- Mapping of the models' intersections and most relevant vulnerabilities for SMEs
- Derivation of counter-measures for a cost-benefit-efficient perspective

As these three aspects do also represent a stepwise approach that can be integrated into an overall risk assessment, this paper will help SMEs to identify their largest gaps in cyber-security based on their existing environment. The mapping of vulnerabilities to the Industry 4.0 environment will enable companies to derive them without specific knowledge about cyber-security, but instead about their IIoT-systems. The goal is to show SMEs an efficient and pragmatic way to start first cyber-security initiatives on their own. The scope is not to make norms and standards obsolete, but to lower the entry threshold for SMEs by shifting the focus and starting point to a well-known area, their IIoT-Systems, and Industry 4.0 environment.

2. State of the art

The research in the field of cyber-security has increased over the last years. Especially the combination of cyber-security aspects in manufacturing companies implementing Industry 4.0 use cases has become an important research topic. This section, therefore, presents important norms and standards, IIoT reference architectures as well as approaches for threat modeling and vulnerability identification and shows their gap in comparison to the practical needs of SMEs.

2.1 Norms and standards

Norms and standards related to information security are often designed based on different target groups and fields of topics. They help to increase the information security level as well as to simplify the communication between different institutions about the controls to be applied. [5] As there are different standards across different countries, institutions, and sectors[1], lately, activities tried to consolidate them as well as make them interoperable. Currently, the standard ISO/IEC 62443 is the most actively processed one in the field of Industry 4.0, while it makes use of existing norms and standards [7].

Within the standard ISO/IEC 62443, the International Electrotechnical Commission (IEC) defines a security standard for an industrial automation and control system (IACS). It consists of several parts and subparts. The first part describes foundational terminology and basic knowledge. The second part especially deals with requirements related to an IACS information security management system. Besides that, it consists of methods related to patch management. Security technologies, levels, and requirements in general and related

[1] The European Union Agency For Network And Information Security (ENISA) published a list with around 50 existing information security and privacy standards for SMEs [6].

to specific topics are described in part three. In more detail, part four lastly deals with security requirements for IACS components and general requirements along the product development process of those components. It takes different principles into account, e.g. defense in depth (different security levels arranged from the outside (lowest security level) to the inside (highest security level)) and zones & conduits (system divided into several zones related to specific security levels and the communication in between).

The international and cross-sector standard ISO/IEC 27001 aims to support companies to manage their information security. It specifies requirements for establishing, implementing, maintaining, and continually improving an information security management system (ISMS). Furthermore, the assessment and treatment of risks related to information security is also part of the standard. The way the requirements are set out in ISO/IEC 27001:2013 is generic so that they can be applied to all organizations. [6] The standard is a relevant part of the superordinate row of ISO/IEC 2700X standards, which in total includes over 20 norms.

The Bundesamt für Sicherheit in der Informationstechnik (BSI) in Germany developed and continually improves the IT-Grundschutz. Since 2005 it is divided into the approach for IT-Grundschutz and several IT-Grundschutz catalogs. Besides management aspects, technical, organizational, personal, and infrastructural controls are described. The four norms BSI-Standard 200-1, 200-2, 200-3, and 100-4 are related to requirements to ISMS, the approach to use the standard, risk analysis based on the IT-Grundschutz, and incident management. The BSI-Standard 200-1 is widely comparable with the ISO/IEC 27001 norm and also considers aspects of ISO/IEC 27000 and 27002. Taken every part into account, the standards consist of more than 5000 pages and 1200 controls. [8]

2.2 IIoT Reference Architectures

Reference architectures are important for describing specific systems. Related to IIoT-systems and Industry 4.0 environments, several well-known architectures have been developed over the last decade. Studies with up to 430 investigated papers show that a large number of architectures exist just in the field of Industry 4.0. In the following, we will describe the most important and near-standard reference architectures in more detail.

The Reference Architecture Model Industrie 4.0 (**RAMI 4.0**), formulated in the norm DIN SPEC 9134, represents one of the first reference models related to Industry 4.0. Besides the definition of terms, it describes different assets in Industry 4.0 and their characteristics. In general, RAMI 4.0 differentiates between the physical world (real assets) and the digital world (data and information). Systems are then described in three axes: **life cycle & value stream** (development to maintenance), **hierarchy levels** (product to connected world), and **architectural layers** (asset to business). The structural design of IIoT-systems, assets, and combination of assets are defined with the help of those axes and layers. Each layer is seen alone but interconnected with the layer above and below. [9]

The Industrial Internet Reference Architecture (**IIRA**) is similar to RAMI 4.0 while describing different layers. In contrast to the three-axes architecture of RAMI 4.0, IIRA uses a **viewpoint-**, **concern-** and **stakeholder-approach** to describe IIoT-systems [10]. Especially the viewpoints (business, usage, functional, and implementation) allow the user to extensively describe the system. They provide stakeholders with the necessary detail to describe their concerns.

Within the Norm **DIN EN 62264-1** a process-driven approach for integrating the corporate and control level is focused. It is based on **ISA-95** specifications and takes the **PERA** (Purdue Enterprise Reference Architecture) model as a basis. The norm serves as a relevant standard for defining the automation pyramid. The automation pyramid has been an important model to describe technical systems and their interconnections related to the shop floor and the automation environment. Nevertheless, due to the paradigm shift through Industry 4.0, the pyramid is becoming outdated, even if its generic structure is still applicable to most manufacturing companies.

2.3 Threat Modeling

SMEs facing challenges with their cyber-security often see themselves struggling with deriving the most relevant threats and vulnerabilities concerning their Industry 4.0 environment. Besides existing studies on the most relevant vulnerabilities such as missing employee awareness or missing patch management, external consultancies assessing these environments as well as expensive hardware or software solutions, SMEs seem to stand alone without any guidance on the topic. A possible way for SMEs to derive their vulnerabilities is given by threat modeling. As a process, it represents a special form of model building. By developing a threat model, companies can derive potential threats for the model of the systems concerned [11]. Extensive threat models are often developed and applied as part of system (software) development to strengthen the principle of "security by design". Therefore, the applicability for manufacturing SMEs is limited, even though principles can be valuable guidelines during development [12]. The framework for modeling threats often consists of the following four steps [11]:

1. Modeling of the system to be built, deployed, or changed
2. Finding threats using existing models such as STRIDE
3. Addressing threats based on the model
4. Validating for completeness and effectiveness

It is important to understand that there is not the “one correct” way for modeling threats. The four-step approach just gives the frame conditions which have to be detailed and tailored to the specific situation in which a company is situated. Furthermore, it is important to always focus on the result to be achieved. If the model shows several threats and works to deal with them, it will empower the company. [11] In combination with other tools, threat modeling gains even more power. Existing vulnerability ontologies [13–15], specialized methods for vulnerability identification [16,17], methods like STRIDE [18] or CVE [19], and automated solutions such as AI-based Twitter searches [20] help to increase the benefit of threat modeling.

Therefore, threat models can be used for developing generic frameworks. In this paper, we made use of threat modeling for the development of the framework and approach in chapter 3. STRIDE will serve as the most mature model in this context.

2.4 Research gap

It can be stated that a lot of standards do exist, but even if they are intended to be universally applicable, they are often not applicable to SMEs due to their scope and size [4]. Not least because of this, there are numerous guides for implementing the various standards (see for example [21,22]). SMEs are facing different challenges than bigger companies, such as restricted budget, a lack of knowledge, and missing structures [6]. Same counts for existing architectures. They are mostly not applicable for SMEs to their cyber-security concerns [12]. Especially RAMI 4.0 and IIRA are not useful in a practical way, because of their generic character [23]. Threat modeling and existing threat models give a good starting point for SMEs to start with their cyber-security. But without knowledge within the company and guidance on choosing the right additional tool, it is hard for SMEs to do it with high completeness and effectiveness [24].

3. Framework

In this paper, we propose a framework based on existing standards, reference architectures, and approaches applicable for SMEs. The framework aims to provide SMEs with an instrument to manage their cyber-security related to Industry 4.0 environments on their own and without deep expertise and a high budget. Within the framework, not only technical but also organizational and personal aspects are taken into account to serve as a holistic approach in SMEs. Furthermore, the framework is developed to be applicable for effectiveness and efficiency.

3.1 Structure of the framework

Following KAMAL [25] respectively ZACHMAN [26], a systematic approach to study cyber-security is based on the decomposition of the system to be modeled answering the following questions:

- **What?** – Description of the system and its components relevant to the threat model
- **Why?** – Description of the primary business objective to accomplish a primary goal
- **How?** – Description of the function to achieve the goal
- **Who?** – Description of the human factor in each system
- **When?** – Description of the system's lifecycle
- **Where?** – Description of the components in the context of the physical environment

Those questions can be mapped on a security-related Industry 4.0 reference architecture developed for this paper shown in Figure 1. The '**What?**' represents affected assets through component layers in accordance to e.g. RAMI 4.0. Furthermore, it is extended by the three important aspects Business ('**Why?**'), Function ('**How?**') and Human ('**Who?**'). The '**When?**' represents the security life-cycle, starting with the initiation phase and ending with disposal, to include principles such as security-by-design and phase-specific vulnerabilities. Lastly, the '**Where?**' shows the physical location respectively zones for (sub-)systems as it does the PERA model for example.

The model claims to be comprehensive, layered, and modular at the same time [25]. Comprehensive means that the model offers the opportunity to derive the most relevant threats respectively vulnerabilities, even if it just represents a part of the real world. While looking at SMEs, focusing on the most relevant vulnerabilities instead of filling lots of libraries, helps to stay focused while having a lack of budget. The layered approach helps to reduce complexity within systems, so that companies, especially SMEs, can partially describe their Industry 4.0 environment. Model modularity means that different situations can be described separately from each other, which lowers the entry point for SMEs using the framework. The six questions represent six viewpoints, described below.

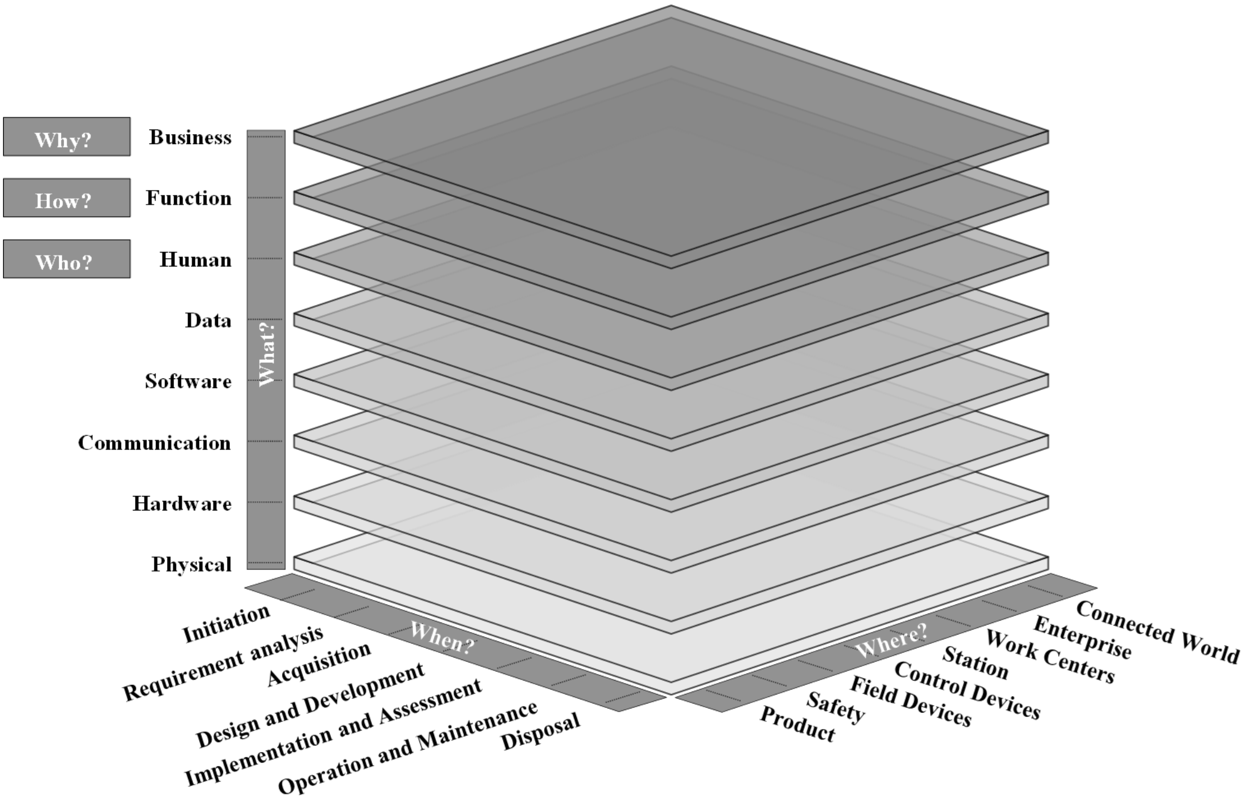

Figure 1: Security-related Industry 4.0 reference architecture

What – Asset-driven: The starting point of modeling the IIoT-system is to make sure to only take those assets into account which are worth protecting the most. These assets can be physical (e.g. machines), software or hardware assets, communication-related assets such as a router, or data in particular.

Why – Business-driven: To be able to make assumptions on the potential risk an IIoT-system is exposed to, the business-driven viewpoint is important to consider business decisions. Whether an IIoT-system has a supportive function or is highly crucial for the stability of the production process implies the needed security level, even if the vulnerabilities may be the same. Furthermore, the viewpoint allows considering stakeholder-specific, supply-chain-related, and tier-oriented aspects.

How – Function-driven: The goal to be achieved by an IIoT-system relies on the system's function. Meant are functional components, their skills as well as their interconnections and interfaces [27]. Concerning cyber-security, a failure of this function would represent an event, which has to be avoided. On the other hand, the system's function should not be influenced negatively by security counter-measures.

Who – Human-driven: To reflect the fact that a large number of attacks on companies are due to employee misconduct [28], the human-driven viewpoint represents the role of the person in front of the system, following the OSI-model and humorously called Layer-8. Besides that, humans are also seen as assets that need to be considered within threat modeling, e.g. concerning environmental threats.

When – Life-cycle-driven: Most of the IIoT-systems do not represent greenfield-like environments. They are embedded in a specific context and situation. Taking these, costs during the design phase and the resulting decrease in business performance into account, the security life-cycle often does not take precedence the running business [29]. Nevertheless, the consideration of each life-cycle phase will help to identify and mitigate vulnerabilities. Each phase is linked to concrete processes and security controls such as the evaluation of tenders within the acquisition phase.

Where – Location-driven: To specify and locate the concrete vulnerability, it seems obvious to model the explicit assets' location. Therefore, the location-driven viewpoint can be seen as an additional viewpoint regarding the assets and their location within the company. For example, IIoT-devices close to the manufacturing process can be mapped on the field device layer, IIoT-devices communicating with SCADA or historian servers on the control layer.

3.2 Framework approach

As the framework itself does not help to identify the most relevant vulnerabilities within IIoT-systems of manufacturing companies, we developed a method in addition to the framework (see Figure 2). It makes use of existing approaches in the field of threat modeling (e.g. [11]) but extends them with a more detailed view on templates and SME-specific challenges. The scalable method works as guidance, mapping the most relevant and universal vulnerabilities to the framework. These vulnerabilities are pre-defined by the author.

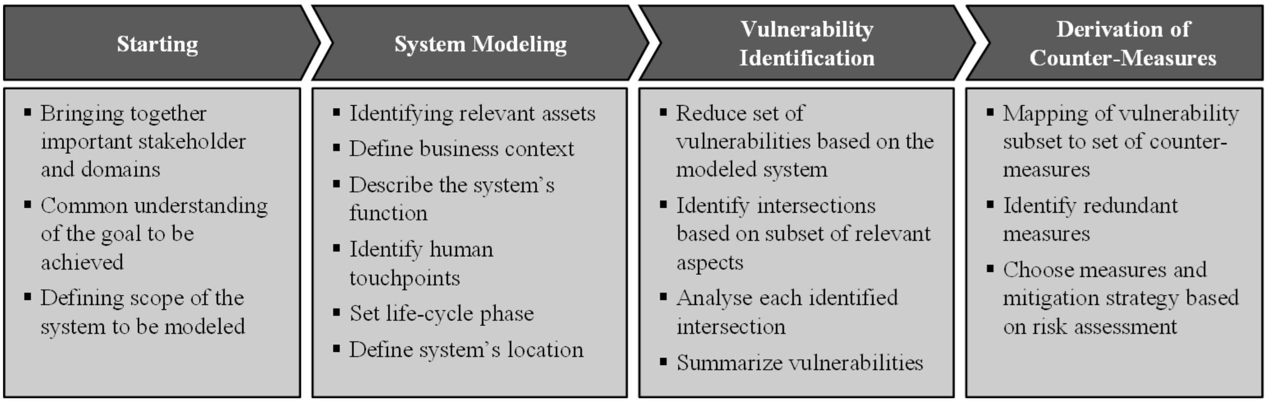
Starting
Bringing together important stakeholder and domains
Common understanding of the goal to be achieved
Defining scope of the system to be modeled
System Modeling
Identifying relevant assets
Define business context
Describe the system`s function
Identify human touchpoints
Set life-cycle phase
Define system`s location
Vulnerability Identification
Reduce set of vulnerabilities based on the modeled system
Identify intersections based on subset of relevant aspects
Analyse each identified intersection
Summarize vulnerabilities
Derivation of Counter-Measures
Mapping of vulnerability subset to set of counter-measures
Identify redundant measures
Choose measures and mitigation strategy based on risk assessment

Figure 2: Structure of the approach

First of all, starting a security project needs management attention and important stakeholder from relevant domains at one table. This secures a common understanding of the goal to be achieved by the security project. Additionally, as part of the contextual integration, the common understanding results in condition frames need to be taken into account when defining the scope of the system to be modeled. The distinction between systems and their subsystems is necessary, as this changes elements such as zones and interconnections. Afterward, the before-mentioned questions are based on given templates. These templates are related to existing methods and frameworks, e.g. modeling data flow diagrams or use case diagrams. The application of templates will help SMEs to better understand the connection between their IIoT-system and cyber-security vulnerabilities. In case some assets and their locations, as well as life-cycle phases, are not relevant to the IIoT-system, they are left out. System-related information regarding the business objective will for example decrease the number of vulnerabilities if the IIoT-system does not have interconnections with external entities. After modeling the system, vulnerability identification takes place. The interconnections of each relevant aspect (see Figure 3) will then lead to vulnerabilities linked to those interconnections. Therefore, the result will be a list of relevant vulnerabilities with respect to the modeled systems. Lastly, the derivation of counter-measures is based on a mapping to the identified vulnerabilities. At this point, it is crucial to compare counter-measures among themselves as they may occur more than once. This will lead to the derivation of mitigation strategies which are developed under the premise of cost-benefit-aspects.

4. Use case example

In this section, we use a compromised use case as an example. Figure 3 creates a better understanding of the mentioned intersections. In this case, we look at the intersection of data as an asset, located close to the control device layer within the acquisition phase (**data × control device × acquisition**). The question to be answered now is which vulnerabilities are linked with this interconnection. In this case, the **STRIDE** framework was used to identify possible vulnerabilities (see Table 1).

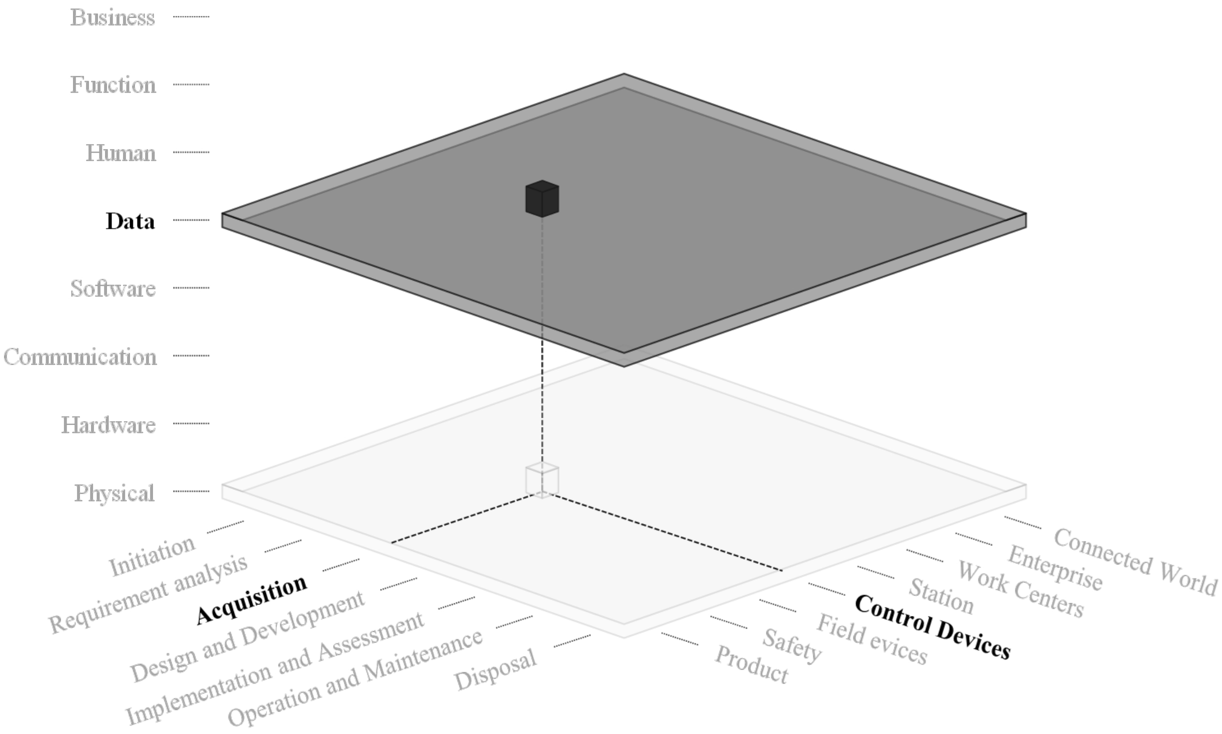

Figure 3: Example of interconnection

In the production environment, there are usually countless control devices that communicate with each other, with field devices, stations, or work centers. It must always be clear who is talking to whom, and that secure authentication is essential. Various authentication methods such as single key, access token, or signatures are possible. Therefore, it is important to think about the appropriate authentication procedure already during the acquisition phase and not to use default keys or methods that are freely available in user instructions or on the internet. This is a widespread attack vector on embedded IoT devices today [30].

Control devices such as PLCs, RTUs, or routers are mainly located in the production environment, where physical access to them cannot be fully controlled. For this reason, it is necessary to consider sufficient physical hardening of the devices already during the acquisition phase to protect their integrity. Physical hardening prevents for example employees or guests from physically manipulating control devices (e.g., drag plugs) which can lead to data loss or an interruption of process control. Furthermore, this can be associated with financial or physical damages, including personal injury.

The purchase of control devices should also be accompanied by the implementation of a suitable event management system. When purchasing control devices, it is therefore important to ensure that they support appropriate functions. This means that access attempts or attacks on individual control devices can be linked to each other (e.g., if IP addresses of accesses are stored). Thereby patterns can be detected, such as attacks on critical production systems. It can also be used to reconstruct and trace attacks.

The acquisition phase deals primarily with the identification of security requirements, the evaluation of proposed security controls, and reviewing and finalizing security design. Therefore, not considering security requirements for control devices such as PLCs represents a vulnerability to the later system, as not assessing the tender and security specification do. Furthermore, this is crucial for future integration activities. [29] For example, the underlying communication of the control devices should be designed with taking future security requirements into account. Otherwise, there is a risk of disclosing confidential data.

A denial-of-service threat affects the availability of devices by using the individual resources of the device. If such attacks are detected at an early stage, appropriate counter-measures can be taken. However, this requires continuous monitoring of the individual data of each device and the search for anomalies. During the acquisition process, care should also be taken to ensure continuous patch management in the future (e.g., that the manufacturer of the control devices provides patches regularly). Among other things, patches are used to eliminate exploits that are used by intruders, for example, to gain additional rights in the system (elevation of privilege). This type of attack is often used, for example, to introduce malware.

Table 1: Exemplary vulnerabilities for data × control device × acquisition

Threat	Property violated	Exemplary vulnerabilities
Spoofing	Authentication	Weak or default authentication methods
Tampering	Integrity	Lack of physical hardening
Repudiation	Non-repudiation	No event management
Information disclosure	Confidentiality	Unencrypted communication
Denial-of-service	Availability	No device monitoring
Elevation of privilege	Authorization	No continuous patch management

5. Discussion and conclusion

The framework and approach presented in this paper show a way to handle cyber-security pragmatically without having profound knowledge or expertise. Therefore, this paper serves as a guide especially for SMEs when facing challenges with cyber-security. Besides numerous other activities, the mentioned approach is an important and necessary step towards SME-specific cyber-security management.

However, as cyber-security is placed in a continuously changing environment, the management of it and the presented method have to be further developed and continuously improved over time. Taking this into account, the method serves as a frame for structuring and handling the topic. Its characteristic of a low threshold, pragmatism, and cost-efficient management address several challenges, but of course does not claim to be complete in a first draft. We consider further activities to be initiated, especially regarding the importance of vulnerabilities concerning the possible risk and its allocation within the model.

References

[1] Schuh, G., 2016. Industrie 4.0 - A Paradigm Shift, in: Haag, C., Niechoj, T. (Eds.), Digital manufacturing. Prospects and challenges, [1. Ed.] ed. Metropolis-Verlag, Marburg, pp. 7–10.

[2] IIC, 2016. Industrial Internet of Things Volume G4: Security Framework. IIC:PUB:G4:V1.0:PB:20160926.

[3] MBMF, 2020. Karliczek: Digitalisierung sicher vorantreiben und technologische Souveränität stärken. Presseportal.de, November 6.

[4] Heidt, M., Gerlach, J.P., Buxmann, P., 2019. Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments. Inf Syst Front 21 (6), 1285–1305.

[5] BSI, 2008. BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise, Bonn.

[6] Manso, C.G., Rekleitis, E., Papazafeiropolous, F., Maritsas, V., 2015. Information security and privacy standards for SMEs: Recommendations.

[7] Ehrlich, M., Wisniewski, L., Trsek, H., Jasperneite, J., 2018. Modelling and automatic mapping of cyber security requirements for industrial applications, in: WFCS 2018. 2018 14th IEEE International Workshop on Factory Communication Systems (WFCS), Imperia. 6/13/2018 - 6/15/2018. IEEE, Piscataway, NJ, pp. 1–9.

[8] Bundesamt für Sicherheit in der Informationstechnik (BSI), 2008. BSI-Standard 100-1: Managementsysteme für Informationssicherheit (ISMS), Bonn.

[9] DIN 91345, 2016. DIN SPEC 91345:2016-04: Referenzarchitekturmodell Industrie 4.0 (RAMI4.0). Beuth Verlag GmbH, Berlin. doi:10.31030/2436156.

[10] Heidrich, M., Leo, J.J., 2016. Industrial Internet of Things: Referenzarchitektur für die Kommunikation. FraunhoferInstiut für Eingebettete Systeme und Kommunikationstechnik ESK.

[11] Shostack, A., 2014. Threat modeling: Designing for security. Wiley, Indianapolis, 590 pp.

[12] Empl, P., Pernul, G., 2021. A flexible Security Analytics Service for the Industrial IoT, in: The Default Password Threat. Virtual, USA. SAT-CPS ´21, ACM, New York, NY, USA. 28. April 2021.

[13] Ahamed, J., Rajan, A.V., 2016. Internet of Things (IoT): Application systems and security vulnerabilities, in: 2016 5th International Conference on Electronic Devices, Systems and Applications (ICEDSA). December 6-8, 2016. IEEE, [Piscataway, NJ], pp. 1–5.

[14] Mozzaquattro, B.A., Agosthino, C., Goncalves, D., et al, 2018. An Ontology-Based Cybersecurity Framework for the Internet of things.

[15] Syed, R., 2020. Cybersecurity vulnerability management: A conceptual ontology and cyber intelligence alert system. Information & Management 57 (6), 1–17.

[16] DeSmit, Z., Elhabashy, A.E., Wells, L.J., Camelio, J.A., 2017. An approach to cyber-physical vulnerability assessment for manufacturing systems. Journal of Manufacturing Systems 43, 339–351.

[17] Hutchins, M.J., Bhinge, R., Micali, M.K., Robinson, S.L., Sutherland, J.W., Dornfeld, D., 2015. Framework for Identifying Cybersecurity Risks in Manufacturing. Procedia Manufacturing 1, 47–63.

[18] Wadhwa, M., 2021. A beginners guide to the STRIDE security threat model. https://www.ockam.io/learn/blog/introduction_to_STRIDE_security_model. Acc. 15 March 2021.

[19] CVE, 2021. Common Vulnerabilites and Exposusres. https://cve.mitre.org/. Accessed 15 March 2021.

[20] Mittal, S., Das, P.K., Mulwad, V., Joshi, A., Finin, T., 2016. CyberTwitter: Using Twitter to generate alerts for cybersecurity threats and vulnerabilities, in: . 2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM), San Francisco, CA, USA. 18.08.2016 - 21.08.2016. IEEE, pp. 860–867.

[21] ISACA, 2017. Implementation Guideline ISO/IEC 27001:2013: A practical guideline for implementing an ISMS in accordance with the international standard ISO/IEC 27001:2013.

[22] SBS. SME guide for the implementation of ISO/IEC 27001 on information security management. Small Business Standards.

[23] AUTONOMIK Industrie 4.0, 2016. Softwarearchitekturen für Industrie 4.0: RAMI und IIRA aus Sicht der projekte im Technologieprogramm AUTONOMIK für Industrie 4.0. VDI/VDE Institut für Innovation und Technik.

[24] Alshboul, Y., Streff, K., 2015. Analyzing Information Security Model for Small-Medium Sized Businesses, in: 21st Americas Conference on Information Systems (AMCIS 2015). Fajardo, Puerto Rico, 13-15 August 2015. Association for Information Systems, Atlanta, Georgia, pp. 1–9.

[25] Kamal, M., 2019. ICS Layered Threat Modeling. Information Security Reading Room.

[26] Zachman, J.A., 2008. The Concise Definition of The Zachman Framework. zachman.com/16-zachman/the-zachman-framework/35-the-concise-definition. Acc. 17 March 2021.

[27] Fraunhofer ESK, 2016. Industrial Internet of Things: Referenzarchitektur für die Kommunikation.

[28] Zimmermann, S., 2019. Menschliches Fehlverhalten und Sabotage sind die größten Bedrohungen: VDMA Industrial Security. https://industrialsecurity.vdma.org/viewer/-/v2article/render/37164217. Accessed 17 March 2021.

[29] CSA, 2017. Security-by-Design Framework. Version 1.0.

[30] Fraunholz, D., Krohmer, D., Anton, S.D., Dieter Schotten, H. (Eds.), 2017. Investigation of Cyber Crime Conducted by Abusing Weak or Default Passwords with a Medium Interaction Honeypot, 7 pp.

Biography

Prof. Dr.-Ing. Dipl.-Wirt. Ing Günther Schuh is the director of the Institute for Industrial Management (FIR) at RWTH Aachen University. He is also head of the chair of production systems and a member of the directorate of the Laboratory for Machine Tools and Production Engineering (WZL) at RWTH Aachen University as well as if the Fraunhofer Institute for Production Technology IPT in Aachen. His research findings include relevant methods and instruments for complexity management, resource-oriented process cost accounting, and participative change management, as well as the concept of the virtual factory.

Jacques Engländer, M. Sc. RWTH has been working as a project manager at FIR at RWTH Aachen University since 2018. In his current position as part of the Information Management division, he supports companies in the design of IT strategies and information security management concerning organizational, technical, and cultural aspects.

Lars Kaminski, M. Sc. started working as a project manager at FIR at RWTH Aachen University in 2019. In his current position within the technical group IT complexity management, he specialized in IT architecture management and the design of transformation strategies for information security.

Dr. Jan Hicking has been head of the division Information Management at FIR at RWTH Aachen University since 2020. Starting in 2017, he received his Ph.D. in 2020 within the field of intelligent products. As head of the division, he is responsible for multifaceted consulting and research projects.

Martin Bülskämper, B. Sc. RWTH has been a research student assistant at FIR at RWTH Aachen University since 2020. As an automation engineer, he combines technical expertise with management aspects such as the management of information security and thus helps manufacturing companies to successfully manage digital transformation projects.