Business Research (2019) 12:523–558
https://doi.org/10.1007/s40685-018-0071-5

ORIGINAL RESEARCH

Assessing IT availability risks in smart factory networks

Björn Häckel[1,2] · Florian Hänsch[3] · Michael Hertel[4] · Jochen Übelhör[2,5]

Received: 23 September 2017 / Accepted: 16 August 2018 / Published online: 25 August 2018

Abstract Emerging smart manufacturing technologies combine physical production networks with digital IT systems, resulting in complex smart factory networks, which are especially vulnerable to IT security risks, such as IT component non-availabilities. Companies must employ extensive IT security measures to secure their production facilities. However, complex network structures and inherent dependencies of smart factory networks complicate corresponding investment decisions and increase the need for appropriate decision support. We develop a risk assessment model that supports companies in the investment decision-making process regarding IT security measures by identifying and evaluating the most critical areas of the information network while considering the underlying production network. For this purpose, IT availability risks are quantified by means of graph theory, matrix notation, and value-at-risk. Our model provides a structured approach and considers network structures and interdependencies. The insights gained by our model present a profound economic basis for investment decisions on IT security measures. By applying our model in an exemplary real-world setting, we analyze various IT security measures and their risk reduction effect.

✉ Jochen Übelhör
jochen.uebelhoer@fim-rc.de

[1] University of Applied Sciences Augsburg, Friedberger Straße 2a, 86161 Augsburg, Germany

[2] Project Group Business and Information Systems Engineering of the Fraunhofer FIT, Augsburg, Germany

[3] Finalix Business Consulting, Baarerstrasse 110A, 6300 Zug, Switzerland

[4] BMW Financial Services, Heidemannstraße 164, 80939 Munich, Germany

[5] FIM Research Center, University of Augsburg, Universitätsstraße 12, 86159 Augsburg, Germany

Keywords Smart factory · Risk assessment · IT availability risks · Risk quantification · Network structure analysis · Investment decision support

1 Introduction

Technological trends, such as the *Internet of Things* (IoT), *cyber-physical systems* (CPS), and other smart manufacturing technologies turn conventional production facilities into so-called *smart factories* (Lasi et al. 2014). There, CPS enable machinery and products to control and monitor production processes collaboratively and to optimize themselves and the production processes (Yoon et al. 2012; Schuh et al. 2014; Hessman 2013). Suppliers, customers, and vendors are increasingly integrated into the production infrastructure, resulting in IT-dependent, intercompany *smart factory networks*, with complex interdependencies. Thereby, the connection of physical production and digital information enables the flexible production of individualized goods, while simultaneously increasing efficiency (Radziwon et al. 2014). Besides manifold potential benefits, a number of new risks arise in smart factory networks. For instance, the digital transformation of production facilities bears considerable investment risks considering the substantial investment volumes that are often required. At the same time, technological risks arise due to the fast development cycles of digital technologies. Given the coordinative role of humans in complex production processes, the importance of humans as a possible source of error for operational risks but also as an object to be protected in the context of safety is also increasing (Hertel 2015). This is accompanied by the increasing complexity of the overall socio-economic system of the smart factory network, which increases the criticality of random and negligent errors and disturbances (Tupa et al. 2017; Geisberger and Broy 2015). Besides these general risks, especially IT security risks are of central importance as smart factory networks rely on communication and real-time information synchronization and, thus, depend on the underlying IT systems, which are mandatory for the reliable operation of the production infrastructure (Zuehlke 2010; Yoon et al. 2012; Tupa et al. 2017). Therefore, smart factory networks are concurrently increasingly vulnerable to IT security risks as they are no longer isolated and closed systems (Yoon et al. 2012; Smith et al. 2007; Tupa et al. 2017). Besides other dimensions of IT security risks including access, accuracy, or accountability, this involves especially IT availability risks. These are becoming one of the most critical threats for companies, as non-availabilities of IT systems significantly hamper the reliable operation of dependent production components, and eventually cause their complete failure (Amiri et al. 2014). Although many companies are extensively engaged in digital transformation, the associated risks are often underestimated or not considered. However, this is of utmost importance as the consequences of IT availability risks in form of business interruptions might lead to considerable damage potentials. These damage potentials are increased by just-in-time and just-in-sequence production principles and ultimately result in severe monetary losses. This especially holds true for highly integrated, interdependent supply networks in which the failure of one company can cause interruptions in the entire supply

network. Accordingly, companies must assign considerable investment volumes to IT security measures to secure their production facilities against IT availability risks and to prevent economic harm. However, the variety of potential measures, the increasing complexity of smart factory networks, and especially the inherent dependency structures significantly complicate the identification of the most critical areas of IT systems with regard to potential threat scenarios. Thus, companies require well-founded approaches that support a comprehensive assessment of IT availability risks and, based on that, enable well thought out investment decisions regarding IT security measures in the course of their IT security strategy.

Due to the outlined complex interdependencies in smart factory networks, a corresponding risk assessment model for IT availability risks must consider—besides specific characteristics of smart factory networks—that non-availability of IT systems interrupts the operation of the dependent production infrastructure (Lee 2008; Lucke et al. 2008; Zuehlke 2010). Additionally, increasing interconnectedness contributes to this increased vulnerability as local failures causing non-availabilities of IT systems can lead to disruptions in the entire value network (Amin et al. 2013; Hallikas et al. 2004). Local failures include, amongst others, simple technical failures, incorrect capacity planning, human errors, natural disasters, or intentional attacks on IT systems. For example, targeted denial-of-service attacks can cause a non-availability of IT components, affecting the functionality of the production network and reducing its productivity (Lucke et al. 2008; Zuehlke 2010; Amin et al. 2013). Numerous examples illustrate this threat potential. First, the German Federal Office for Information Security (abbreviated as BSI) mentions in its status report on information security that hackers attacked a steel plant by intruding its office network. After advancing into the production control network and attacking the control components of the blast furnace, the blast furnace was left in an "undefined status" and could not be shut down in a controlled manner. As a result, the blast furnace and other parts of the plant were severely damaged (BSI 2014). This illustrates that due to ongoing interconnectedness, investments in IT security measures are of critical significance, even in traditional production facilities. Another example is the Stuxnet worm attack in 2010, which targeted industrial control systems in high-security infrastructures, such as atomic plants. The Stuxnet incident revealed that the interconnectedness of applications presents a serious security issue and demonstrated that even the control system's disconnection from the Internet as well as personal access restrictions are insufficient as protection for industrial control systems (Karnouskos 2011). Considering these threat scenarios, companies must employ IT security measures to secure their CPS infrastructure against IT availability risks. Appropriate IT security measures include, but are not limited to, redundancies through backup components, industrial hardware with integrated IT security mechanisms, intrusion detection systems, or appropriate service-level agreements (Byres and Lowe 2004; Cardenas et al. 2008; Yadav and Dong 2014; Zambon et al. 2007).

Given the variety of potential IT security measures, in combination with limited personal and financial resources, the corresponding investment decisions regarding IT security measures must be based on a profound economic basis, considering costs, benefits, and risk aspects (Cavusoglu et al. 2004; Gordon et al. 2003; Huang

2010). For this, the most critical areas of a smart factory network's IT system must be identified and evaluated with a structured approach, to invest available funds in the most effective way (i.e., reducing IT availability risks to the best possible extent). Thereby, an analysis must consider the diverse, complex network structures and dependencies between the physical production world and the digital IT systems of the smart factory network. To support companies in their corresponding decision processes, we develop a structured approach for the identification and evaluation of a smart factory network's most critical areas regarding IT availability risks and formulate the following two research questions:

RQ1 How can a smart factory network, consisting of dependent and connected production components and IT systems, be modeled and formalized?

RQ2 How can IT availability risks of IT systems in a smart factory network be quantified to identify the most critical nodes?

To answer these research questions, we first model and formalize the smart factory networks' general setting by means of graph theory and matrix notation. Then, we quantify IT availability risks by applying the risk measure Value at Risk (VaR). While there are a few multi-criteria decision-making approaches that try to integrate interdependencies, causes, and effect relations like the DANP approach of Ramkumar and Jenamani (2015) for the assessment of sustainability induced in supply chains by e-procurement, approaches are missing that consider a monetary financial perspective, analyze root causes and damage potentials, and transfer these to a monetary basis. Against this backdrop, our approach focusses on the root causes of damage and the resulting propagation effects within smart factory networks and uses VaR as a suitable risk measure, which indicates damage with a confidence level, to condense the effects and, thus, provide a monetary valuation that is suitable for management practice due to the wide spread and acceptance of VaR as a standard risk measure. In particular, our approach allows for analyzing the damaging effects that result from failures of single IT components by taking into account the manifold and complex interdependencies in smart factory networks. By means of this, it enables companies to identify the most critical IT components and to derive a solid design of their smart factory information network. Further, our results demonstrate that the criticality of an IT component is determined by numerous factors that have to be considered in the risk assessment. Accordingly, our approach addresses a relevant real-world problem and contributes to literature and practice as it enables a structured analysis of increasingly complex smart factory networks under consideration of not only direct but also indirect dependencies among the components of the smart factory network, propagation effects and the resulting damages. Key findings and contributions include:

- We find that the complex network structures and direct and indirect dependency relationships have a considerable influence on the effects of IT availability risks. Thus, a targeted degree of interconnectedness and a solid design of the smart factory network is crucial for IT security.
- Various influencing factors such as dependency relationships to other components, the degree of productivity interference on the production process, affected

process steps, respective damage potentials, utilization of production components, and compensation effects influence the criticality of IT components and have to be considered.
- Due to the large number of possible IT security measures, these must be assessed in an economically sound manner, taking into account the cost–benefit aspect and its effect on the overall system. For this, our structured approach helps to assess risks associated with the ever increasing interconnection within smart factories, to assess where interconnections and dependencies should be deliberately avoided and where redundancies should be deliberately created, e.g., by means of backup servers or cloud-based modules.
- Insights gained by our approach provide practitioners with a risk assessment tool that supports companies with risk-oriented guidance regarding a solid design of their smart factory and identifies the most critical IT components for the derivation of an appropriate IT security strategy.

The remainder of our paper is organized as follows: Sect. 2 provides an overview of the theoretical background. In Sect. 3, we outline the basic idea and develop a risk assessment model to address our research questions. In Sect. 4, we demonstrate the applicability of the developed risk assessment model by analyzing an exemplary real-world scenario and conducting sensitivity analyses. Finally, Sect. 5 provides managerial implications before Sect. 6 presents a conclusion, and denotes limitations and an outlook on further research.

2 Theoretical background and research methodology

Subsequently, we provide a comprehensive overview of the theoretical background and our research methodology. First, we discuss scientific and application-oriented literature regarding smart factory networks, and specify the associated role of IT systems. Then, we substantiate the significance of related IT availability risks, and define central requirements for an adequate risk assessment approach regarding IT availability risks in smart factory networks. Second, we examine the corresponding literature, and carve out the research gap. And third, we outline the methodological approach applied to address this research gap.

2.1 Smart factory networks and corresponding IT availability risks

Given the advancements of smart manufacturing technologies and the innovative nature of smart factory networks, scientific literature is constantly evolving and contains a diverse body of literature (e.g., see Haller et al. 2009; Iansiti and Lakhani 2014; Turber and Smiela 2014; Strozzi et al. 2017). Further, there are numerous studies and application-oriented examples of research institutes exploring and describing the implementation of smart manufacturing technologies (e.g., see Hessman 2013; Lucke et al. 2008; Radziwon et al. 2014; Yoon et al. 2012; Zuehlke 2010; Shariatzadeh et al. 2016; Zhong et al. 2017). In corporate practice, we can observe that IoT-based technological solutions such as radio frequency

identification (RFID) are widely implemented enabling, for example, the real-time acquisition of data and the real-time monitoring of objects within production processes (Lucke et al. 2008; Fleisch and Thiesse 2007; Zhong et al. 2017). However, the comprehensive and holistic implementation of smart manufacturing technologies in production facilities serving as test beds remains object to laboratory research facilities, such as *SmartFactory*^{KL}, or pilot facilities, such as the *Siemens Electronic Works Facility* or the *WITTENSTEIN bastian' Production Facility* (Hessman 2013; Zuehlke 2010; Schlick et al. 2014). This was also found in a dynamic literature review performed by Strozzi et al. (2017). To structure the diverse body of literature on smart factories, they performed a combination of systemic literature review and bibliographic network analysis. Thereby, they revealed that the biggest literature stream focusses on RFID technology and agent-based intelligent decision support system architecture, both aspects concerning monitoring and scheduling of production processes. Further, they found that research focusses on "models, frameworks, and architectures related to the implementation of the Smart Factory […], along with high-level 'landscape' analyses." A recent example of such research is the work of Jung et al. (2017), in which a reference factory design and improvement activity model is introduced for designing new and improving existing factories. The model highlights interrelationships of implemented technologies and provides an indication for further improvements through sensors, software tools, or gathered data. Another finding of the study by Strozzi et al. (2017) is that research focuses more on topics related to the development and adoption of software tools and cloud applications instead of topics related to the adoption of new technologies in manufacturing processes. For instance, Shariatzadeh et al. (2016) develop an IoT platform-based system architecture and a generic framework for communication interfaces between the digital factory and the smart factory. Other researchers address the potential of the digital twin concept in regard to near-real time data acquisition and analysis (e.g., see Uhlemann et al. 2017; Borodulin et al. 2017; Qi and Fao 2018). In summary, it can be concluded that scientific contributions "propose conceptual works and experiments, and rarely actual test-beds and lessons learned from the practice are described and discussed" (Strozzi et al. 2017).

Another shortcoming of the current literature is the lack of a common definition of the term *smart factory*, although widely used in both scientific literature and practice (Radziwon et al. 2014). Based on a collection of different definitions, Radziwon et al. (2014) define the smart factory as a "manufacturing solution that provides such flexible and adaptive production processes that will solve problems arising on a production facility […]." Hermann et al. (2015) define the smart factory as a "factory where CPS communicate over the IoT and assist people and machines in the execution of their tasks". They further describe, that "within the modular structured Smart Factories […], CPS monitor physical processes, create a virtual copy of the physical world and make decentralized decisions". Based on *SmartFactory*^{KL} and adopting the idea of IoT, Zuehlke (2010) describes that a "factory-of-things will be composed of smart objects which interact based on semantic services." Yoon et al. (2012) describe a smart factory as a "factory system in which autonomous and sustainable production takes place". And Lucke et al.

(2008) envision the smart factory as a "real-time, context-sensitive manufacturing environment that can handle turbulences in production using decentralized information and communication structures for an optimum of production processes."

These definitions reflect the specific characteristics of smart factory networks, such as their modular design, which enables functionalities like flexibility, reconfigurability, and adaptability (Brettel et al. 2014; Radziwon et al. 2014; Zuehlke 2010). These functionalities enable smart factory networks to respond to circumstances and turbulences in the real-time production, such as the non-availability of single production components (Lucke et al. 2008). Further, smart factory networks attempt to offer increased productivity, optimized processes, improved capacity utilization, and reduced lead times, as well as enhanced energy and resource efficiency (Brettel et al. 2014; Chui et al. 2010; Radziwon et al. 2014; Schuh et al. 2014; Yoon et al. 2012; Shrouf et al. 2014). These benefits contribute to the ability to produce highly individualized products in low batch sizes in a considerably short time-to-market, at costs comparable to those of mass production (Lasi et al. 2014). This is of central importance for future competitiveness in all manufacturing industries, as customer expectations shift toward mass customization, shorter innovation cycles, and customer participation models (Lasi et al. 2014; Yoon et al. 2012; Iansiti and Lakhani 2014; Turber and Smiela 2014).

The characteristics of smart factory networks are facilitated through concepts such as IoT and production-oriented CPSs, which involve *smart objects,* such as intelligent machinery and products. CPS integrate computing and communication capabilities in physical production processes to combine the cyber and physical world (Lee et al. 2015; Wang et al. 2016). Smart objects are connected over the Internet, or other network infrastructures, to form dynamic, intelligent, and self-controlling networks (Broy et al. 2012; Schuh et al. 2014). Within these networks, smart objects control and monitor the production process collaboratively through machine-to-machine communication and exchange information to optimize themselves and the production process (Brettel et al. 2014; Hessman 2013; Schuh et al. 2014; Yoon et al. 2012). Hence, smart objects represent elementary components of the collaborative production infrastructure (Zuehlke 2010; Yoon et al. 2012). Although smart objects control and optimize themselves autonomously on a workflow level, central IT systems are required for an overarching planning and coordination of decentralized smart objects. For example, central IT systems must provide parameters and framework conditions to define a possible course of action for the autonomous control and optimization of smart objects (Schuh et al. 2014). These IT systems are connected with other internal and external networks to facilitate information exchange and collaboration within the supply network. The necessary infrastructure is typically company specific and can be on-premise, cloud-based, or a hybrid form of both (Zuehlke 2010; Yoon et al. 2012; Karnouskos and Colombo 2011; Colombo et al. 2013; Shrouf et al. 2014; Haller et al. 2009).

Due to the high level of interconnectedness between production and IT components, the operation of the physical production process depends on the flawless operation of IT services. Consequently, smart factory networks face new IT security threats that concern the four dimensions of IT security risks *availability*,

access, *accuracy*, and *accountability* (Westerman and Hunter 2009). Thereby, the threats stem from four channels: (1) software bugs and hardware malfunctions, (2) open Internet protocols and shared networks, (3) the numerous parties involved, and (4) a large number of field devices that can be accessed (Amin et al. 2013). IoT and smart manufacturing technologies change requirements on IT security (Wegner et al. 2017) and "the concept of Industry 4.0 generates new categories of risks […] because of the increase of vulnerabilities and threats" (Tupa et al. 2017). Tupa et al. (2017) argue that "the connection of cyber-space, sophisticated manufacturing of technologies and elements, and using outsourcing of services [are] the main factors increasing vulnerability" and that "the implementation of Industry 4.0 has shown that the connections between humans, systems and objects have become a more complex, dynamic and real-time optimized network". For instance, central components of an IT infrastructure like an on-premise server are no longer the only critical components of an information network. In fact, all components, including remote manufacturing equipment and internal and external sensors, become critical as "industrial control systems are becoming the target for malicious cyber intrusions" (Wegner et al. 2017). Further, SCADA systems, that control manufacturing processes, were initially designed to operate on closed networks. With IoT applications, SCADA systems are increasingly based on cloud technology resulting in increased interconnectivity and, ultimately, vulnerability (Eden et al. Eden 2017). Therefore, "the challenge to maintain availability will increase as manufacturing evolves from a centralized system supported by external suppliers to a distributed system in which production occurs closer to the point of use" stretching potential points of failure (Wegner et al. 2017).

Given this increasing dependency of the production infrastructure on the reliable functioning of the IT services and the real-time constraint of smart factory networks, especially non-availabilities, that is, the non-usability of an on-demand service, is becoming one of the most critical threats in smart factory networks (Amiri et al. 2014; Cardenas et al. 2008; Lee 2008). Non-availabilities can be caused by events including intentional attacks, such as denial-of-service attacks, simple human errors, random technical failures, or incorrect capacity planning (Amin et al. 2013). Further, the smart factory's interconnectivity and IT-based integration with its supply network, aside from the benefits incurred through improved collaboration, increase IT availability risks because former protective barriers are at least partially removed and the amount of potential entry points increases (Eden et al. 2017; Smith et al. 2007). For example, modern industrial control systems are connected to office networks and external systems for information exchange, and are no longer isolated through *air gaps* (Byres 2013). A study by Byres and Lowe (2004) emphasizes this increased vulnerability and reveals that security incidents increasingly stem from external sources (70%), compared to internal sources (30%). They mention the increasing interconnection of critical systems and resulting interdependencies as a reason for this development, among others. In combination with the highly interconnected information network of a smart factory, a non-availability of one component can spread in the entire network resulting in cascading failures (Amin et al. 2013). These reinforce the initial failure and can lead to the loss of the operational capability of the entire smart factory network (Danziger et al. 2016).

Consequently, IT availability risks play a major role in smart factory networks, and companies must apply corresponding IT security measures.

In this context, comprehensive IT availability risk management in smart factory networks requires economically profound analyses, and a structured, methodological approach to identify and quantify existing IT availability risks and to lay the ground for corresponding IT security investments. For this purpose, the most critical components of the IT system must be identified based on the effects of a component's non-availability on the production process. An adequate risk assessment approach must take account of smart factory networks' specific characteristics. Thereby, the modeling of corresponding dependency structures represents an essential requirement for the analysis of resulting cascade failures in the production process. Thus, we formulate the following requirements for an appropriate risk assessment approach for smart factory networks, which is able to support investment decisions regarding IT security measures: (R1) the network structures of the IT system, including dependencies between IT components, must be considered. (R2) The production system's interdependencies and network structures must be considered. (R3) Losses in the production process caused by IT non-availabilities must be quantified and assigned to responsible IT components, while considering the production infrastructure's dependencies on the IT system.

2.2 Approaches regarding the assessment of IT availability risks

Risk assessment is an elementary step within the risk management cycle that can be structured along the four phases of (1) identification, (2) assessment, (3) control, and (4) monitoring (Hallikas et al. 2004; Harland et al. 2003). The goal of risk assessment is to identify and evaluate risks in order to decide on appropriate security measures. For this, companies engaged in smart factory networks require appropriate structured approaches for the evaluation of IT availability risks that fulfill the stated requirements R1–R3 due to the aforementioned, specific challenges of smart factory networks (Tupa et al. 2017). For risk assessment within information systems, there exist a magnitude of different approaches within the literature. While some suggest frameworks and approaches for information systems in general, others place a special focus on the characteristics of their respective application field as vulnerabilities and accompanying losses are highly specific, due to characteristics such as IT architecture, or business operations' varying dependencies on IT services.

Based on a structured review of 125 risk assessment approaches for information systems, Shameli-Sendi et al. (2016) develop a taxonomy that structures risk assessment approaches along the four categories *appraisement*, *perspective*, *resource valuation*, and *risk measurement*. Thereby, *appraisement* differentiates risk assessment approaches from a methodological perspective into *quantitative*, *qualitative*, and *hybrid* approaches (Shameli-Sendi et al. 2016). Quantitative methods deploy mathematical functions, objective measurements, and quantitative data to evaluate risk (Karabacak and Sogukpinar 2005; Suh and Han 2003; Sun et al. 2006). For example, the risk assessment framework developed by Jaisingh and Rees (2001) uses the quantitative risk measure VaR to assess IT security risks. The

derived information can then be used to analyze the relationship between the cost of security measures and the risk reduction effects achieved. Niesen et al. (2016) develop a conceptual framework for data-driven risk assessment based on real-time operational data that becomes available in smart factory environments. By means of their approach, live monitoring of different types of risk becomes feasible. However, their approach does not allow the consideration of specific types of IT related threats, especially availability risks, as appropriate data and relevant indicators are missing. This shows that quantitative approaches often face a lack of necessary detailed data. Further, disadvantages include time-consuming and expensive calculation processes, the complex implementation in practice, and the difficult interpretation of results (Shameli-Sendi et al. 2016). In contrary, qualitative methods use descriptive variables to evaluate the likelihood of occurrence, and the impact of IT non-availability (Caralli et al. 2007; Aagedal et al. 2002). As they do not rely on accurate historical data and are much easier to understand and implement in contrast to quantitative methods, they are widely used in practice (Shameli-Sendi et al. 2016). For instance, Silva et al. (2014) develop a multi-dimensional risk management model based on Failure Mode and Effect Analysis (FMEA) and fuzzy theory that analyses five dimensions of information security risks: access to information and systems, communication security, infrastructure (hardware and networks), security management, and secure information systems development. Thereby, FMEA provides a structured approach for assessing failure modes according to three risk factors occurrence, severity, and detection that are assessed by expert estimations. The derived results provide information regarding the criticality of the investigated failures that produce vulnerabilities to the company's information system. Eom et al. (2007) develop a risk assessment approach for the evaluation of assets regarding their degree of contribution to related business processes. For this, they apply with Delphi teams a qualitative risk analysis methods. Besides the merits of qualitative approaches, shortfalls are that they often lack measurable detail and monetary results to support investment decision making considering cost-efficiency and that results are often times subjective and prone to errors and imprecision (Shameli-Sendi et al. 2016). To overcome the weaknesses of sole quantitative or qualitative approaches, there are hybrid methods combining both types to enable a simple and fast qualitative assessment as well as detailed quantitative analysis for more critical aspects (Yadav and Dong 2014; Rainer et al. 1991; Shameli-Sendi et al. 2016). For example, the initial quantitative risk assessment method developed by Zambon et al. (2007) considers the IT architecture and dependencies between IT constituents, based on a time-dependent model for business processes. Based on this, they extend their model to a qualitative model for the analysis of availability risks in IT architectures, requiring only commonly available input data (Zambon et al. 2011).

Another category for risk assessment approaches introduced by Shameli-Sendi et al. (2016) is *risk measurement* that differentiates approaches into the two types *non-propagated* and *propagated*. While approaches of the *non-propagated* type neglect the propagation of an attack impact on dependent nodes, risk assessment approaches of the *propagated* type consider impact propagation in networks to obtain a more precise picture of damage potential (Shameli-Sendi et al. 2016).

Regarding non-propagated types, Zhong et al. (2017) develop a quantitative approach based on RFID and laser scanners to visualize the manufacturing environment for the real-time observation of production and detection of risks and disturbances. Although their model enables real-time monitoring, it does not allow to analyze the causes of occurring failure propagation and, thus, lacks the possibility to analyze dependency structures. Further, it lacks the possibility to quantify the resulting damages from occurring failures and disturbances within the production process. In contrast, there are some approaches that consider propagation effects within information systems. For instance, Fenz et al. (2011) develop a software-based risk management methodology that supports investment decision making while considering the business criticality of information assets based on their involvement in business processes. Ackermann and Buxmann (2010) develop a risk assessment model for IT-based service networks that supports IT security investment decisions. This model quantifies IT security risks in relation to different IT security measures, and considers dependencies between different services of the network (i.e., transferred data). Finally, Papa et al. (2011) develop a qualitative risk assessment model for Supervisory Control and Data Acquisition (SCADA) embedded systems, focusing on availability risks. Their model calculates corresponding risk scores for each SCADA element, considers effects for the entire system, and determines protection measures to reduce risk. Despite these examples, Shameli-Sendi et al. (2016) state that there are only few risk assessment approaches that consider propagation effects, although these are essential to assess the entire damage potential caused by attacks and errors in complex network environments to provide a profound basis for economically sound investment decisions.

Further, there is no assessment approach, thus far and to the best of our knowledge, for IT availability risks in smart factory networks, that is, no existing approach that considers the specific characteristics of smart factory networks and consequently fulfills the stated requirements R1–R3. However, the consideration of network structures including dependencies between IT components and the production system's interdependencies and network structures, as well as the transfer of damage potentials to a monetary valuation represent a necessary step in the course of an appropriate risk assessment within smart factory networks. Such an approach is necessary to support organizations with risk-oriented guidance in deducing reasonable investment strategies with regard to IT security measures. As the modeling of dependency structures under consideration of propagation effects represents an essential requirement in this endeavor, we aim to address this research gap in the following section by developing a first approach based on graph theory and matrix notation. We chose graph theory and matrix notation as these are widely used and easily comprehensible methods to depict network structures and complex dependency relations and allow the consideration of characteristics of smart factory networks. Further, we apply VaR as an accepted and widely used standard risk measure to quantify damage potentials with a confidence level and to provide a monetary valuation that is suitable for management practice.

2.3 Research approach and applied concepts

To answer the research questions raised in Sect. 1, under consideration of the requirements set forth in Sect. 2.1, we develop a structured approach for an appropriate assessment of IT availability risks in smart factory networks. This approach uses graph theory and matrix notation methods, as they are widely utilized methods for formalized representation and the analysis of complex and interdependent networks. For example, Wagner and Neshat (2010), Faisal et al. (2006), and Buldyrev et al. (2010) use graph theory and matrix notation to analyze risk in supply chains and critical infrastructures regarding vulnerability, risk mitigation, and cascading failures in interdependent networks. Graph theory enables a relatively simple and transparent application of our approach. These are two important characteristics, since our model represents a first approach that should be easy to use and should have a certain degree of scalability. Besides graph theory, there are other approaches for the formalized representation of networks such as petri nets or system dynamics if other priorities are to be set, for example, if the analyses should be more detailed or more detailed stochastics (e.g., stochastic recovery times) should be used (e.g., Arns et al. 2002; Wu et al. 2007; Fridgen et al. 2014). However, in our opinion, graph theory seems to be an appropriate method for a first attempt, especially for reasons of transparency and complexity reduction. Further, we apply the risk measure VaR for the quantification of IT availability risks, as it is a widely utilized risk measure for downside risks.

To develop and analyze our model, we use the research paradigm introduced by Meredith et al. (1989). This approach structures research into a "continuous, repetitive cycle of description, explanation, and testing." By going through these stages in an iterative process, the description and explanation of an observable economic fact in a structured manner are possible. First, we formally describe cause-and-effect-relationships that determine the threat potential of an IT component (e.g., the basic structures and dependencies of smart factory networks). As new findings cannot always be derived from practical observations, we use a formal deductive modeling approach. Afterward, we discuss and explain the derived findings and give practical recommendations. An application in an exemplary real-world scenario indicates the utility of our risk assessment model as an appropriate and profound basis for decision support regarding IT security investments and serves as a starting point for its empirical validation. However, the testing of the findings shall be subject to future case study research.

3 Risk assessment model

Our risk assessment model considers relevant smart factory characteristics and identifies the most critical IT components of a smart factory's information network concerning IT availability risks by quantifying the corresponding threat potentials. In the following subsection, we describe the elementary steps of the model as shown in Fig. 1. The basic idea of our risk assessment model is to analyze the threat potential posed by the non-availability of an information network's IT component to

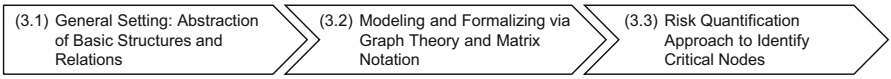

Fig. 1 Methodical procedure of the model development

the production network of a smart factory. This threat potential arises as the functionality and productivity of the production network depend on the reliable operation of the information network. In order to quantify the resulting threat potentials, we apply graph theory and matrix notation as well as VaR. The results gained by our model are of central importance to ensure a cost-efficient usage of usually scarce IT budget and to support companies' investment decisions since available funds for IT security measures must be invested in the most efficient way. First, we present an abstraction of the smart factory's general setting, including its basic structures and relations (Sect. 3.1). Based on this abstraction, we then describe our risk quantification algorithm. At this, we model and formalize the smart factory structure by means of graph theory and matrix notation (Sect. 3.2). Subsequently, the threat potential of each IT component is quantified (Sect. 3.3).

3.1 General setting

The basic structure of a smart factory consists of two connected networks: the production network and the information network, as illustrated in Fig. 2. First, there are different manufacturing machines in the production network performing various production procedures. These machines process products and are organized in process steps, whereby a certain process step contains machines with identical capabilities. Manufacturing machines are equipped with *embedded systems*, which consist of electronic hardware (e.g., a microchip) and a software component. The embedded systems enable the manufacturing machines to control themselves autonomously to a certain point, and to synchronize process information via the information network. Hence, we consider the embedded systems as parts of the *information network*. In addition to the embedded systems, the information network comprises further components performing various IT services crucial for the reliable operation of the smart factory. These IT services range from machine control and

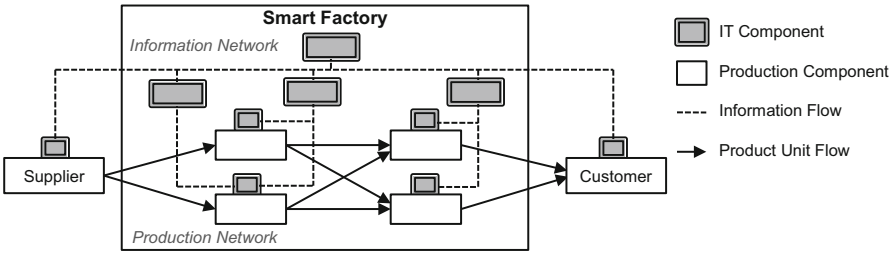

Fig. 2 Simplified structure of the smart factory

manufacturing execution, to enterprise level and machine communication applications. The different applications may be hosted on on-premise hardware or are obtained as cloud-based solutions. The respective IT infrastructure is also considered as an IT service.

As a result, a hierarchical structure emerges inducing *functional dependencies* between IT components. These functional dependencies exist *directly* between two IT components (e.g., applications depend on the server) or *indirectly* over at least one other IT component (e.g., an embedded system depends on the server over an application hosted on that server). A company may also include *redundancies* within the information network through backup components to secure certain IT services and to prevent single-point failures. If all IT services operate reliably, the manufacturing machines are able to coordinate themselves in a highly flexible and adaptive manner. This includes, for example, the adjustment of the product flow in the case of a manufacturing machine's non-availability. In addition to manufacturing components, there are suppliers vertically and horizontally integrated into the supply network, and customers receiving the completed products. Both are defined as parts of the production network due to their importance and because local interruptions affect the smart factory. Considering the integration of external partners into a smart factory's IT system, both suppliers and customers are connected through external data interfaces. Given the dependencies within and between these networks, a diverse and complex *dependency structure* emerges, in which the production components depend on several components of the information network for functionality. This dependency structure is of central relevance in our model, because it provides the basis for the quantification of the IT component's availability risks. Based thereupon, we analyze the consequences of an IT component's non-availability by deriving unprocessed units, which occur in a fixed time period. By analyzing the resulting risk values of all IT components, we are able to prioritize IT components in terms of their threat potential to the production network.

In the following subsection, we outline the algorithm and its assumptions (see Fig. 3) in more detail. First, we formalize and model the basic structures of the smart factory and its networks by means of graph theory and matrix notation. The resulting smart factory dependency structure lays the groundwork for the risk quantification based on VaR, which will be discussed in the subsection afterwards.

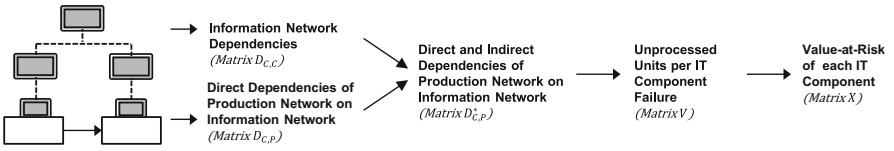

Fig. 3 Operational steps of the risk assessment algorithm

3.2 Modeling of the smart factory

In the following, we describe, model, and formalize the smart factory's two connected and dependent networks. Thereby, we elaborate on the underlying assumptions regarding the basic structures and characteristics of both networks, their components, and their connections and dependencies.[1]

Assumption 1 (A1) *The production network P consists of a finite set of smart production components* p_i *with* $i = 1, \ldots, m \in \mathbb{N}$ *(nodes) performing specific production procedures and a finite set of arcs (edges) connecting the production components.*

The smart production components p_i perform production procedures to process *product units* $u \in \mathbb{N}$ and are assigned to a *process step* l with $l = 1, \ldots, L \in \mathbb{N}$ in correspondence to their respective production task. The suppliers and customers are modeled to be a part of the production network and are also denoted as production components p_i. The capabilities of production components are identical within a process step l, but differ between process steps. Regardless of the process step, each production component p_i has a given *capacity* $q_i \in \mathbb{N}$ to process a given number of units u in the considered time period. In combination with current *capacity utilization* $qu_i \in \mathbb{N}$ of a production component, *idle capacity* $qi_i \in \mathbb{N}$ of a production component can be derived by Eq. (1):

$$qi_i = q_i - qu_i \quad \text{with} \quad qu_i \leq q_i. \tag{1}$$

If a process step l consists of more than one production component, product units can be flexibly routed to any of the assigned production components, under consideration of respective idle capacities. Therefore, utilization of the smart factory and individual production components are important factors determining the smart factory's flexibility and adaptability.

A2 *The information network C consists of a finite set of IT components* c_s *with* $s = 1, \ldots, k \in \mathbb{N}$ *and a finite set of arcs connecting the IT components.*

IT components c_s of the information network C perform various IT services s. Thereby, each IT service is provided by one IT component and may be backed up by a redundant IT component, denoted as $c_{s.2}$. Depending on the specific layout of the information network, different types of IT components can be included, such as hardware components, software modules, embedded systems, and external data interfaces. This flexibility enables the adaption of the algorithm to any information network layout (e.g., on-premise vs. cloud-based) without changing the algorithm's overall approach. Considering the layout and hierarchical structure of the information network and its IT services, there are direct functional dependencies between IT components, such as the dependency of an application on its host server. Binary *information network dependency matrix* $D_{C,C}$ defined by Eq. (2) represents all direct functional dependencies:

[1] The reader might find it helpful to reference to Fig. 4 while reading the following subsections to better comprehend the used notations.

$$D_{C,C} = \begin{bmatrix} d_{c_1,c_1} & \cdots & d_{c_1,c_k} \\ \vdots & \ddots & \vdots \\ d_{c_k,c_1} & \cdots & d_{c_k,c_k} \end{bmatrix}. \quad (2)$$

The numerical value of the binary variable $d_{c_s,c_s} \in \{0;1\}$ expresses whether there is a direct functional dependency between two IT components.

A3 *Production components depend either directly or indirectly on IT components in regard to functionality.*

As already described, the smart production components' ability to synchronize information via the information network C is an essential requirement for reliable functioning of the production network. The resulting *direct functional dependencies* of production components on IT components are expressed using the binary *direct functional dependency matrix* $D_{C,P}$, defined by Eq. (3):

$$D_{C,P} = \begin{bmatrix} d_{c_1,p_1} & \cdots & d_{c_1,p_m} \\ \vdots & \ddots & \vdots \\ d_{c_k,p_1} & \cdots & d_{c_k,p_m} \end{bmatrix}. \quad (3)$$

Thereby, binary variable d_{c_s,p_i} equals one for the dependency relationship between production components and their respective embedded systems, as the latter establishes the connection to the information network and is the interface between smart production components and digital information flow. For all other IT components, variable d_{c_s,p_i} equals zero, since production components are not directly connected with them. However, production components can still depend *indirectly* on those IT components, as IT services are unavailable if IT components providing those services are unavailable. This is due to the transitivity of IT component failures, meaning that, for example, the failure of a server affects production components through the triggered failure of a software application (Zambon et al. 2007). Further, existing *redundancies* in the information network must be considered, as redundant IT components prevent single-point failures of backed up components, thereby influencing the dependency structure of the smart factory (Cardenas et al. 2008). To consider both direct and indirect functional dependencies and redundancies in the information network, we apply a set of matrix calculations based on matrix algebra, which will be not explained in full detail, but be briefly described in the following.

First, we determine all direct and indirect functional dependencies within the information network by raising matrix $D_{C,C}$ to higher powers, according to the algorithm by Festinger et al. (1949), and combining the resulting matrices in the binary matrix $\bar{D}_{C,C}$. Multiplying matrix $\bar{D}_{C,C}$ with the *direct functional dependency matrix* $D_{C,P}$ delivers all indirect functional dependencies of production components on IT components (matrix $\bar{D}_{C,P}$). Adding the matrices $D_{C,P}$ and $\bar{D}_{C,P}$ results in the *direct and indirect functional dependency matrix* $\bar{\bar{D}}_{C,P}$, containing both the *direct* and *indirect* functional dependencies of production components on IT components. We now adjust matrix $\bar{\bar{D}}_{C,P}$ for possible redundancies based on the number of IT

components c_s available for the execution of an IT service s. In particular, if a production component depends on more than one IT component, the dependency is removed because the failure of a redundant IT component is backed up. First, we aggregate the available IT components of each IT service s in a binary matrix $Z_{S,C}$, and only the main IT components of each IT service s in matrix $\tilde{Z}_{S,C}$. Multiplying matrix $Z_{S,C}$ with matrix $\bar{\bar{D}}_{C,P}$ delivers matrix $\bar{Z}_{S,P}$, which represents the number of available IT components for each production component with regard to an IT service s. Subsequently, all values of $\bar{Z}_{S,P}$, which do not equal one, are set to zero. This results in the binary matrix $\bar{\bar{Z}}_{S,P}$ with all production components depending only on one IT component with regard to an IT service s. Lastly, we multiply matrix $\bar{\bar{Z}}_{S,P}$ with the transposed main IT component matrix $\dot{Z}_{C,S}$ to derive the *dependency matrix* $D^*_{C,P}$, as defined by Eq. (4). The resulting *dependency matrix* $D^*_{C,P}$ defined by Eq. (4) contains all direct and indirect functional dependencies of production components on IT components and considers redundancies in the information network. Thereby, the binary variable $d^*_{c_s,p_i} \in \{0;1\}$ equals one if there is a direct or indirect functional dependency; otherwise, $d^*_{c_s,p_i}$ equals zero:

$$D^*_{C,P} = \begin{bmatrix} d^*_{c_1,p_1} & \cdots & d^*_{c_1,p_m} \\ \vdots & \ddots & \vdots \\ d^*_{c_k,p_1} & \cdots & d^*_{c_k,p_m} \end{bmatrix}. \tag{4}$$

So far, *dependency matrix* $D^*_{C,P}$, as a central artifact of our algorithm and essential for the risk quantification approach, was derived considering the production network (A1), the information network (A2), and the functional dependencies between the two networks (A3). These steps lay the ground for the risk quantification approach, which identifies and evaluates critical IT components regarding IT availability risks.

3.3 Risk quantification approach

The risk quantification approach determines the unprocessed units caused by the non-availability of an IT component based on the smart factory's dependency structure. The resulting *VaR values* represent the central results of our model and enable the identification of the most critical IT components. The following section elaborates on the risk quantification approach and its assumptions in more detail.

A4 *The non-availability of an IT component restricts the productivity of dependent production components.*

As technical failures and attacks result in the non-availability of the affected IT component, we assume that an IT component fails completely and do not consider partial functionality interferences. Accordingly, a failing IT component c_s is not able to provide its IT service s and interferes dependent production components' productivities, leading to decreased production capacities. Thereby, we observe the consequences of an IT component's non-availability in a fixed time period and assume that the IT component failure occurs at the beginning of the considered

period and lasts until its end. The production components' interference differ for each IT component and can range from a partial capacity reduction, (e.g., through a restricted automation) to a complete failure. The interference degree of each IT component is expressed by the exogenous *interference degree variable* $\bar{r}_{c_s} \in \{0;1\}$ and is based on expert estimations. Applying an exogenous input parameter is a reasonable approach because experienced company experts can adequately assess the effects of an IT component's non-availability on its dependent production components based on their knowledge and expertise. Further, it would be possible to differentiate the interference degree of an IT component on a more detailed level for each production component. However, for reasons of simplicity, we break down the required data on a reasonable and manageable granularity level and assume that an IT component's interference degree is identical for all production components. Multiplying the values of the *dependency matrix* $D^*_{C,P}$ with $\bar{r}_{c_s}$ according to Eq. (5) derives the *interference variable* $r_{c_s,p_i} \in \{0;1\}$, expressing the degree of productivity reduction of a production component p_i, if an IT component c_s, fails:

$$r_{c_s,p_i} = \bar{r}_{c_s} * d^*_{c_s,p_i}. \tag{5}$$

If a productivity reduction occurs, $0 < r_{c_s,p_i} \leq 1$; otherwise, $r_{c_s,p_i} = 0$. If the reduced capacity is less than the utilization, that is, the interference cannot be absorbed by idle capacity, the productivity reduction causes *initially unprocessed units* v_{c_s,p_i} at the production component p_i, as calculated by Eq. (6):

$$v_{c_s,p_i} = \max\left(qu_i - q_i * \left(1 - r_{c_s,p_i}\right); 0\right). \tag{6}$$

A5 *Initially unprocessed units* v_{c_s,p_i}*, caused by the interference of an affected production component, can be (partially) compensated by other production components.*

The smart factory's ability to flexibly combine the production components in temporary production lines enables the compensation for initially unprocessed units v_{c_s,p_i}. However, the compensation is only possible if compensating production components possess the same production capabilities and, hence, belong to the same process step l as the affected production component. Further, compensating production components must have idle capacity left. The *compensable units* w_{c_s,p_i} provided by a compensating production component are calculated as described by Eq. (7):

$$w_{c_s,p_i} = \max\left(q_i * \left(1 - r_{c_s,p_i}\right) - qu_i; 0\right) \tag{7}$$

After deriving the initially unprocessed units and the compensable units on a production component level, we aggregate both values separately for each process step l. By subtracting the compensable units $w_{c_s,l}$ from the initially unprocessed units $\bar{v}_{c_s,l}$ on the process step level according to Eq. (8), the *unprocessed units* $v_{c_s,l}$ per process step l after the compensation effect can be derived:

$$v_{c_s,l} = \max\left(\bar{v}_{c_s,l} - w_{c_s,l}; 0\right) \tag{8}$$

A6 *Unprocessed units* $v_{c_s,l}$ *at a process step* l*, cause a continual production failure in following process steps due to the lack of workable units.*

As we assume that each unit of process step $l+1$ requires one unit from the preceding process step l, production failures are passed through all subsequent process steps. This production failure cycle continues until the last process step is reached. Further, the number of unprocessed units might increase in later process steps if the IT component's non-availability also affects that process step. Accordingly, we transfer the unprocessed units $v_{c_s,l}$ to following process steps with further matrix calculations. The *resulting unprocessed units matrix* $V^*_{C,L}$ defined by Eq. (9) represents all unprocessed units $v^*_{c_s,l}$ per process step l after consideration of the compensation effect and continual production failure:

$$V^*_{C,L} = \begin{bmatrix} v^*_{c_1,1} & \cdots & v^*_{c_1,L} \\ \vdots & \ddots & \vdots \\ v^*_{c_k,1} & \cdots & v^*_{c_k,L} \end{bmatrix}. \tag{9}$$

A7 *Unprocessed units $v^*_{c_s,l}$ at a process step l cause monetary losses.*

The losses caused by unprocessed units reflect the value added during the production process in the respective process steps. The losses are assigned proportionally to each process step according to the respective activities performed in each process step. Process step-specific loss values are necessary because different *impact locations* of IT component failures cause different effects in the production network. For example, a production failure in the first process step results in no processed units; in contrast, a production failure in an advanced process step results in semi-finished units, which present a value because their time-to-market is shorter due to their advanced production state. The information about process step-specific loss values is available through accounting and performance measurement methods, such as activity-based costing and, hence, can be easily assessed and applied as exogenous input parameters to our model (Cooper and Kaplan 1991). Based thereupon, we apply the VaR to quantify the consequences of an IT component's non-availability in the considered time period. The VaR is a downside risk measure and a "standard benchmark" (Duffie and Pan 1997, p. 3) for the measurement of a company's exposure to financial risks, i.e., potential loss. For a given time period and probability (or confidence level) $(1-\alpha)$, the VaR is defined as the loss over the time period that is exceeded with probability α (Duffie and Pan 1997; Jorion 2006). We apply the VaR in our model for risk quantification as loss values corresponding to an IT component's non-availability are not fixed and may vary due to market-induced interference factors and random effects, such as price and demand fluctuations. Therefore, we assume that losses are normally distributed with an expected loss value μ_l and a standard deviation σ_l per unprocessed unit u for each process step l, expressed in monetary units (in US$). The use of a normal distribution is justifiable because variations of the value added are driven by market parameters, causing both positive and negative deviations. However, other distributions, such as the lognormal distribution, can be used, if the normal distribution is inappropriate in specific applications. The definition of a confidence level $(1-\alpha)$ takes into account the risk attitude. In most cases, no sufficient historical data basis exists to derive loss values and standard deviations solely by

means of statistical analyses. Therefore, the loss extends and probabilities must be estimated by experts (Hovav and D'Arcy 2003; Gordon and Loeb 2002; Mercuri 2003). Additionally, the excessive amounts of production-related data could be used to support these expert estimations (Lucke et al. 2008). With this information, the VaR of each IT component c_s for each process step l, denoted as $x_{c_s,l}$, can be derived by Eq. (10), with $N_{(1-\alpha)}$ being the $(1-\alpha)$ quantile of the normal distribution:

$$\mathrm{VaR} = x_{c_s,l} = \left(\mu_l * v^*_{c_s,l}\right) + N_{(1-\alpha)} * \left(\sigma_l * v^*_{c_s,l}\right). \tag{10}$$

The *risk value matrix* $X_{C,L}$, defined by Eq. (11), represents all VaR values of each IT component c_s for each process step l:

$$X_{C,L} = \begin{bmatrix} x_{c_1,1} & \cdots & x_{c_1,L} \\ \vdots & \ddots & \vdots \\ x_{c_k,1} & \cdots & x_{c_k,L} \end{bmatrix}. \tag{11}$$

The row sums $\sum_{l=1}^{L} x_{c_s,l}$ of matrix $X_{C,L}$ show the total VaR, caused by the non-availability of an IT component c_s. Ranking these values derives a priority order regarding the IT component's threat potential. This represents the central result of our risk assessment model, quantifying the consequences of an IT component's non-availability.

Our model's described risk quantification approach enables the consideration of diverse and complex *network structures* and *dependencies* between the production and information networks of the smart factory (A4). Further, with the compensation effect (A5) and continual production failure (A6), the model considers two key characteristics of a smart factory: the flexible combination of production components and the unit flow dependencies within the production network. By determining the resulting unprocessed units, and by quantifying the corresponding financial damage based on VaR (A7), the model derives a *risk value vector*, with risk values for each IT component. This information enables management to identify the information network's components most critical to the production network and to ground the corresponding investment decisions regarding IT security measures on a profound basis.

4 Exemplary application

In the following section, we demonstrate the applicability of our risk assessment model in an exemplary smart factory that is oriented on a real-world scenario of producing customized sports shoes. Afterwards, we conduct sensitivity analyses regarding the capacity utilization and the impact of varying loss potential estimations to evaluate the basic effects of two major influencing factors. Finally, we analyze the risk reduction effects of different IT security measures by comparing the model's results based on the *with-and-without-principle* to demonstrate the model's application in an investment decision process. We refrain from comparing our model and its results with other risk assessment methods for reasons of

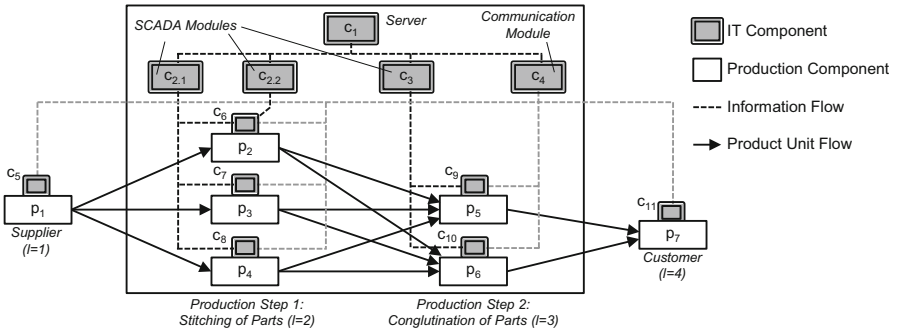

Fig. 4 Exemplary smart factory

evaluation, as we doubt the value of such a comparison due to the lack of comparable methods. Although there are other methods for the assessment of information risks such as the discussed FMEA model by Silva et al. (2014) or the model by Zambon et al. (2007), none of them incorporates the specific characteristics of smart factory networks, such as network structures or network interdependencies. However, this would be necessary for a meaningful and conclusive comparison with our model. Instead, we believe that further evaluation of our model in concrete real-world scenarios, with real-world data, is a promising next step for future research activities.

4.1 Exemplary smart factory setting

The smart factory in our application example is an automated production facility for the custom production of sports shoes.[2] The factory produces sports shoes, which are customized by customers online with regard to shoe type, fabrics, and colors. The company is deploying smart manufacturing technologies in the factory to produce the shoes in the shortest time possible. This enables the highly flexible custom production of sport shoes in a batch size of one, at costs comparable to mass production. Figure 4 illustrates the exemplary setting of the smart factory.

The customer (p_7) customizes a sports shoe on the sports goods manufacturer's online platform. Once completed, a data interface (c_{11}) automatically transmits the order to the smart factory. In correspondence to the customers' specifications, the necessary semi-finished parts are ordered automatically from the supplier (p_1). For this purpose, another data interface (c_5) connects the supplier with the smart factory. Once the raw materials are received, smart manufacturing machines first stitch the parts of the shoes together (p_2, p_3, and p_4), then conglutinate the stitched parts (p_5 and p_6). All machines, that is, sewing machines and conglutination machines, are equipped with embedded systems (c_6, c_7, c_8, c_9, and c_{10}) connecting the machines with the information network and enabling their communication. The information

[2] The smart factory example is geared to the "SPEEDFACTORY" research project, funded by the German Federal Ministry of Economics and Energy (2015).

Table 1 IT component assignment

IT service s	1	2	3	4	5	6	7	8	9	10	11
Main IT component	c_1	$c_{2.1}$	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}	c_{11}
Backup IT component		$c_{2.2}$									

Table 2 Interference degrees of IT components

IT component c_s	c_1	$c_{2.1}$	$c_{2.2}$	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}	c_{11}
Interference degree $\bar{r}_{c_s}$	100%	75%	75%	75%	75%	50%	50%	50%	50%	50%	50%	50%

network contains a communication module (c_4), facilitating information synchronization between smart manufacturing machines, and providing all required optimization parameters. By synchronizing status information, such as utilization, idle capacity, and queued orders, the smart manufacturing machines optimize product flow through the production process. Further, SCADA modules ($c_{2.1}$, $c_{2.2}$, and c_3) for the manufacturing machines control and monitor the assigned machines' production activities. The SCADA module $c_{2.1}$ controls the sewing machines p_2, p_3, and p_4, and SCADA module c_3 controls the conglutination machines p_5 and p_6. Thereby, sewing machine p_2 has an additional backup module ($c_{2.2}$) securing the main module ($c_{2.1}$). Accordingly, the backup module is an existing redundancy. All software modules ($c_{2.1}$, $c_{2.2}$, c_3, and c_4) are hosted on a company-owned server (c_1), located on the premises of the smart factory. The assignment of the IT components to the respective IT services is illustrated in Table 1.

The non-availability of IT components causes different interference degrees for the dependent production components (see Table 2). Thereby, non-availability of the server (c_1) causes a complete standstill of the dependent production components because all software services are interrupted. The non-availability of a software module causes an interference of 75% because either the information synchronization is disrupted or machine control functions are no longer provided. However, the affected machines' emergency routines enable a partial continuity of the production process. As a result, the production machines are only able to produce 25% of their actual capacity. The non-availability of an embedded system causes an interference of 50% because the dependent production components' information synchronization is hampered. Lastly, the non-availability of a data interface causes an interference of 50% because either the automated ordering process with the supplier is hampered and manual backup processes do not achieve the same efficiency, or the customer's ability to customize products is restricted.

Once the production of an order is completed, the sports shoes are shipped to the customer. The smart factory has a capacity of 120 units and a utilization rate of

Table 3 Capacity and utilization of production components

Production component p_i	p_1	p_2	p_3	p_4	p_5	p_6	p_7
Capacity q_i (units)	120	40	40	40	60	60	120
Utilization qu_i (units)	120	40	40	40	60	60	120

100%. The production components' capacities, utilizations, and idle capacities are shown in Table 3.

4.2 Analysis of basic scenario

By applying our risk assessment model to the exemplary smart factory, we can identify the IT components most critical to the production network. First, the matrix calculations obtain all functional dependencies of production components on IT components. The derived *dependency matrix* $D^*_{C,P}$ is multiplied by the interference degrees $\bar{r}_{c_s}$, illustrated in Table 2. Based thereupon, we derive the *unprocessed units* $v^*_{c_s,l}$ according to the risk quantification approach. In combination with the expected losses and standard deviations noted in Table 4, we calculate the threat potential based on the VaR for each IT component c_s, with a confidence level $(1-\alpha)$ of 95%.

The resulting *risk value matrix* $X_{C,L}$, noted in Table 5, presents the total threat potential $(\sum_{l=1}^{4} x_{c_s,l})$ posed by the non-availability of each IT component c_s.

The derived information regarding the threat potential of individual IT components, and their rank in relation to other IT components, identifies the most critical IT components. Additionally, the results of our risk assessment model reveal the following insights:

- The server of the smart factory (c_1) causes the *maximum possible threat potential*, with a VaR of \$7169, as its non-availability results in a complete standstill in the production network.
- The supplier data interface (c_5) ranks third, and before the SCADA modules (fourth and fifth, respectively), although the supplier data interface has a lower interference degree than the SCADA modules. This can be explained by the *impact location* of the failing IT components. The supplier data interface influences the first process step, in contrast to the SCADA modules, which influence later process steps. Therefore, an interesting insight is that the impact location in the production network is an important factor because the supplier data interface's restriction causes production failures in all subsequent process steps of our smart factory example. Further, the SCADA module for the sewing machines has a partial backup, which reduces its threat potential.

Table 4 Loss values of process steps

Process step l	1	2	3	4
Expected loss μ_l (\$)	5	10	10	15
Standard deviation σ_l (\$)	1.5	3	3	4.5

Table 5 Analysis results and risk value matrix

IT Comp. $\boldsymbol{c_s}$	c_1	$c_{2.1}$	$c_{2.2}$	c_3	c_4	c_5	c_6	$\boldsymbol{c}_7$	$\boldsymbol{c}_8$	$\boldsymbol{c}_9$	$\boldsymbol{c}_{10}$	$\boldsymbol{c}_{11}$	$\sum$
VaR $x_{(c_s,1)}$ ($)	896	0	0	0	672	448	0	0	0	0	0	0	
VaR $x_{(c_s,2)}$ ($)	1792	896	0	0	1344	896	299	299	299	0	0	0	
VaR $x_{(c_s,3)}$ ($)	1792	896	0	1344	1344	896	299	299	299	448	448	0	
VaR $x_{(c_s,4)}$ ($)	2688	1344	0	2016	2016	1344	448	448	448	672	672	1344	
VaR $\sum_{l=1}^{4} x_{(c_s,l)}$ ($)	7169	3136	0	3360	5376	3584	1045	1045	1045	1120	1120	1344	29,346
Rank	1	5	12	4	2	3	9	9	9	7	7	6	

- The embedded systems of the conglutination machines (c_9 and c_{10}) rank seventh and before the sewing machines' embedded systems (c_6, c_7 and c_8), although they affect a later process step. This is due to the utilization of the conglutination machines, which with 60 units are more substantial than the sewing machines' 40 units and, hence, lead to higher threat potentials.

Of course, the complexity of the exemplary smart factory is limited and, therefore, the server's first rank may seem obvious. However, smart factory networks in practice are far more complex and unmanageable because they consist of considerably more production components and IT components, inducing a highly complex dependency structure. Further, we assumed a symmetric setting regarding the production components' capacities within a process step, meaning that all production components in a process step possess identical capacities. This might also differ in practice, as machines are constantly developed and production facilities typically grow over time, resulting in a heterogeneous machinery pool. Nevertheless, the results and insights of our application clearly indicate the need for decision support through a structured approach that assesses the availability risks of individual IT components. With the information provided by our risk assessment model, the focal company's management can discuss potential IT security measures and can profoundly ground corresponding investment decisions.

4.3 Sensitivity analysis

We conduct sensitivity analyses in the following subsections to evaluate the results and basic effects of the two major influencing factors, that is, the utilization and loss potentials. Thereby, we use the smart factory setting from our demonstration example above.

4.3.1 Utilization variation

For the utilization variation, we increase the utilization of all production components gradually, from 1 to 100%, and evaluate the effects on the VaR values of the IT components and the VaR sum. Thereby, the VaR sum $\sum_{s=1}^{k}\left(\sum_{l=1}^{L} x_{c_s,l}\right)$ of the *risk value matrix* $X_{C,L}$ makes no statement regarding the information network's total threat potential because our model analyzes scenarios with individual IT component failures. However, the VaR sum can be used as an indicator of the vulnerability of the production network to IT component non-availabilities. All other parameters, such as interference degrees and loss potentials, are kept constant. The effects of an increasing utilization on our model's results can be seen in Fig. 5.

The VaR sum increases with an increasing utilization because more units are in the production process. However, the slope of the curve is not linear and illustrates four kink points at which the slope increases. The kink points are caused by IT components whose non-availabilities have no effect up to a certain utilization threshold. This effect can be seen in more detail in Fig. 6, which shows the curve of each IT component relative to the utilization. One reason for the kink points is an interference degree less than 100%. Depending on the utilization, the restricted

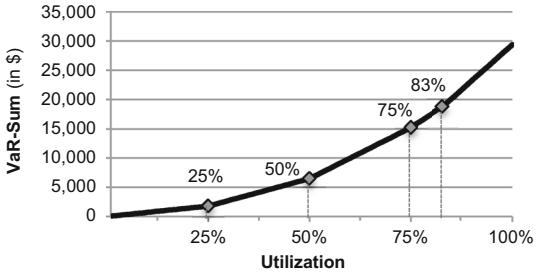

Fig. 5 Utilization variation—VaR-sum

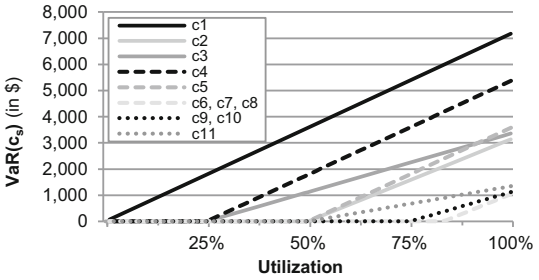

Fig. 6 Utilization variation—VaR (c_s)

production components can still process some or even all, product units with their reduced capacity. For example, the software modules (c_2, c_3, and c_4) have an interference degree of 75%. Accordingly, the non-availability of the communication module (c_4) and the SCADA module (c_3) has no effect until the threshold reaches 25%. The sewing machines' SCADA module ($c_{2.1}$) causes no losses even until the threshold reaches 50% because of its partial backup. The embedded systems have an even higher threshold. First, this is caused by the interference degree of 50%, but also by the compensation effect for utilizations less than 100%. Accordingly, the threshold of the embedded system is 75% (c_9 and c_{10}) and 83%, respectively (c_6, c_7, and c_8). Thereby, the sewing machines' embedded systems have a higher threshold because three machines are available for compensation within the stitching step, in contrast to two machines in the conglutination step.

4.3.2 Loss potential variation

In addition to the utilization, we analyze the impact of loss potential estimations on the results of our model in the example smart factory scenario to demonstrate the effects of inaccurate expert estimations. Thereby, we multiply the loss values μ_l and σ_l with a variable β to demonstrate the effects of an underestimation ($\beta < 1$), respectively an overestimation ($\beta > 1$). All other input parameters are constant. The effects of deviating loss potential estimations for different, higher utilizations are shown in Fig. 7, with $0.5 \leq \beta \leq 1.5$. The underestimation of loss potentials results in lower, and the overestimation in higher, threat potentials. Accordingly, the curves show an ascending slope. Thereby, the slope of a curve increases for higher utilizations.

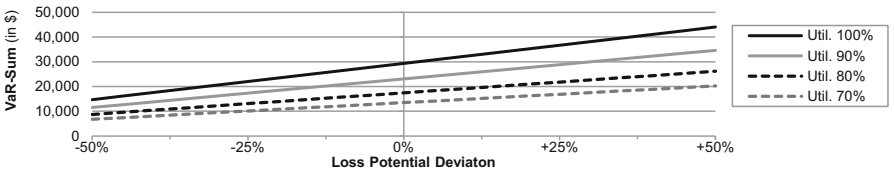

Fig. 7 Impact of deviating loss potential estimation

Of course, there are other influencing factors aside from utilization and loss potentials, such as the smart factory's network structure, and the interference degrees of IT components. However, varying other factors does not change the fundamental tendencies and effects described in this section.

4.4 IT security measure analysis

In the following, we analyze various IT security measures for our smart factory example by comparing the model's results based on the *with-and-without principle*. This demonstrates our model's applicability for the economic analyses of potential IT security investments and, thus, for the profound support of valuable investment decisions. For this, we compare the VaR sum of our basic scenario setting ($29,346) to settings with additional IT security measures and apply the VaR sum as an indicator for the vulnerability of the production network to IT component non-availabilities. This determines the impact of an IT security measure on the production network's vulnerability, and hence, enables a risk-oriented evaluation. Accordingly, the results can be used as a basis for investment decisions. As our model is based on the smart factory's network structure, it is highly suitable to analyze structure-based IT security measures.

For instance, these include redundancies in the information network. However, we also want to note other process-based measures. As we demonstrated during the sensitivity analyses, reduced loss potentials in specific process steps can reduce the overall threat potential. Thus, improving processes to reduce loss potentials is an effective way to reduce an overall threat potential. As loss potentials are input parameters in our model, it is not possible to explain the cause-effect chain of process-based measures and the reduced loss potentials as their effect. However, our model can illustrate the impact of reduced loss potentials on the production network's vulnerability to IT component non-availabilities if the reduced loss potentials are used as adjusted input parameters. Structure-based measures are supposed to be highly effective against IT availability risks, including redundancies within the information network. Thereby, measures such as backup IT components or cloud-based applications influence dependency relations by preventing single-point failures of IT components. For example, the basic scenario of our example application contains a redundancy, securing the SCADA service for sewing machine p_2 due to the partial backup SCADA module ($c_{2.2}$). Without the redundancy, the VaR increases to $30,915. Accordingly, the partial backup component reduces the

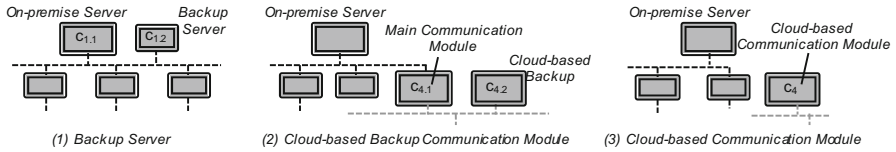

Fig. 8 Exemplary IT security measures

VaR sum by 5.1%. In the following, we add further IT security measures, as illustrated in Fig. 8, to the information network, in addition to the already existing partial backup component ($c_{2.2}$).

Installing a backup server (1) is an appropriate IT security measure because our model in the example application revealed that the server (c_1) is the most critical IT component. The VaR sum decreases to \$22,178, which equals a reduction of 24.4% in comparison to the basic scenario, because of this security measure. The hereby occurring trade-off between the high investment volume and the risk reduction effect demonstrates that our algorithm is of value because it enables a risk-oriented evaluation of investment alternatives and allows for the profound grounding of investment decisions. The second measure is a cloud-based backup for the communication module (c_4) (2). Cloud-based applications are especially effective because they not only remove the direct dependency of production components on the locally hosted, secured application, but they also remove the indirect dependency of production components on the server if the production components do not depend on other applications hosted on that server. This is, for example, the case for the supplier (p_1) and the customer (p_7), whose data interfaces only depend on the server because of the communication module (c_4). Accordingly, the cloud-based backup communication module also removes the customer and supplier's dependencies on the server, and reduces the VaR sum by 21.4% to \$23,704. The last measure analyzed is the complete switch of the communication module, from a module hosted on a company-owned server to a cloud-based module (3). As a result, the communication module no longer depends on the functioning of the server; hence, functional dependencies within the information network are removed. However, the production components still depend on the cloud-based communication module for the corresponding communication IT service because there is no redundant backup for that service. Accordingly, the VaR only decreases by 3.1% to \$28,450.

5 Managerial implications

Subsequently to the exemplary application, sensitivity analysis, and IT security measure analysis, we discuss managerial implications derived from the development of our risk assessment model in the following:

1. The results gained in the course of our research clearly indicate the need for decision support through a structured approach. The complexity that arises from the multitude of direct and indirect dependencies in ever complex smart factory information networks and the resulting propagation effects of failures can no longer be mastered by human decision makers alone due to an increasing lack of transparency. In this regard, our structured approach presents a risk-oriented guidance for practitioners in the course of their digital transformation.
2. There is a multitude of different IT security measures that companies can apply as part of their IT security strategy. These differ in their modes of action, but ultimately their effect on the possible extent of damage is decisive. Thereby, some IT security measures target specific critical components in the information network, in particular structural IT security measures such as redundancies through backup systems. In contrast, other IT security measures have a more holistic effect on the information network such as process-related IT security measures, e.g., reduced damage potentials through improved recovery measures. Here, our structured approach serves as guidance in the derivation of an appropriate IT security strategy. It supports investment decisions on a profound economic basis, as it helps to identify the most critical IT components and quantifies the threat potentials resulting from propagation effects.
3. A decisive lever for the IT security strategy is the degree of interconnectedness within the smart factory information network. Companies are faced with the question of where interconnectedness makes sense and creates added value and where air gaps should be deliberately made or redundancies should be created. For this, our approach provides a risk-oriented guidance for the solid design of smart factory information networks.
4. The insights gained by the sensitivity analysis demonstrate the importance of the utilization as an influencing factor. We were able to show that the threat potential increases with an increasing utilization because risk reduction effects, such as the compensation ability, decrease gradually. Considering the high utilization of smart factories through automation and optimization technologies as key benefits, the threat potentials posed by IT availability risks will be rather high in smart factories (Radziwon et al. 2014; Schuh et al. 2014).
5. The insights gained by the loss potential sensitivity analysis demonstrate that the underestimation or overestimation of loss values has a greater effect on the model's results in application scenarios with high utilizations. Therefore, considering the probable high utilization of smart factories, the loss potential estimation's accuracy is of crucial importance for risk quantification to derive accurate results.
6. Our risk assessment model examines IT availability risks primarily on the internal company level. In times of comprehensive, cross-company, Internet-based interconnection of information systems, however, the supply chain level becomes particularly important for companies' IT security strategy. For this purpose, our approach can also be extended across companies to make the prevailing complexity tangible and controllable.

The described managerial implications are highly relevant as they indicate aspects of IT security and IT availability risks in smart factory information networks that have to be considered when deciding on a suitable IT security strategy. Accordingly, they provide valuable guidance for companies in the course of their digital transformation.

6 Conclusion, limitations, and further research

The increasing adoption of smart manufacturing technologies promises great potential, leading to a paradigm shift in manufacturing. The emerging smart factory networks constitute automated and flexible production facilities and can efficiently produce individualized products in low batch sizes at a cost-efficient level. However, the criticality of IT systems and the interconnectedness of IT and production systems cause an increase in the vulnerability to IT availability risks. Considering this threat scenario, companies must employ extensive IT security measures to secure their production facilities. However, the highly complex, interconnected, and interdependent smart factory networks complicate investment decisions regarding possible IT security measures. Thus, decision makers face significant difficulties regarding the allocation of available funds in the most efficient way.

Therefore, we develop a risk assessment model for the quantification and evaluation of IT availability risks in smart factory networks that serves as the basis for corresponding investment decisions. We first model and formalize the smart factory networks' general setting, with its basic structures and relations, by means of graph theory and matrix notation. Then, we quantify IT availability risk by applying the VaR. Our research contributes to the literature and practice as it enables a structured analysis of increasingly complex smart factory networks under consideration of not only direct but also indirect dependencies. While other risk assessment approaches like multi-criteria decision models often times address different dimensions of damage and do not consider root causes, our approach focusses on propagation effects and the resulting damages within smart factory networks. Accordingly, our research is rooted in the propagation and damaging effects based on the complex interdependencies in smart factory networks. Our structured approach helps to assess the risks associated with the ever increasing interconnection within smart factories, to assess where interconnections and dependencies should be deliberately avoided and where redundancies should be deliberately created, e.g., by means of backup servers or cloud-based modules. Hence, the insights gained by our model provide practitioners with a risk-oriented guidance regarding the solid design of smart factory networks in the course of their digital transformation. Further, it helps to identify the most critical IT components and consequently offers a profound economic basis for corresponding investment decisions regarding IT security mitigation measures. Thus, it also supports the derivation of an appropriate IT security strategy. Based on the results of our model, other subsequent approaches, such as multi-criteria decision-making models, can then be applied. For example, based on a multi-criteria decision model, an optimal portfolio of IT security measures could be derived by taking into account different

decision criteria and dimensions. Corresponding approaches already exist, for example, in the area of cloud computing, for which Shameli-Sendi and Cheriet (2014) propose a risk assessment model based on fuzzy multi-criteria decision-making or Akinrolabu et al. (2018) propose a cloud supply chain cyber risk assessment model which applies decision support analysis and supply chain mapping for the identification, analysis and evaluation of cloud risks. Besides the risk-oriented guidance as the basis for subsequent decision making, our risk assessment model provides the possibility to consider a cross-company view regarding the effects of interorganizational information systems, as cross-company ecosystems increases constantly in the course of the ongoing digitalization. We demonstrate the model's applicability in a setting based on an exemplary real-world scenario, and conduct sensitivity analyses. Our results demonstrate that the criticality of an IT component is determined by numerous factors: the dependency relationships to production components, the degree of productivity interference caused by the IT component failure, the IT component failure's impact location within the production process, loss potentials in the respective process steps, the utilization of dependent production components, and the extent of the possible compensation effect. The variety of these influencing factors and their complex interplay clearly indicate the need for a risk assessment model enabling a structured analysis and supporting investment decisions.

Nevertheless, there are some limitations to our results, which represent potential areas for further research. First, we do not consider the possibility of negative, upward feedback effects within the information network. For example, a failing machine, which cannot upload information due to its failing embedded system, in turn affects the overall system. Additionally, we apply our risk assessment model in an exemplary application to demonstrate its applicability and its basic functionality. For further evaluations, it would be beneficial to apply our model in different real-world scenarios, with real-world data. Further, our model focuses on IT availability risks. The incorporation of other dimensions of IT security risk, such as accuracy, access, and accountability, would further increase the model's value regarding the identification of critical IT components. Another area for further research is the trade-off between the risk reduction effects of idle capacity and accompanying opportunity costs, which should be addressed by an optimization model built from our risk assessment model. Additionally, investment decisions regarding IT security measures include other aspects, such as the overall investment budget and the relation between a measure's efficiency and the required investment volume, which are not addressed in this paper.

Other than these limitations, we made certain model assumptions that limit the model's applicability, but that, in our opinion, are reasonable to keep the model's complexity moderate. Nevertheless, relaxing some model assumptions offers potential areas for the model's further development. First, our model assumes that IT components fail completely because technical failures and attacks result in the complete non-availability of IT components. Partial functionality interferences of IT components are not considered. As this could occur in some specific threat scenarios, such as data manipulations, the inclusion of this aspect could be a potential extension of our model. Second, our model analyzes the event of an IT component's non-

availability and its implications in a fixed time period. Thus, another substantial extension would involve including a timing component and, thus, developing our approach further to a continuous-time model. Third, though our model considers individual interference degrees for the respective IT components, we assume that an IT component's non-availability causes identical interference degrees on all dependent production components. We believe that this approach is reasonable because it includes the interference degrees on a detailed IT component level. A further differentiation on the production component level would cause an increase in complexity, while the added value seems questionable. However, a further differentiation of interference degrees on a production level would be possible.

Despite these limitations, we strongly believe that the developed risk assessment model presents a substantial step toward the profound management of IT availability risks in smart factory networks and supports the corresponding investment decision process. This is of particular importance because the continuous progression of IoT, CPS, and other smart manufacturing technologies requires the ongoing development of appropriate risk assessment methods.

References

Aagedal, Jan Øyvind, Den Braber, Folker, Dimitrakos, Theo, Gran, Bjørn Axel, Raptis, Dimitris, and Stolen, Ketil. 2002. Model-based risk assessment to improve enterprise security. In *Proceedings of the 5th IEEE international enterprise object computing conference*, 51–62. Lausanne.

Ackermann, Tobias, and Buxmann, Peter. 2010. Quantifying risks in service networks: Using probability distributions for the evaluation of optimal security levels. In *Proceedings of the Americas conference on information systems*. Lima, Peru.

Akinrolabu, Olusola, Steve New, and Andrew Martin. 2018. Cyber supply chain risks in cloud computing—Bridging the risk assessment gap. *Open Journal of Cloud Computing* 5 (1): 1–19.

Amin, Saurabh, Galina A. Schwartz, and Alefiya Hussain. 2013. In quest of benchmarking security risks to cyber-physical systems. *IEEE Network* 27 (1): 19–24.

Amiri, Amin Khodabandeh, Cavusoglu, Hasan, and Benbasat, Izak. 2014. When is IT unavailability a strategic risk? A study in the context of cloud computing. In *Proceedings of the 35th international conference on information systems*. Auckland.

Arns, Michael, Martin Fischer, Peter Kemper, and Carsten Tepper. 2002. Supply chain modelling and its analytical evaluation. *Journal of the Operational Research Society* 53 (8): 885–894.

Borodulin, Kirill, Radchenko, Gleb, Shestakov, Aleksandr, Sokolinsky, Leonid, Tchernykh, Andrey, and Prodan, Radu. 2017. Towards digital twins cloud platform: Microservices and computational workflows to rule a smart factory. In *Proceedings of the 10th international conference on utility and cloud computing*, Austin.

Brettel, Malte, Niklas Friederichsen, Michael Keller, and Marius Rosenberg. 2014. How virtualization, decentralization and network building change the manufacturing landscape: An industry 4.0 perspective. *World Academy of Science: Engineering and Technology International Journal of Mechanical, Aerospace, Industrial, Mechatronic and Manufacturing Engineering* 8 (1): 37–44.

Broy, Manfred, María Victoria Cengarle, and Eva Geisberger. 2012. Cyber-physical systems: Imminent challenges. In *Large-scale complex IT systems. Development, operation and management*, ed. R. Calinescu and D. Garlan, 1–28. Berlin: Springer.

BSI 2014. The State of IT Security in Germany 2014. https://www.bsi.bund.de/EN/Publications/SecuritySituation/SecuritySituation_node.html. Accessed April 21, 2015.

Buldyrev, Sergey V., Roni Parshani, Gerald Paul, H.Eugene Stanley, and Shlomo Havlin. 2010. Catastrophic cascade of failures in interdependent networks. *Nature* 464: 1025–1028.

Byres, Eric. 2013. The air gap: SCADA's enduring security myth. *Communications of the ACM* 56 (8): 29–31.

Byres, Eric, and Lowe, Justin. 2004. The myths and facts behind cyber security risks for industrial control systems. In *Proceedings of the VDE congress*, 213–218.

Caralli, Richard A., Stevens, James F., Young, Lisa R., and Wilson, William R. 2007. Introducing OCTAVE Allegro: Improving the information security risk assessment process. *Technical Report No. CMU/SEI-2007-TR-012, ESC-TR-2007-012,* 1–154.

Cardenas, Alvaro A., Saurabh Amin, and Shankar Sastry. 2008. Secure control: Towards survivable cyber-physical systems. *System* 1: 1–5.

Cavusoglu, Hasan, Huseyin Cavusoglu, and Srinivasan Raghunathan. 2004. Economics of IT security management: Four improvements to current security practices. *The Communications of the Association for Information Systems* 14: 65–75.

Chui, Micheal, Markus Löffler, and Roger Roberts. 2010. The internet of things. *McKinsey Quarterly* 2: 1–9.

Colombo, Armando Walter, Karnouskos, Stamatis, and Bangemann, Thomas. 2013. A system of systems view on collaborative industrial automation. In *Proceedings of the IEEE international conference on industrial technology*, Cape Town, 1968–1975.

Cooper, Robin, and Robert S. Kaplan. 1991. Profit priorities from activity-based costing. *Harvard Business Review* 69 (3): 130–135.

Danziger, Michael M., Louis M. Shekhtman, Amir Bashan, Yehiel Berezin, and Shlomo Havlin. 2016. Vulnerability of interdependent networks and networks of networks. In *Interconnected networks*, ed. Antonios Garas, 79–99. Cham: Springer.

Duffie, Darrell, and Jun Pan. 1997. An overview of value at risk. *The Journal of Derivatives* 4 (3): 7–49.

Eden, Peter, Blyth, Andrew, Jones, Kevin, Soulsby, Hugh, Burnap, Pete, Cherdantseva, Yulia, and Stoddart, Kristan. 2017. SCADA system forensic analysis within IIoT. In *Cybersecurity for industry 4.0—Analysis for design and manufacturing,* eds. L. Thomas and D. Schaefer, 73–101. Cham: Springer.

Eom, Jung-Ho, Park, Seon-Ho, Han, Young-Ju, and Chung, Tai-Myoung. 2007. Risk assessment method based on business process-oriented asset evaluation for information system security. In *Proceedings of the international conference on computational science*, 1024–1031.

Faisal, M.N., D.K. Banwet, and R. Shankar. 2006. Supply chain risk mitigation: Modeling the enablers. *Business Process Management Journal* 12 (4): 535–552.

Fenz, Stefan, Andreas Ekelhart, and Thomas Neubauer. 2011. Information security risk management: In which security solutions is it worth investing? *Communications of the Association for Information Systems* 28 (1): 329–356.

Festinger, Leon. 1949. The analysis of sociograms using matrix algebra. *Human Relations* 2: 153–158.

Fleisch, Elgar, and Thiesse, Frédéric. 2007. On the management implications of ubiquitous computing: An IS perspective. In *Proceedings of the 15th European conference on information systems*, St. Gallen, pp. 1929–1940.

Fridgen, Gilbert, Christian Stepanek, and Thomas Wolf. 2014. Investigation of exogenous shocks in complex supply networks—A modular petri net approach. *International Journal of Production Research* 53 (5): 1387–1408.

Geisberger, Eva, and Manfred Broy. 2015. *Living in a networked world—Integrated research agenda cyber-physical systems*. Munich: Acatech National Academy of Science and Engineering.

German Federal Ministry of Economics and Energy 2015. SPEEDFACTORY—Automatic custom manufacture of sports shoes and textiles. http://autonomik4.pt-dlr.de/en/SPEEDFACTORY.php. Accessed March 27, 2015.

Gordon, Lawrence A., and Martin P. Loeb. 2002. The economics of information security investment. *ACM Transactions on Information and System Security* 5 (4): 438–457.

Gordon, Lawrence A., Martin P. Loeb, and Tashfeen Sohail. 2003. A framework for using insurance for cyber-risk management. *Communications of the ACM* 46 (3): 81–85.

Haller, Stephan, Stamatis Karnouskos, and Christoph Schroth. 2009. The internet of things in an enterprise context. In *Future internet—FIS 2008, John Domingue*, ed. D. Fensel and P. Traverso, 14–28. Berlin: Springer.

Hallikas, Jukka, Iris Karvonen, Urho Pulkkinen, Veli-Matti Virolainen, and Markku Tuominen. 2004. Risk management processes in supplier networks. *International Journal of Production Economics* 90 (1): 47–58.

Harland, Christine, Richard Brenchley, and Helen Walker. 2003. Risk in supply networks. *Journal of Purchasing and Supply Management* 9 (2): 51–62.

Hermann, Mario, Pentek, Tobias and Otto, Boris. 2015. Design principles for industrie 4.0 scenarios—A literature review. *Technische Universität Dortmund - Working Paper 01/2015*.

Hertel, Michael. 2015. Risiken der Industrie 4.0: Eine Strukturierung von Bedrohungsszenarien der Smart Factory. *HMD - Praxis der Wirtschaftsinformatik* 52 (5): 724–738.

Hessman, Travis. 2013. The dawn of the smart factory. *Industry Week* 14: 14–19.

Hovav, Anat, and John D'Arcy. 2003. The impact of denial of service attack announcements on the market value of firms. *Risk Management and Insurance Review* 6 (2): 97–121.

Huang, C. Derrick. 2010. Optimal investment in information security: A business value approach. In *Proceedings of the pacific Asia conference on information systems*, Taipei, 444–451.

Iansiti, Marco, and Karim R. Lakhani. 2014. Digital ubiquity: How connections, sensors, and data are revolutionizing business. *Harvard Business Review* 92 (11): 91–99.

Jaisingh, Jeevan, and Rees, Jackie. 2001. Value at risk: A methodology for information security risk assessment. In *Proceedings of the 6th INFORMS conference on information systems and technology*, Miami, 1–15.

Jorion, Philippe. 2006. Value at risk: The new benchmark for managing financial risk (3rd ed.). McGraw-Hill. ISBN 978-0-07-146495-6.

Jung, Kiwook, SangSu Choi, Boonserm Kulvatunyou, Hyunbo Cho, and K.C. Morris. 2017. A reference activity model for smart factory design and improvement. *Production Planning and Control* 28 (2): 108–122.

Karabacak, Bilge, and Ibrahim Sogukpinar. 2005. ISRAM: Information security risk analysis method. *Computers and Security* 24: 147–159.

Karnouskos, Stamatis, and Colombo, Armando Walter. 2011. Architecting the next generation of service-based SCADA/DCS system of systems. In *Proceedings of the 37th annual conference on IEEE industrial electronics society*, Melbourne, pp. 359–364.

Karnouskos, Stamatis. 2011. Stuxnet Worm impact on industrial cyber-physical system security. In *Proceedings of the 37th annual conference on IEEE industrial electronics society*, Melbourne, 4490–4494.

Lasi, Heiner, Peter Fettke, Hans-Georg Kemper, Thomas Feld, and Michael Hoffmann. 2014. Industry 4.0. *Business and Information Systems Engineering* 6 (4): 239–242.

Lee, Edward A. 2008. Cyber physical systems: Design challenges. In *Proceedings of the 11th IEEE international symposium on object oriented real-time distributed computing*, Orlando, 363–369.

Lee, Jay, Behrad Bagheri, and Hung-An Kao. 2015. A cyber-physical systems architecture for industry 4.0-based manufacturing systems. *Manufacturing Letters* 3: 18–23.

Lucke, Dominik, Carmen Constantinescu, and Engelbert Westkämper. 2008. Smart factory—A step towards the next generation of manufacturing. In *Manufacturing systems and technologies for the new frontier—The 41st CIRP conference on manufacturing systems*, ed. M. Mitsuishi, K. Ueda, and F. Kimura, 115–118. London: Springer.

Mercuri, Rebecca T. 2003. Analyzing security costs. *Communications of the ACM* 46 (6): 15–18.

Meredith, Jack R., Amitarh Raturi, Kwasi Amoako-Gyampah, and Bonnie Kaplan. 1989. Alternative research paradigms in operations. *Journal of Operations Management* 8 (4): 297–326.

Niesen, Tim, Houy, Constantin, Fettke, Peter, and Loos, Peter. 2016. Towards an integrative big data analysis framework for data-driven risk management in Industry 4.0. In *Proceedings of the 49th Hawaii international conference on system sciences*, 5065–5074.

Papa, Stephen, Casper, William, and Nair, Suku. 2011. Availability-based risk analysis for SCADA embedded computer systems. In *Proceedings of the world congress in computer science, computer engineering and applied computing*, Las Vegas.

Qi, Qinglin, and Fei Fao. 2018. Digital Twin and big data towards smart manufacturing and industry 4.0: 360 Degree comparison. *IEEE Access* 6: 3585–3593.

Radziwon, Agnieszka, Arne Bilberg, Marcel Bogers, and Erik Skov Madsen. 2014. The smart factory: Exploring adaptive and flexible manufacturing solutions. *Procedia Engineering* 69: 1184–1190.

Rainer, Rex Kelly, Charles A. Snyder, and Houston H. Carr. 1991. Risk analysis for information technology. *Journal of Management Information Systems* 8 (1): 129–147.

Ramkumar, Maria Arputham, and Mamata Jenamani. 2015. Sustainability in supply chain through e-procurement—An assessment framework based on DANP and liberatore score. *IEEE Systems Journal* 9 (4): 1554–1564.

Shameli-Sendi, Alireza, Rouzbeh Aghababaei-Barzegar, and Mohamed Cheriet. 2016. Taxonomy of information security risk assessment (ISRA). *Computers and Security* 57: 14–30.

Sendi, Alireza Shameli, and Mohamed Cheriet. 2014. Cloud computing: A risk assessment model. In *IEEE International Conference on Cloud Engineering*.

Shariatzadeh, Navid, Thomas Lundholm, Lars Lindberg, and Gunilla Sivard. 2016. Integration of digital factory with smart factory based on internet of things. *Procedia CIRP* 50: 512–517.

Schlick, Jochen, Stephan, Peter, Loskyll, Matthias, and Lappe, Dennis. 2014. Industrie 4.0 in der praktischen Anwendung. In *Industrie 4.0 in Produktion, Automatisierung und Logistik*, 57–84. Wiesbaden: Springer.

Schuh, Günther, Potente, Till, Varandani, Rawina, Hausberg, Carlo, and Fränken, Bastian. 2014. Collaboration moves productivity to the next level. In *Proceedings of the 47th CIRP conference on manufacturing systems*, Windsor, 3–8.

Shrouf, Fadi, Ordieres, Joapuin, and Miragliotta, Giovanni. 2014. Smart factories in industry 4.0: A review of the concept and of energy management approached in production based on the internet of things paradigm. In *Proceedings of the IEEE international conference on industrial engineering and engineering management*, Selangor, 697–701.

Silva, Maisa Mendonça, Anna Paula Henriquies de Gusmão, Thiago Poleto, Lúcio Camara e Silva, and Ana Paula Cabra Seixas Costa. 2014. A multidimensional approach to information security risk management using FMEA and fuzzy theory. *International Journal of Information Management* 34: 733–740.

Smith, Grafton Elliot, Kenneth Watson, Will Baker, and Pokorski Jon. 2007. A critical balance: Collaboration and security in the IT-enabled supply chain. *International Journal of Production Research* 45 (11): 2595–2613.

Strozzi, Fernanda, Claudia Colicchia, Alessandro Creazza, and Carlo Noè. 2017. Literature review on the 'Smart Factory' concept using bibliometric tools. *International Journal of Production Research* 55 (22): 1–20.

Suh, Bomil, and Ingoo Han. 2003. The IS risk analysis based on a business model. *Information and Management* 41: 149–158.

Sun, By Lili, Rajendra P. Srivastava, and Theodore J. Mock. 2006. An information systems security risk assessment model under the Dempster–Shafer theory of belief functions. *Journal of Management Information Systems* 22 (4): 109–142.

Tupa, Jiri, Jan Simota, and Frantisek Steiner. 2017. Aspects of risk management implementation for industry 4.0. *Procedia Manufacturing* 11: 1223–1230.

Turber, Stephanie, and Smiela, Christoph. 2014. A business model type for the internet of things. In *Proceedings of the 22nd European Conference on Information Systems*, Tel Aviv.

Uhlemann, Thomas H.-J., Crhristoph Schock, Christian Lehmann, Stefan Freiberger, and Rolf Steinhilper. 2017. The digital twin: Demonstrating the potential of real time data acquisition in production systems. *Procedia Manufacturing* 9: 113–120.

Wagner, Stephan M., and Nikrouz Neshat. 2010. Assessing the vulnerability of supply chains using graph theory. *International Journal of Production Economics* 126: 121–129.

Wang, Shiyong, Jiafu Wan, Di Li, and Chunhua Zhang. 2016. Implementing smart factory of industrie 4.0: An outlook. *International Journal of Distributed Sensor Networks* 12 (1): 1–10.

Wegner, Andre, James Graham, and Eli Ribble. 2017. A new approach to cyberphysical security in industry 4.0. In *Cybersecurity for industry 4.0—Analysis for design and manufacturing*, eds. L. Thomas and D. Schaefer, 59–72. Cham: Springer.

Westerman, Georg F., and Hunter, Richard. 2009. Developing a common language about IT risk management. *MIT Sloan School Working Paper 4933-11 - CISR Working Paper No. 377*.

Wu, Teresa, Jennifer Blackhurst, and Peter O'Grady. 2007. Methodology for supply chain disruption analysis. *International Journal of Production Research* 45 (7): 1665–1682.

Yadav, Surya B., and Tianxi Dong. 2014. A comprehensive method to assess work system security risk. *Communications of the Association for Information Systems* 34: 169–198.

Yoon, Joo-Sung, Seung-Jun Shin, and Suk-Hwan Suh. 2012. A conceptual framework for the ubiquitous factory. *International Journal of Production Research* 50 (8): 2174–2189.

Zambon, Emmanuele, Bolzoni, Damiano, Etalle, Sandro, and Salvato, Marco. 2007. Model-based mitigation of availability risks. In *Proceedings of the 2nd IEEE/IFIP international workshop on business-driven IT management*, Munich, pp. 75–83.

Zambon, Emmanuele, Sandro Etalle, Roel J. Wieringa, and Pieter Hartel. 2011. Model-based qualitative risk assessment for availability of IT infrastructures. *Software and Systems Modelling* 4 (10): 553–580.

Zuehlke, Detlef. 2010. SmartFactory—Towards a factory-of-things. *Annual Reviews in Control* 34: 129–138.

Zhong, Ray Y., Xun Xu, and Lihui Wang. 2017. IoT-enabled smart factory visibility and traceability using laser-scanners. *Procedia Manufacturing* 10: 1–14.