Bus Inf Syst Eng 62(4):323–345 (2020)
https://doi.org/10.1007/s12599-019-00610-6

RESEARCH PAPER

Modeling IT Availability Risks in Smart Factories

A Stochastic Petri Nets Approach

Daniel Miehle · Björn Häckel · Stefan Pfosser · Jochen Übelhör

Received: 23 September 2017 / Accepted: 11 June 2019 / Published online: 19 August 2019

Abstract In the course of the ongoing digitalization of production, production environments have become increasingly intertwined with information and communication technology. As a consequence, physical production processes depend more and more on the availability of information networks. Threats such as attacks and errors can compromise the components of information networks. Due to the numerous interconnections, these threats can cause cascading failures and even cause entire smart factories to fail due to propagation effects. The resulting complex dependencies between physical production processes and information network components in smart factories complicate the detection and analysis of threats. Based on generalized stochastic Petri nets, the paper presents an approach that enables the modeling, simulation, and analysis of threats in information networks in the area of connected production environments. Different worst-case threat scenarios regarding their impact on the operational capability of a close-to-reality information network are investigated to demonstrate the feasibility and usability of the approach. Furthermore, expert interviews with an academic Petri net expert and two global leading companies from the automation and packaging industry complement the evaluation from a practical perspective. The results indicate that the developed artifact offers a promising approach to better analyze and understand availability risks, cascading failures, and propagation effects in information networks in connected production environments.

Keywords Smart factory · Information network · Information network analysis · IT availability risks · Petri nets

Accepted after three revisions by Jan Mendling.

Electronic supplementary material The online version of this article (https://doi.org/10.1007/s12599-019-00610-6) contains supplementary material, which is available to authorized users.

D. Miehle
Technical University of Munich, Boltzmannstraße 3, 85748 Garching bei München, Germany
e-mail: daniel.miehle@tum.de

B. Häckel
Project Group Business & Information Systems Engineering of the Fraunhofer FIT, Professorship for Digital Value Networks, University of Applied Sciences Augsburg, Friedberger Straße 2a, 86161 Augsburg, Germany
e-mail: bjoern.haeckel@fim-rc.de

S. Pfosser
BMK Group, Werner-von-Siemens-Straße 6, 86159 Augsburg, Germany
e-mail: stefan.pfosser@bmk-group.de

J. Übelhör (✉)
Project Group Business & Information Systems Engineering of the Fraunhofer FIT, FIM Research Center Finance & Information Management, University of Augsburg, Universitätsstrasse 12, 86159 Augsburg, Germany
e-mail: jochen.uebelhoer@fim-rc.de

1 Introduction

A recent worldwide survey by PricewaterhouseCoopers (PwC) among 2000 participants from nine major industrial sectors and 26 countries showed that 54% of the participants considered business interruptions due to cyber-security breaches the main challenge for smart factories (PwC 2016a). Thereby, in contrast to traditional factories, smart factories enhance production systems through horizontal and vertical integration of information systems

representing a central characteristic of the Industry 4.0 vision (Acatech 2013). In this context, additional IT availability risks arise from digitalization and interconnection of production (Amin et al. 2013). As production infrastructures in smart factories become increasingly intertwined with information and communication technology (ICT), the operational capability of smart factories increasingly depends on the high availability of information systems (Lucke et al. 2008). Thereby, concepts such as the Internet of Things (IoT) and Cyber-Physical Systems (CPS) intensify the digital interconnection of production via intra- and inter-organizational information networks (Acatech 2013).

On the one hand, the comprehensive interconnection and resulting real-time availability of information enable innovative production principles and business models offering extensive advantages (e.g., increased flexibility and efficiency of production) (Iansiti and Lakhani 2014). On the other hand, however, highly interconnected smart factories are becoming more vulnerable to IT availability risks (e.g., due to the removal of protective air gaps or interconnection of production and office environments) (Smith et al. 2007; Amiri et al. 2014; Smith et al. 2007). Moreover, the integration of Internet-based applications (e.g., cloud computing) and the growing collaboration with value chain partners (customers or vendors) reinforce this threat potential due to the growing number of possible access points for malicious cyber-attacks (Smith et al. 2007; Yoon et al. 2012). This was also found by the study of PwC as the number of cyber-attacks on businesses rose by 38% in 2015 (PwC 2016b). Consequently, companies face the challenge to cope with this increased threat potential. In addition to intentional attacks, unintentional errors (e.g., technical defects or human errors) can heavily compromise the availability of information networks directly and indirectly.

As physical production processes in smart factories are highly dependent on the underlying information network, threats can affect the operational capability of both information and production networks (Broy et al. 2012). In addition, threats now also include the propagation of locally occurring interruptions within interconnected information and production networks even without physical connections (Smith et al. 2007). Thus, informational dependencies that arise from the increasing interconnection and use of real-time information are becoming more important. Moreover, information-based systemic risks that may spread across smart factory boundaries in interconnected digitalized networks are also identified as one of the most important challenges in the field of computer science and business informatics, where they are known as the "*grand challenges*" (Buhl and Penzel 2010; Mertens and Barbian 2015). Accordingly, IT availability risks have become one of the most important threats in smart factories (Amiri et al. 2014).

This has also been shown by numerous incidents. One well-known example is the *Stuxnet* worm, which infected the industrial control system of a nuclear power plant in Iran in 2011 (The New York Times 2011). Today, attacks can heavily impede the production of a factory and are a threat of upmost relevance as e.g., 70% of the companies of a recent study state that they were attacked within the last two years (BSI 2017). The same study revealed that every second successful attack causes production downtimes or a loss of operations. In this context, the *locky* or *WannaCry* ransomware (e.g., Merkur 2018) is another impressive example, how intentional attacks can spread within a company, even when starting at only one weak point. Thereby, the weak point does not have to be directly connected to production components, as, for instance, malicious attackers targeted the industrial control system of a steel mill via the office network to compromise the operation of blast furnaces in 2014 (BSI 2014). Moreover, errors can lead to far-reaching disturbances: for instance, an incorrect software update forced a nuclear power plant into an emergency shutdown for 48 h in the US in 2008 (Washington Post 2008) and a technical defect of a single hard disk resulted in a server shutdown for 19 h in three clinics in Germany (BSI 2016).

Considering the technical developments and described threat scenarios, companies face the challenge of dealing with increasingly complex information networks regarding IT availability risk and their inherent dependency structures. Thereby, especially the dynamic behavior including cascading failures and stochastic propagation effects are of critical importance as single point failures can spread in the entire network and cause severe damage in the smart factory, e.g., in terms of production downtime and economic damage. Accordingly, companies are confronted with new challenges regarding a comprehensive risk management. Thereby, companies have to go through the four phases of risk management including (1) identification, (2) quantification, (3) control, and (4) monitoring (Hallikas et al. 2004). For this, companies require appropriate methods for the modeling and simulation of such information networks (Lasi et al. 2014) capturing the peculiarities of information networks in smart factories as a first step. As necessary concepts for an appropriate modeling of information networks do not exist so far, we state the following research question.

RQ How can the information network of a smart factory be modeled to depict and simulate IT availability risks?

Following the design science research (DSR) approach (Hevner et al. 2004), we introduce a stochastic Petri net approach, which enables a structured depiction of

information networks in smart factories. This allows the analysis of IT availability risks and the identification of weak spots within the information network. Our approach depicts the structure of information networks by modeling single components and informational dependencies between them. Hence, our approach facilitates the risk-oriented analysis of single components as well as of the whole information network. Further, it enables the simulation and analysis how different patterns of information networks are affected by certain threat scenarios and how propagation effects occur and spread in different patterns (e.g., the security level of components). For example, with regard to the mentioned examples, our approach could have been used preventively to model, simulate, and analyze the information network in the course of risk management. On this basis, weak points for attacks and critical dependencies would have become apparent, for which targeted security measures could then have been taken. Although this would not have made a 100% protection possible, a reduction of risk, for example by reducing the probability of a successful attack, would have been possible. This is particularly important in smart factories, as the vulnerability of smart factories increases significantly due to the increasing dependency relations within the information network.

Following the publication schema suggested by Gregor and Hevner (2013), this paper is organized as follows. In the next section, we provide an overview of related work regarding smart factories and IT availability risks. Based on the literature, we derive design objectives and requirements for an appropriate modeling approach. In Sect. 3, we specify Petri nets (PN) as the modeling language used in our approach. Section 4 describes our modeling approach as one essential artifact of our research. In Sect. 5, we evaluate our modeling approach by performing a feature comparison and demonstrating the applicability and feasibility of our artifact by simulating an exemplary information network based on a real-world setting. Further, to complement the evaluation from a naturalistic perspective, we integrate the insights of interviews with two experts from global leading companies in the robotic automation and packaging industry, and an academic PN expert. Finally, in Sect. 6, we discuss the results and limitations of our research and provide an outlook on future research.

2 Theoretical Background and Design Objectives

In this section, we review current literature on smart factories and categorize IT availability risks and threats in smart factories. Based on the literature, we define design objectives (DO) to lay the foundation for the development of our artifact in correspondence with our research question.

2.1 Smart Factories

The investigated body of literature comprises *infrastructural aspects* (Lucke et al. 2008; Yoon et al. 2012; Zuehlke 2010; Colombo and Karnouskos 2009), *characteristics* (Brettel et al. 2014; Radziwon et al. 2014; Schuh et al. 2014), as well as *challenges* (Amin et al. 2013; Broy et al. 2012; Cardenas et al. 2009; Sridhar et al. 2012; Sadeghi et al. (nd)) regarding smart factories. Although widely used in literature and practice (Radziwon et al. 2014), there is no common definition of the term *smart factory*, so far. Based on the analysis 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*" and describe, that "*within the modular structured Smart Factories […], CPS monitor physical processes, create a virtual copy of the physical world and make decentralized decisions*". And adopting the idea of IoT, Zuehlke (2010) describes a smart factory that is composed of smart objects that are able to "*self-organize to fulfil a certain task*" by interacting with each other via wireless communication infrastructures. These definitions reflect the specific characteristics of smart factories, such as their modular and decentralized design, which enables functionalities like production flexibility, reconfigurability, and adaptability and that distinguish a smart factory from a conventional factory (Brettel et al. 2014; Radziwon et al. 2014; Zuehlke 2010).

In contrast to traditional factories, smart factories enhance manufacturing systems through horizontal and vertical integration representing a fundamental characteristic of the industry 4.0 vision (Acatech 2013). Horizontal integration refers to the integration of IT systems across value chains both within a company and between several different companies. This results in the creation of new internal and external connections for data analysis or supply chain operations as well as the abandoning of air gaps. Vertical integration refers to the integration of IT systems across the different levels of the automation pyramid (cf. Fig. 1). Through the integration of production-oriented CPSs, so called Cyber-Physical Production Systems (CPPSs), the levels of the automation pyramid (i.e., field to business level) gradually vanish and are replaced by networked and decentrally organized services (Brettel et al. 2014; Monostori 2014). CPPSs integrate computing and communication capabilities in physical production environments realizing the fusion of the cyber and physical world (Lee et al. 2015; Wang et al. 2016). Accordingly, CPPSs are able to sense, monitor, and control physical

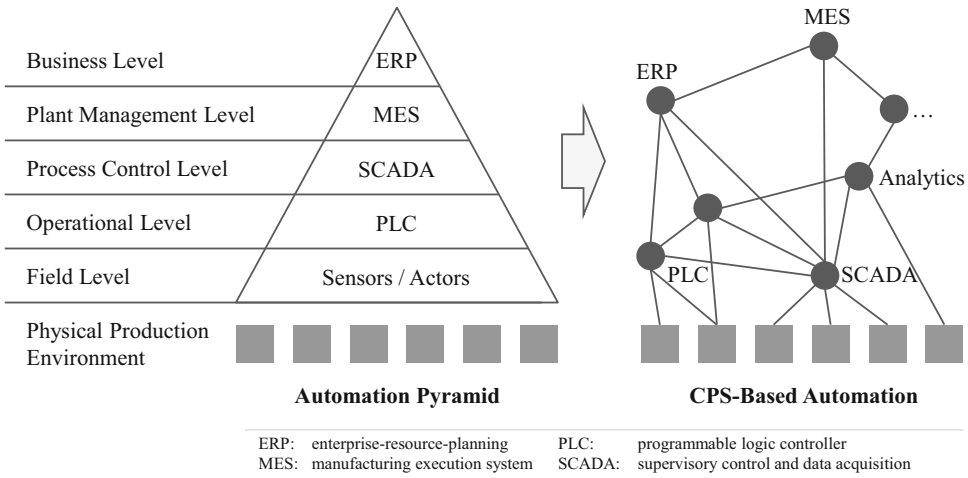


Fig. 1 Vertical integration – Decomposition of automation hierarchy – own illustration based on VDI (2013)

production in an autonomous manner and interact with each other in real-time (Brettel et al. 2014). Based on the described characteristics in existing literature, we obtained the following detailed structure of a smart factory as shown in Fig. 2.

The structure of a smart factory comprises a physical production environment and an information network. Following the definition of IT infrastructure (Weill and Vitale 2002), we characterize an information network in the context of smart factories as a horizontally and vertically integrated network of hardware, software, and service components (i.e., information network components) supporting IT-enabled processes in the physical production environment. The physical production environment consists of several production components (e.g., smart industrial robots, smart machines, and smart transport systems) that perform one or multiple tasks and can be combined flexibly according to the requirements of a product (Lasi et al. 2014; Lucke et al. 2008). Production components are equipped with a multitude of sensors and/or actuators that are connected to programmable logic controller (PLC) as well as to higher level IT services and data storages via the information network (Lee et al. 2015; Lucke et al. 2008; Zuehlke 2010). The information network seamlessly connects so far separated information network components within a company and across company borders enabling a flexible and reconfigurable production (Lucke et al. 2008; Yoon et al. 2012). Sensors and actuators translate signals between the physical and cyber world. Thus, they can be considered as bridge components that are part of both the production environment and the information network (Hao and Xie 2009). Thereby, sensors gather physical production data (e.g., temperature, pressure) for tasks such as quality management or predictive maintenance (e.g., checking oil level). Actuators execute production tasks based on control commands from PLCs (Lee et al. 2015; Zuehlke 2010). PLCs ensure the self-control of certain tasks and the exchange of relevant production data between machines and between information network components such as IT services (Lucke et al. 2008). IT services include applications such as enterprise resource planning (ERP) or manufacturing execution systems (MES). The server infrastructure for IT services and data storage can either be hosted on premise or in the cloud (Colombo and Karnouskos 2009; Yoon et al. 2012; Zuehlke 2010). Applications will increasingly be running in the cloud in the future. In addition, there are numerous external interfaces to value chain partners that are essential for the increased flexibility

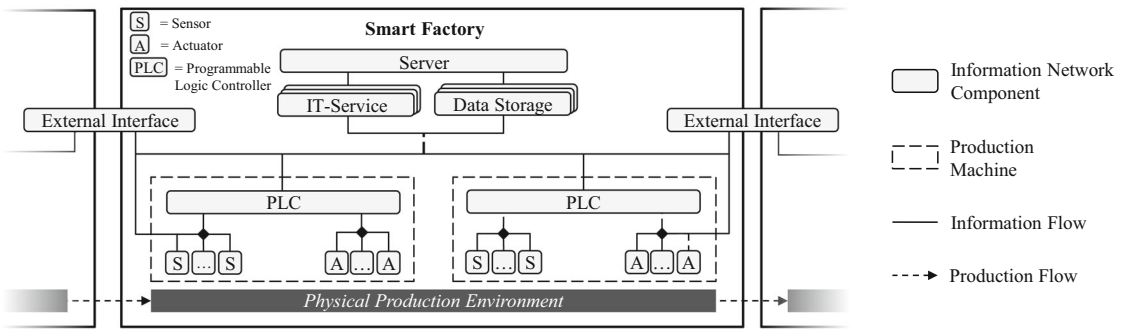


Fig. 2 Basic structure of a smart factory – own illustration based on Lucke et al. (2008) and Yoon et al. (2012)

of the production system and the optimization of production processes extending the information network of a smart factory (Broy et al. 2012; Acatech 2013). In conclusion, the information network consists of a multitude of different types of information network components increasing the overall complexity of production facilities.

For one thing, *"a networked machine is more valuable than isolated ones"* and enables the creation of *"autonomous and intelligent applications"* (Wan et al. 2013). At the same time, however, the increasing vertical and horizontal integration of ICT and the growing importance of real-time information in smart factories lead to information networks with complex and manifold informational dependencies. Hence, a structured modeling approach is required to provide transparency and to allow the identification of critical components and dependencies. Therefore, the modeling approach should provide a formal representation to support companies with the analysis of information networks in smart factories. This enables a detailed, simulation-based analysis and the comparability of different information network designs. Further, a graphical representation of the modeling approach would be beneficial as it enables a transparent representation of the mode of operation of a modeled information network component. As information networks can be of different sizes in dependence of the size of the overall production facility (ranging from a few hundred components to several tens of thousands components, e.g., Siemens Electronics Factory in Amberg with $>$ 1.000 PLC components besides other IT components (Siemens 2017)), the modeling approach should be able to depict single components, subnetworks (e.g., production cells), and entire smart factory networks. Thereby, we understand scalability as the ability of our modeling approach to handle an increasing number of components. Against this background, we define the following design objectives.

DO.1 *Graphical and formal representation:* To enable the depiction and simulation-based analysis of IT availability risks, the modeling approach has to provide an appropriate formal and mathematical representation of information networks in smart factories and a graphic representation of the modeling approach.

DO.2 *Scalability:* To depict information networks of different sizes and complexity, the modeling approach should capture single components, subnetworks, and entire smart factory networks in a scalable and comprehensible manner.

2.2 IT Availability Risks and Threats in Smart Factories

In this subsection, we describe *IT availability risks* in smart factories. Following the definition of risk by Kaplan and Garrick (1981), we differentiate between *availability risks* and *threats. Threats* describe the source of *availability risks*, whereas *availability risks* describe the effects, more specifically the damage potential. Thus, a *threat* is an event that can compromise components of information networks and even cause the entire smart factory to fail (BSI 2016). As shown in Fig. 3, *threats* in smart factories include both intentional *attacks* and unintentional *errors* (Amin et al. 2013).

An *attack* is any intentional threat event that may result in loss of the functionality of a component (Amin et al. 2013). According to the motivation of potential attackers, the following types of attacks can be distinguished. *Internal attacks* (e.g., social engineering) are executed by attackers from inside the organization (i.e., employees), whereas *external attacks* (e.g., malware infections, attacks on control components or Denial-of-service (DoS) attacks) are executed by attackers from outside the organization (e.g., cybercriminals) (Cardenas et al. 2009). Thereby, production machines are an easy target for attackers as they usually run custom and often obsolete software solutions and, thus, are rather poorly secured. An *error* is any unintentional threat event that may result in loss of the functionality of a component (Amin et al. 2013). Errors can be differentiated between *technical errors* (e.g., technical defects), *operator errors* (e.g., erroneous entry of data), and *organizational errors* (e.g., incorrect software update) (Amin et al. 2013).

To better understand availability risks in smart factories and their relations to threats, vulnerabilities, and countermeasures as well as reinforcers, we describe their relations as depicted in Fig. 4.

As already mentioned, *threats* are defined as the source of *availability risks*. By exploiting the *vulnerabilities* of a *component*, *threats* can compromise directly and indirectly specific *components* of the information network. The resulting *informational risks* (e.g., availability issues, loss of data) can be evaluated, for instance, by means of the remaining availability of the information network. *Countermeasures* can reduce the *vulnerabilities* of *components* and *informational risks*, for instance, to avert operational interruptions. We adopt the idea of *reinforcers* introduced by Keller and König (2014, p 6), which are caused mainly by the underlying network structure. Thereby, *reinforcers* (e.g., structural design, propagation effects) can increase the *vulnerabilities* of *components* and *availability risks*. Informational dependencies that arise from (1) the high number of interconnected components and (2) the

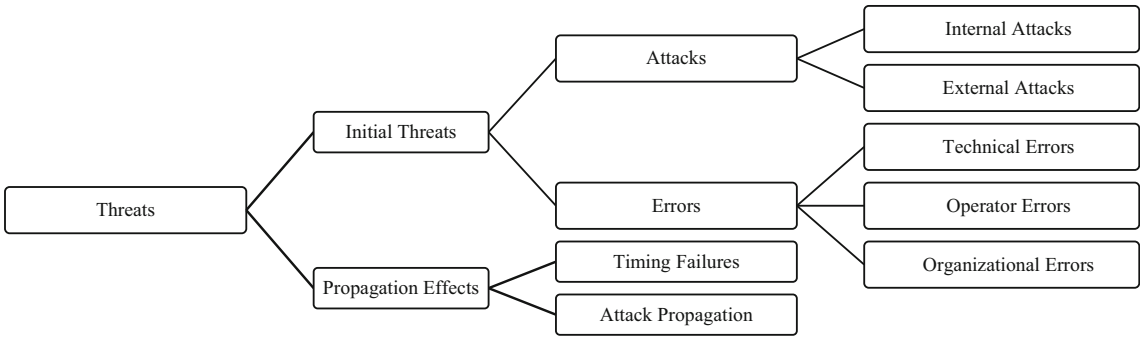


Fig. 3 Classification of threats in smart factories – own illustration

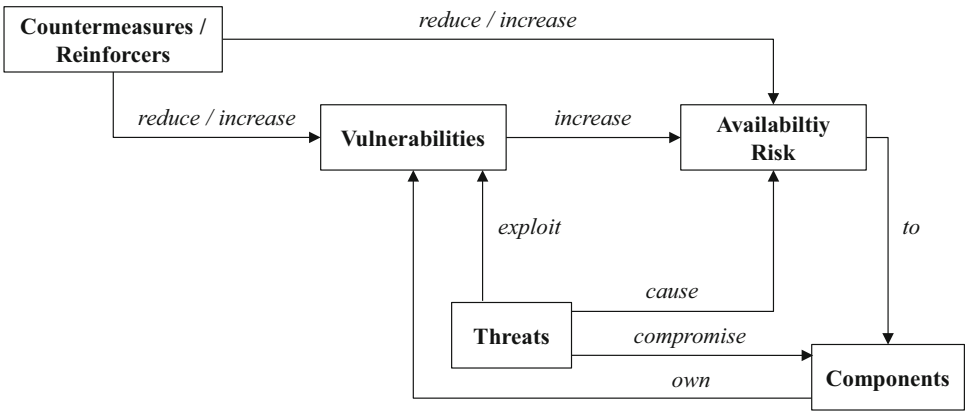


Fig. 4 Availability risk relations in smart factories – own illustration based on Common Criteria (2006) and Keller and König (2014)

increasing use of real-time information reinforce in particular the *vulnerabilities* of *components* in smart factory information networks.

Thereby, especially IoT and smart manufacturing technologies cause increased vulnerabilities and change requirements on IT security in smart factories (Wengert et al. 2016). 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*". Accordingly, "*the concept of Industry 4.0 generates new categories of risks […] because of the increase of vulnerabilities and threats*" (Tupa et al. 2017). Consequently, all components of the information network are critical as "*industrial control systems are becoming the target for malicious cyber intrusions*" (Wengert et al. 2016). For example, SCADA systems, that were initially designed to operate on closed networks, are increasingly based on cloud technology resulting in increased interconnectivity and, ultimately, vulnerability (Eden et al. 2017). Thus, "*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*" increasing potential points of failure (Wengert et al. 2016). Additionally, due to the highly interconnected structure of information networks in smart factories, the failure of a component can cause the failure of another component resulting in cascading failures (Amin et al. 2013). These cascading failures reinforce the initial failure and cause new threats that can lead to the loss of the operational capability of the entire information network (Danziger et al. 2016).

Despite the theoretical and practical relevance of cascading failures in smart factories, corresponding research remains insufficient until today and do not address the specific characteristics of information networks in smart factories. For instance, Zambon et al. (2011) developed a risk assessment method for business processes that considers the IT architecture and dependencies between IT components. Sathanur and Haglin (2016) introduce a *centrality measure* that indicates the influences of each node on the network by considering direct and indirect compromise through attack propagating. Amin et al. (2013) provide a framework for assessing security risks that can be caused by attacks or error based on a *game-theoretic* approach. However, these approaches only allow a static analysis and thus, neglect dynamic effects like cascading failures within information networks. Other research

analyses informational risks that exist in the context of supply chain networks and critical infrastructures. For instance, Wagner and Neshat (2010) develop an index to evaluate the vulnerability of supply chain processes to informational risks. However, they focus on a static analysis and do not explicitly consider propagation effects in smart factories. In addition, they analyze the vulnerability of the overall network and do not focus on the criticality of single components. Since propagation effects are interdependent and dynamic, Buldyrev et al. (2010) consider the spread of information risks within interdependent networks analyzing the criticality of nodes for network stability. Although this approach meets requirements like cascading failures, it does not take into account the characteristics of smart factory information networks like different component states. Thus, to the best of our knowledge, there is no appropriate approach for the modeling of smart factory information networks that considers adequately network structures, inherent dependencies, and cascading failures.

Therefore, in our approach, we consider cascading failures through two types of propagation effects, namely deterministic (i.e., timing failure) and stochastic effects (i.e., attack propagation). First, deterministic *timing failures* occur if a supporting component is not able to transmit necessary information to other dependent components within a specified time constraint. Second, after an attack successfully compromised a component (e.g., the memory of a production machine), the affected component can compromise other connected components within the information network, what we refer to as stochastic *attack propagation*. Further, we consider the error of components by means of stochastic *time to error* and the corresponding recovery of failed components by means of stochastic *time to recovery* that allows us to consider the resilience of smart factories within the modeling approach and the analysis of different security measures.

To determine whether an information network component is available and, thus, to determine the operational capability of smart factories, possible states of a component have to be defined (Arshad et al. 2006). Therefore, a component can exhibit only one state at a certain point in time in our modeling approach. Thus, our modeling approach considers time as discrete. For this, there is an absolute clock that defines a time line consisting of equidistant points in time. The time unit between two points in time can be defined depending on the application. For example, it seems reasonable to define it as 1 min in our application example as we do not consider a hard real-time constraint. In case of a hard real time constraint, for instance in case of critical safety properties of a system, it could also be defined as a millisecond or a second. Based on the described *threats* in smart factories, the following states of a component result: *operational (OP)*, *on hold (OH)*, *failed after attack (FA)*, and *failed after error (FE)*. As shown in Table 1, these states and the resulting availability of a component, are defined by two attributes: (1) *function executable*, which indicates whether a component is technically able to execute its function; and (2) *information accessible*, which indicates whether necessary information is accessible within a given (real-time) constraint.

We consider a component to be *operational* if it can execute its function and necessary information is accessible on time. In contrast, a component is *on hold* if it is technically able to execute its function, but necessary information is not accessible punctually (e.g., due to the failure of a supporting component). Further, attacks and errors can affect the operational capability of a component. In this case, a component is no longer able to execute its function and hence, exchange information with other components. In this case, it does not matter if necessary information is accessible as the component is not able to execute its function. According to the source of the failure, we distinguish between the states *failed after attack* and *failed after error*. We assume that a component is *available* if it exhibits the state $s \in \{OP\}$ and *unavailable* if it exhibits one of the other states $s \in \{OH, FA, FE\}$.

To apply appropriate countermeasures against IT availability risks, companies need to determine the state of each component. In particular, the resulting dynamic behavior of information networks (i.e., state changes initiated by threats) is of upmost importance and has to be captured. Thereby, both deterministic (e.g., *timing failures*) and stochastic (e.g., *attack propagation* or *time to error*) effects influence the dynamic behavior in different manners. For example, while deterministic timing failures occur after a predictable time span of a component's unavailability, the propagation of an attack depends on the underlying stochastic propagation probabilities. Hence, the consideration of both deterministic and stochastic effects is required. Therefore, we state the following design objective.

DO.3 *Threats:* To enable the analysis and comparability of different threats in smart factories, the modeling approach has to capture the characteristics of different threats and corresponding propagation effects.

2.3 Requirements for the Modeling Approach

Based on the described design objectives, we derive requirements for an adequate modeling approach. These have been discussed in the course of the conducted expert interviews and were confirmed by the experts. The requirements substantiate the design objectives and exemplify relevant characteristics that an adequate modeling

Table 1 Component states

State	Operational (OP)	On hold (OH)	Failed after attack (FA)	Failed after error (FE)
Function executable	Yes	Yes	No	No
Information accessible	Yes	No	Yes/no	Yes/no
Component available	Yes	No	No	No

approach has to exhibit. By means of the derived requirements, it is possible to evaluate the developed modeling approach regarding its suitability to answer the stated research question.

DO.1 *Graphical and formal representation*

- R.1 *Graphical notation:* To enable a visual and comprehensible depiction of the operational mode of the modeling approach, the modeling approach should provide a graphical notation.
- R.2 *Mathematical definition:* To enable the simulation of information networks and the analysis of failure propagation after attacks and errors (e.g., calculation of ITIL-Availability-Management-KPIs), the modeling approach should provide an exact mathematical definition.

DO.2 *Scalability*

- R.3 *Modeling module:* To enable the scalability of the approach and the comprehensible modeling of large information networks, the modeling approach should be able to depict an information network component as a generic modeling module.

DO.3 *Threats*

- R.4 *Operational states:* To enable the availability analysis of information networks, the modeling approach has to capture the component states (see Table 1).
- R.5 *Dynamic behavior:* To depict the dynamic behavior of information networks, the modeling approach has to capture propagations effects, i.e., the propagation of attacks and timing failures, in discrete time steps.
- R.6 *Stochastic behavior:* To depict the stochastic behavior of threats, the modeling approach has to consider the probability of a successful attack and its propagation as well as exponentially distributed timing aspects such as "*time to error*" and "*time to recovery*" after an error of a component occurs.

2.4 Methods for the Modeling and Analysis of Networks

Despite its high theoretical and practical relevance, research on the formal modeling of information networks in smart factories remains insufficient. Accordingly, the analysis and optimization of information networks regarding IT availability risks remain major challenges. In the following, we provide an overview of formal modeling approaches dealing with networks that are subject to random failures, cascading failures, and exogenous shocks in the context of supply chain and critical infrastructure networks as they may provide adequate starting points.

Graph theory represents a basis for the formal modeling of networks. Here, each actor of a network is represented by a node and dependencies between actors are represented as edges between two nodes (Wagner and Neshat 2010). For instance, Buldyrev et al. (2010), Faisal et al. (2007), and Wagner and Neshat (2010) use graph theory to identify and quantify risks in supply chains and critical infrastructure networks. Wagner and Neshat (2010) provide an index to measure the vulnerability of supply chains and Faisal et al. (2007) develop a framework to quantify information risks in supply chains based on graph theory. However, these approaches do not consider dynamic aspects and, thus, are not appropriate for the analysis of propagation effects in information networks of smart factories. In contrast, Buldyrev et al. (2010) develop a framework that considers the dynamics of cascading failures in interdependent networks. However, the approach only considers functional and non-functional states of network actors and neglects more detailed operational states. An extension of the graph theory is the *random graph* developed by Erdös and Rényi (1960)that combines graph theory and probability theory to analyze complex networks that are subject to random failures (Albert et al. 2000; Ash and Newth 2007; Gao et al. 2012). However, random graph approaches do not allow the depiction of given real-world information network structures as nodes are connected randomly (Gao et al. 2012). Altogether, the presented approaches focus on the analysis of the overall network and, hence, do not allow the fine granular identification and analysis of critical components, what is a prerequisite for the development of sensible countermeasures. Furthermore, PN enable the formal modeling of networks

considering dynamic and stochastic aspects (Arns et al. 2002). Wu et al. (2007) introduce the disruption analysis network (DA_NET) approach based on PN to model and quantify the propagation of disruptions in supply chains. Extending the DA_NET approach, Fridgen et al. (2014) provide a modular modeling approach that enables the simulation and quantification of exogenous shocks in supply networks considering dynamic and stochastic aspects. Although these approaches provide a solid foundation in modeling, they do not consider the peculiarities of information networks in smart factories (e.g., operational states, timing failures). However, there is also a growing number of scientific literature that deals with the description and quantification of security risks in smart factories (Amin et al. 2013; Broy et al. 2012; Cardenas et al. 2009; Sadeghi et al. (nd); Sathanur and Haglin 2016). For instance, based on a game-theoretic approach, Amin et al. (2013) provide a framework for assessing security risks to CPS that can be caused by security attacks or random errors. Sathanur and Haglin (2016) introduce a centrality measure for the assessment of vulnerability in CPS by considering direct compromise and indirect compromise through attack spread. However, these approaches neglect different operational states and important aspects such as dynamic behavior of propagation effects. Nevertheless, to enable the assessment of IT availability risks in a sensible manner, informational dependencies within information networks must be considered. To the best of our knowledge, there exists no formal modeling approach for the depiction of information networks in smart factories. Therefore, in this paper we focus on the modeling of information networks considering IT availability risks. Our approach enables the simulation of different information network settings and different threats in an integrated manner.

3 Modeling Approach Based on Petri Nets

To address the raised research question, we follow the guidelines for DSR from Hevner et al. (2004) and apply the DSR methodology from Peffers et al. (2007) to develop a modeling approach as design artifact (Offermann et al. 2010). Therefore, the DSR methodology (Peffers et al. 2007) suggests the following six activities for the development of artifacts: (1) identify problem; (2) define design objectives for solution; (3) design and develop; (4) demonstrate; (5) evaluate; and (6) communicate. Step 1 was already addressed in Sect. 1 by highlighting the relevance of formalized modeling approaches for the depiction and simulation of information networks in smart factories. In Sect. 2, we deduced design objectives for our artifact as well as requirements for the modeling approach (step 2) to ensure that our artifact helps to solve the research question. In this section, we start with the design and development of our artifact (step 3).

We base our modeling approach on PN that were developed by Carl Adam Petri (1962) as PN fulfill the postulated requirements (cf. sect. 2). PN provide an intuitive *graphical notation* as well as a *formal notation* enabling the mathematical analysis of information networks (van der Aalst 1998), fulfilling requirements *R.1* and *R.2*. As existing PN approaches do not consider specific characteristics of smart factory information networks, we build on different PN approaches as a basis for the development of our modeling approach under consideration of the possessed requirements. First, to handle the complexity of large information networks and to enhance practicability, we adapt the concept of modularization developed for supply chains (Fridgen et al. 2014) fulfilling requirement *R.3*. Further, as PN consist of passive places and active transitions that symbolize *states* and *actions* (i.e., *state changes*), respectively, they fulfill requirement *R.4*. To cover *dynamic behavior*, firing delays are associated to transitions, specifying the duration of activities (Murata 1989). Several concepts regarding firing delays can be distinguished. For instance, Ramchandani (1974) developed *timed Petri nets* that associate a deterministic firing delay to each transition. Merlin (1974) introduced *time Petri nets (TPN)* that use time intervals to describe lower and upper bounds for the duration of activities. In *stochastic Petri nets (SPN)*, an exponentially distributed firing delay is assigned to transitions (Molloy 1981). Further, Marsan et al. (1984) introduced *generalized stochastic Petri nets (GSPN)* that consider immediate transitions (zero firing delay) as well as timed transitions (exponentially distributed firing delay) extending SPN. Regarding requirement *R.5*, we adapt the GSPN approach by Marsan et al. (1984) using immediate and timed transitions to capture the *dynamic behavior* (e.g., propagation of attacks and timing failures) of information networks. Thereby, the timing requires preselection rules for transitions that come into conflict when multiple transitions share input places and can fire at the same point in time competing for the same token. The preselection of transitions can be performed, beside others, deterministically with *priorities* or randomly with *probabilities* (Balbo and Silva 1998). Necessary information for the parametrization of priority values could be gathered from technical data sheets of IT components and system specifications. To depict *stochastic events* (e.g., attacks on specific components), probabilities can be assigned to transitions fulfilling requirement *R.6*. Thereby, probability values for attacks can be derived from official statistics (e.g., from the European Union Agency for Network and Information Security – ENISA Threat Landscape Report). The obtained values could be adjusted

based on expert's expectations (e.g., regarding the development of the number of attacks) or individual internal measurements (e.g., the installation of a new cyber security system). Regarding internal errors, internal incident reports can be the basis for the estimation of appropriate probability values. Moreover, to depict timing failures between dependent components, we adapt the idea of guard functions from *colored Petri nets (CPN)* (Jensen 1991). Accordingly, considering the aforementioned requirements R.1 to R.6, we use GSPN with immediate and exponentially distributed firing times and enhance the GSPN with deterministic and stochastic preselection of transitions as well as guard functions to fulfill the derived requirements. This enables the consideration of specific characteristics of smart factory information networks such as the dynamic behavior, i.e., propagation effects and timing failures within the information network.

3.1 Mathematical Specification

In this subsection, we briefly describe the basic functioning of PN and specify the mathematical definition of our modeling approach. PN are defined as bipartite graphs consisting of places, transitions, and arcs. If places additionally carry tokens, PN are called "*marked PN*". The current state of a PN is specified by its marking, i.e., the number of tokens on each place. The PN changes its state by the enabling of transitions which remove tokens from input places and create tokens on output places. A detailed explanation and functional description of PN can be found by Murata (1989).

To describe the information network by means of our modeling approach in a formalized way, there is a finite set of places $P = \bigcup_{i=1}^{m} \{p_i\} = \{p_1, \ldots, p_m\}$.[1] Further, there is a finite set of transitions $T = \bigcup_{j=1}^{n} \{t_j\} = \{t_1, \ldots, t_n\}$, consisting of immediate and timed transitions. These include timed transitions with different timing requirements like the special case of real-time constraints or other timing requirements (for instance, for repair times), as well as transitions without timing specifications defining pure YES/NO decisions (for instance, transitions that determine whether a component is affected by an attack or not). Arcs are divided into two finite sets of directed arcs: the input matrix $I \subseteq (P \times T)$ defines arcs from places to transitions, whereas the output matrix $O \subseteq (T \times P)$ defines arcs from transitions to places. The binary variables $I_{i,j}$ and $O_{i,j}$ equal 1 if there exists a directed arc from place p_i to transition t_j or from transition t_j to place p_i, respectively. Otherwise, $I_{i,j}$ and $O_{i,j}$ equal 0. The entries of the input and output matrices are determined by the structure of the information network. The resulting incidence matrix A is calculated by equation (Eq.) 1:

$$\boldsymbol{A} = \boldsymbol{O} - \boldsymbol{I} \tag{1}$$

The marking vector $M^h = \left[M^h(p_1); \ldots; M^h(p_m)\right]$, contains for each point in time h with $h \in \{0, \ldots, H\}$ the number of tokens on each place p_i, where M^0 indicates the initial marking vector. If there is more than one transition requiring the same input token from a common input place at h, there is a conflict. The conflict resolution type vector $CR = [cr_1; \ldots; cr_m]$ assigns each place p_i its type of conflict resolution determining whether a conflict is resolved by priority $(cr_i = 0)$ or probability $(cr_i = 1)$.. According to the conflict resolution type, the conflict parameter vector $CP = [cp_1; \ldots; cp_n]$ assigns each transition t_j a specific priority or probability, respectively. Further, the guard function vector $G^h = \left[g^h(t_1); \ldots; g^h(t_n)\right]$ with $g^h(t_j) \in \{true, false\}$ assigns each transition t_j additional enabling conditions. Therefore, a transition t_j is enabled if (1) each input place contains enough tokens and (2) the enabling conditions of the assigned guard function $G^h(t_j)$ are fulfilled, i.e. $g^h(t_j) = true$. Hence, the enabling vector $E^h = \left[e^h(t_1); \ldots; e^h(t_n)\right]$ with $e^h(t_j) \in \{0, 1\}$ determines whether a transition t_j is enabled at point in time h. The transition type vector $TT = [tt_1; \ldots; tt_n]$ determines whether a transition is an immediate $(tt_j = 0)$ or timed $(tt_j = 1)$ transtion. Further, the fire rate vector $FR = [fr_1; \ldots; fr_n]$ specifies the firing rate determining the firing delay of timed transitions. Whenever a timed transition is enabled, a random firing delay is assigned to it. With every time step, the firing delay decreases. Once the firing delay equals zero the transition fires. Therefore, the firing vector $F^h = \left[f^h(t_1); \ldots; f^h(t_n)\right]$ with $f^h(t_j) \in \{0, 1\}$ determines whether a transition t_j fires at h. Thereby, the marking of the next point in time $h + 1$ is calculated by Eq. 2:

$$\boldsymbol{M^{h+1}} = \boldsymbol{M^h} + \boldsymbol{A} \cdot \boldsymbol{F^h} \tag{2}$$

As the information network is composed of several components, we define a set of components $C = \bigcup_{k=1}^{o} \{c_k\} = \{c_1, \ldots, c_o\}$. For example, and in reference to Fig. 2, a set of components can include, but is not limited to, servers, cloud-based or on-premise hosted IT services, data storage, external interfaces, and sensors, actuators, and embedded systems of smart production machines. Each component c_k is described by a subset of places $P_c \subseteq P$ and a subset of transitions $T_c \subseteq T$ (Vladimir 2011). To depict timing failures and, hence, informational dependencies between components, the *unavailability* of a component c_k at a certain point in time h and the *maximum acceptable interruption time* between two components c_k and $c_{\hat{k}}$ are required. For this, the unavailability of a

[1] **Table A.1** in the online appendix provides an overview of the nomenclature of our PN specification (available online via http://springerlink.com).

component, that represents the duration of a component's unavailability, is depicted by matrix $U^h = [u^h(c_1); \ldots; u^h(c_o)]$ with $u^h(c_1) \in \mathbb{N}_0$ and the *maximum acceptable interruption time* is depicted by matrix L with $L_{k,\hat{k}} \in \mathbb{N}$.

4 Modeling Procedure

In this section, we illustrate our modeling procedure for answering our research question. Following Simon (1996), we conducted several generate-and-test cycles during the design process to derive an appropriate approach fulfilling the derived design objectives and requirements. To depict components and their interdependencies, we develop a modeling module representing one essential artifact of our research. Thereby, each component c_k is illustrated by a modeling module, framed by a rounded rectangle as shown in Fig. 5.

A modeling module consists of six places (p_1 to p_6) and seven transitions (t_1 to t_7). The *state* places p_1 to p_4 (white circles) represent the current state $s \in \{OP, OH, FA, FE\}$ of a component. The *operational* state, for instance, is represented by one token on place p_1, summarized by the marking vector of the state places $M^h = [1; 0; 0; 0; 0; 0]$. Figure 6 shows all states a component can exhibit and their depiction by our modeling module. The *on hold* state is defined by a token on the places p_1 and p_2. Further, the *failed after error* and the *failed after attack* states are depicted by a token on place p_3 or place p_4, respectively.

The structure of complex information networks can be built up by means of the modeling modules. Therefore, the modeling modules can interact with each other via *interface* places (striped circles) that are positioned on the borderlines of the module, as well as via guard functions that are assigned to transitions. The *input interface place* (IIP) p_5 and the *output interface place* (OIP) p_6 facilitate the depiction of attacks and attack propagation within the information network by connecting components according to information flows between them. The guard functions depict if required information is available within a given

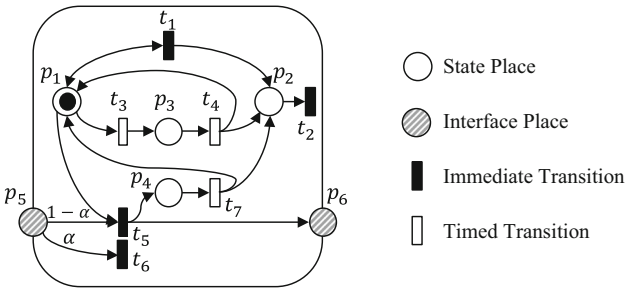


Fig. 5 Modeling of an information network component

time. As seen in Fig. 5, four immediate transitions (black rectangles) depict whether there is a timing failure or not (t_1 and t_2), or whether an attack harms a component or not (t_5 and t_6). Moreover, three timed transitions (white rectangles) depict the *time to error* (t_3) as well as the *time to recover* after an error or attack (t_4 and t_7). Thereby, the *time to error* represents the assumed time span between errors, i.e., the time between the occurrences of two errors. The *time to error* can be assessed based on historical data regarding the number of errors in a certain interval. The *time to recovery* includes both the predicted times for detection and repair of a failure after an error or attack. Taking the *operational* state as a starting point, we describe in the following how (1) timing failures, (2) errors, and (3) attacks as well as their propagation within the information network are depicted in our modeling approach.

The **timing failure model** is depicted by means of the state places p_1 (for status *OP)* and p_2 (for status *OH*), the transitions t_1 and t_2, and the assigned guard functions $G^h(t_1)$ and $G^h(t_2)$. Thereby, the guard functions monitor whether the unavailability $U^h(c_k)$ of other components exceeds the maximum acceptable interruption time $L_{k,\hat{k}}$ (cf. Fig. 7).

To demonstrate the timing failure mechanism, we consider an example consisting of two components c_1 and c_2. Component c_2 (e.g., a sensor) supports component c_1 (e.g., an embedded system) with necessary information. Hence, the operational capability of component c_1 depends on the information transmitted by component c_2 in real-time. Figure 6 shows the subsequent states of component c_1. The guard function $G^h(t_1)$ is *true* if the unavailability of component c_2 exceeds the maximum acceptable interruption time (e.g., due to a technical defect) enabling transition t_1 of component c_1 (step 1/ h = 1). Subsequently, transition t_1 fires and an additional token is created on place p_2 changing the state of component c_1 from *operational* to *on hold* (step 2/ h = 27). As there is both an arc from p_1 to t_1 and from t_1 to p_1, the marking of place p_1 after firing is the same. Once component c_2 is recovered and its unavailability is less than the maximum acceptable interruption time, guard function $G^h(t_2)$ of component c_1 is *true*, enabling transition t_2. The firing of transition t_2 only consumes the token on place p_2 as transition t_2 is a sink transition without outgoing arcs (step 3/ h = 43). Therefore, the state of component c_1 changes from *on hold* back to *operational*.

Moreover, the **error model** enables the consideration of randomly occurring errors such as technical defects or erroneous entry of data by operators and their effects on the operational capability of the smart factory. For this, the error model comprises a sequence of the three states

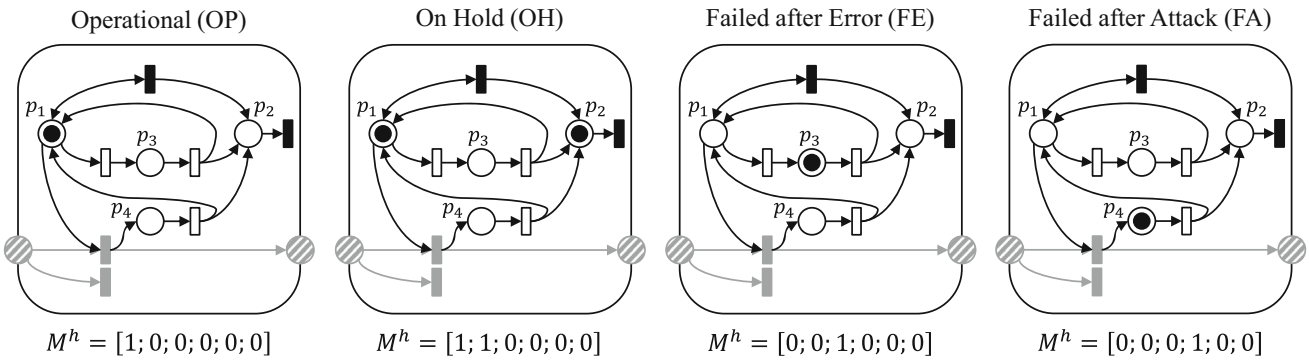


Fig. 6 Component states depicted in the model

operational, failed after error, and *on hold* as shown in Fig. 8.

The exponentially distributed firing delays of the error sequence are described by the error rate λ_E and the error recovery rate λ_{ER}. These fire rates define the stochastic *time to error* (e.g., TTE = 25) and *time to recovery* (e.g., TTR = 10) that are associated to the timed transitions t_3 and t_4. The information about their parametrization is available through sources such as maintenance information of manufacturers, and hence, can be assessed and applied as exogenous input parameters to our model. After the assigned *time to error* elapsed, transition t_3 fires, representing the occurrence of an error of the component (step 1/ $h = 1$). Therefore, transition t_3 consumes the token on place p_1 and creates a token on place p_3 changing the state of the component from *operational* to *failed after error* (step 2/ $h = 26$). Subsequently, transition t_4 is enabled and the random firing delay *time to recovery* is assigned to it. Once the *time to recovery* is elapsed and the component is recovered, transition 4 fires and the component exhibits the *on hold* state (step 3/ $h = 36$). In this state, the component monitors whether all necessary information from supporting components is accessible. Once all necessary information is accessible, the component's state switches back to *operational* (step 4/ $h = 37$), otherwise the component stays *on hold* (see *timing failure model* described above).

Finally, the **attack model** includes the three states *operational, failed after attack*, and *on hold* as well as the IIP p_5 and OIP p_6 as shown in Fig. 9.

The occurrence of an attack is represented by the presence of a token on the IIP p_5 enabling both transitions t_5 and t_6 (step $1/h = 1$). Whether an attack is successful (t_5 fires) or not successful (t_6 fires) is determined randomly according to the assigned probabilities $1 - \alpha$ and α, respectively. Hence, the parameter α can be interpreted as a measure for the security level of components. If an attack is *not* successful, transition t_6 consumes the token on IIP p_5 and the component remains in the *operational* state (step 2a/ $h = 2$). In contrast, if the attack is successful, transition t_5 consumes the tokens on the state places p_1 and IIP p_5 and creates a token on the state place p_4 and OIP p_6 (step 2b/ $h = 2$). The token on the state place p_4 initiates the recovery of the component and the token on OIP p_6 depicts the attack propagation to other, connected components. Subsequently, transition t_7 is enabled and the attack recovery rate λ_{AR} defines the stochastic *time to recovery* (e.g., TTR = 10) assigned to transition t_7. Once the *time to recovery* is elapsed and the component is recovered, the component switches to the *on hold* state (step 3/ $h = 12$) and monitors whether all necessary information from supporting components are accessible (see the *timing failure model* described above). Finally, the component is in the *operational* state again/step 4/ $h = 13$).

As shown in Fig. 10, the **attack propagation** is depicted by the OIP and IIP on the borderlines of the modeling modules. We apply the idea of fusion of places as described by Murata (1989), where the OIP of component c_1 and the corresponding IIP oFf component c_2 are represented by the same place p_i. Hence, if an attack is successful and a token is created on the OIP of component c_1 there is also a token on the corresponding IIP of component c_2 enabling the above-described attack model. Moreover, if a component is connected to more than one other component, the number of OIPs within a modeling module can be expanded to an arbitrary number as indicated in component c_2 (cf. Fig. 10).

Further, to represent the stochastic occurrence of attacks and to simulate the expected number of attacks in a certain time interval, we adopt a **shock module** as introduced by Fridgen et al. (2014). The shock module shown in Fig. 11 comprises one transition t_1 and one or multiple OIPs. Transition t_1 is a source transition (i.e., without input places) and, thus, is always enabled. The attack rate λ_A defines the random firing delay *time to attack* that is associated with transition t_1. After the firing delay elapsed, transition t_1 fires and creates a token on the OIP representing the occurrence of an attack. Thereby, one OIP of the shock module is connected to one IIP of a modeling module. To

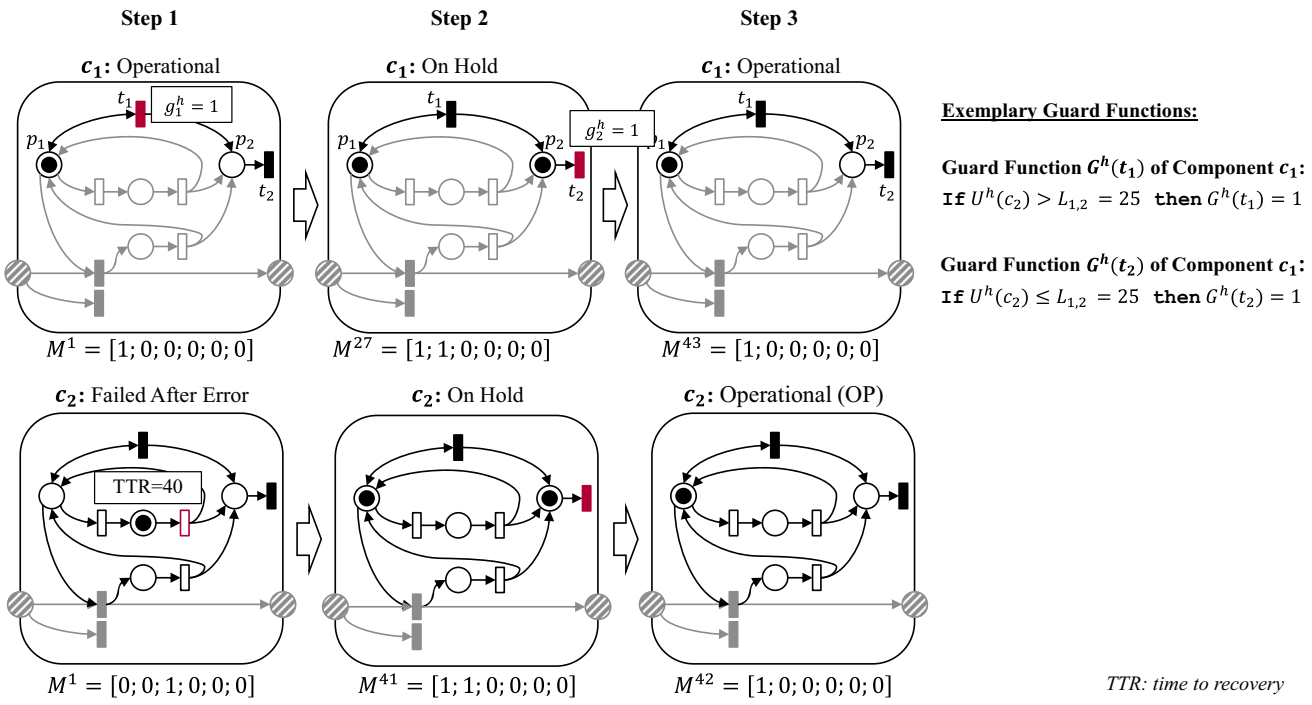


Fig. 7 Timing failure sequence

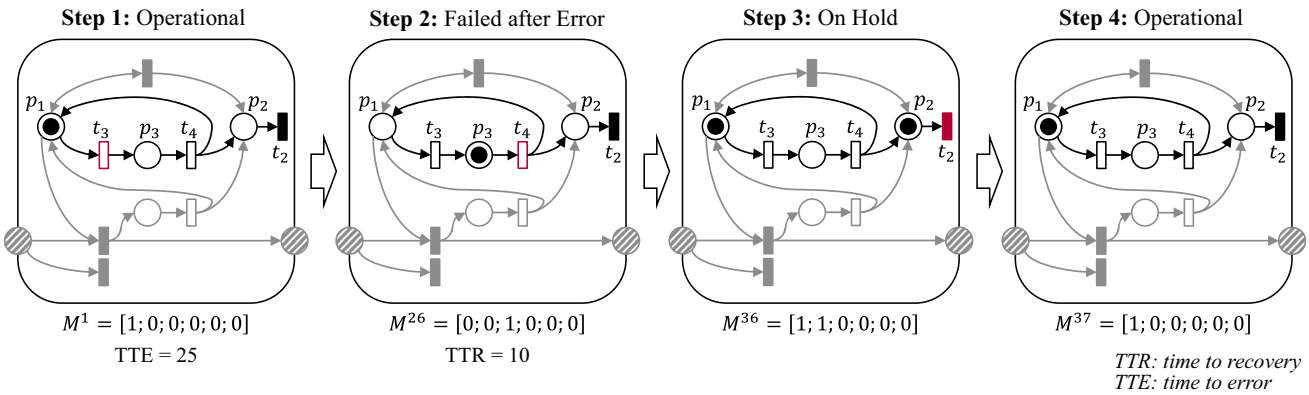


Fig. 8 Error sequence

depict simultaneous attacks (Amin et al. 2013) the number of OIPs within the shock module can be expanded analogously to the modeling module (cf. Fig. 11).

5 Evaluation

Following Sonnenberg and vom Brocke (2012), within this section, we demonstrate and evaluate the feasibility and applicability of our modeling approach. For this purpose, they propose a combination of ex-ante and ex-post evaluation activities (Eval1 to Eval4) in artificial and naturalistic environments. Thereby, Eval1 requires the presentation of the research topic as a meaningful DSR problem and the formulation of design objectives. Eval2 validates the design specification against the postulated design objectives. Eval3 aims to validate the feasibility of a prototype in an artificial setting. Finally, Eval4 serves the purpose of validating the applicability of the developed artifact from a naturalistic perspective.

We already conducted Eval1 activity in Sects. 1 and 2 by identifying the need for a formalized approach for the modeling of information networks in smart factories. Sections 3 and 4 described the logical reasoning of our artifact, the modeling approach.

In Sect. 5.1, we validate the design specification against the possessed design objectives and requirements from the literature by means of a feature comparison. Further, in

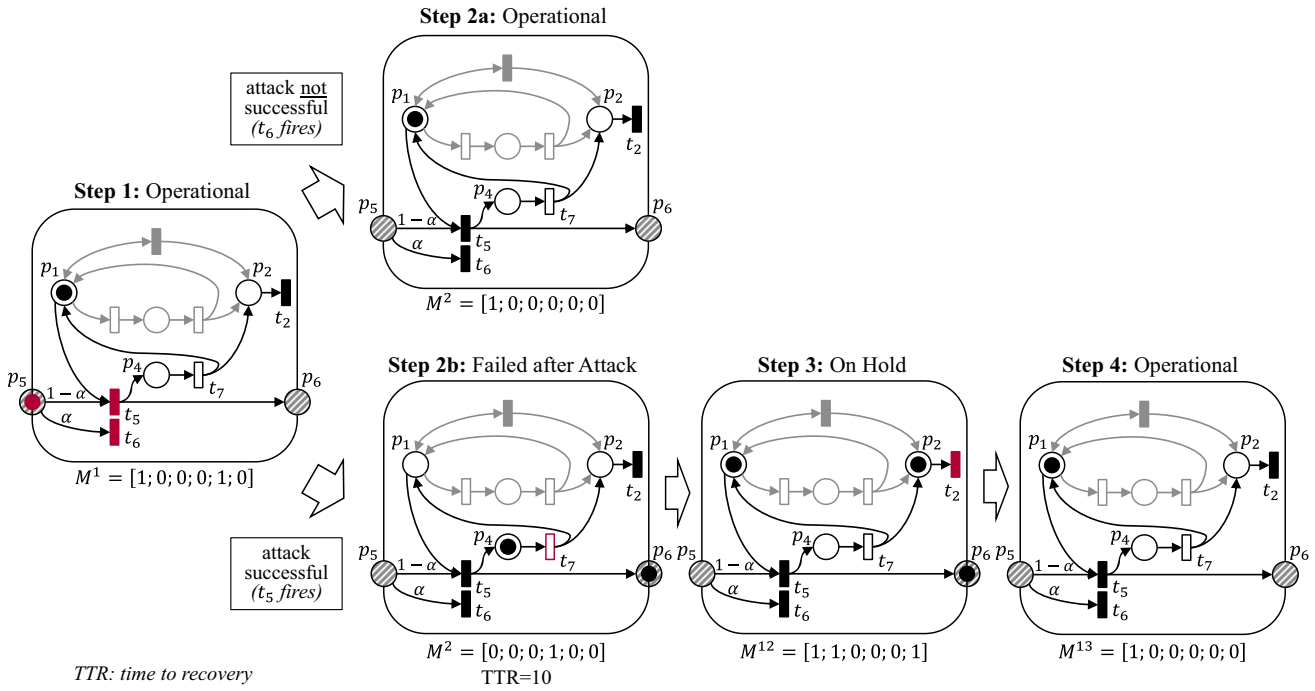
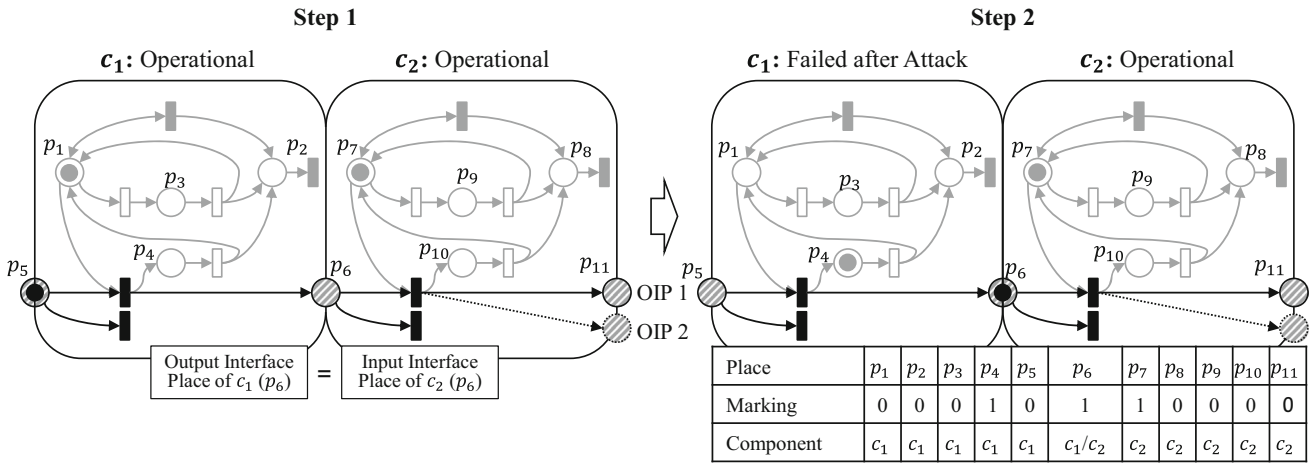


Fig. 9 Attack sequence

Sect. 5.2, we simulate an exemplary information network based on a real-world setting in an artificial setting (Eval3) to demonstrate the feasibility of our modeling approach and to show that our artifact behaves as intended for single test cases (Sonnenberg and Vom Brocke 2012). In Sect. 5.3, we apply key figures that are based on the data generated by our modeling approach to demonstrate its usefulness for the analysis of an information network, its interdependencies, and the propagation behavior of failures over time. Finally, to validate the modeling approach from a naturalistic perspective (Eval4), we interview experts from two leading global companies in the automation and flexible packaging sector and an academic PN expert (cf. Sect. 5.4).

5.1 Feature Comparison

In Sect. 2, we derived design objectives for the development of our modeling approach. We compare these design objectives with the design specifications of our developed modeling approach to validate whether our developed artifact fulfills these design objectives (Venable et al. 2012).



Place	p_1	p_2	p_3	p_4	p_5	p_6	p_7	p_8	p_9	p_{10}	p_{11}
Marking	0	0	0	1	0	1	1	0	0	0	0
Component	c_1	c_1	c_1	c_1	c_1	c_1/c_2	c_2	c_2	c_2	c_2	c_2

Fig. 10 Attack propagation sequence

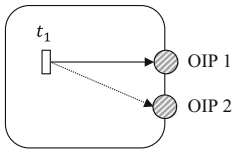


Fig. 11 Structure of a shock module

DO.1 *Graphical and formal representation:* Our modeling approach is based on PN providing both a graphical representation of modeling modules and a formal representation of information networks. Owing to the exact mathematical definition of PN, it is possible to convert information networks into mathematical equations enabling computer-based simulations of complex real-world settings.

DO.2 *Scalability:* Our modeling approach depicts the information network as a multitude of single modeling modules and dependencies between them. This modularization enables the modeling of information networks of different sizes and compositions.

DO.3 *Threats:* Our modeling approach provides the possibility to model and simulate different threats (intentional attacks via virus attacks and technical errors) as well as associated propagation effects (attack and timing failure propagation) (cf. sect. 4).

Based on this design objective comparison, we can state that our developed modeling approach fulfills all design objectives derived in Sect. 2.

5.2 Simulation Based Analysis of an Exemplary Information Network

To demonstrate the feasibility of our modeling approach, we simulate an exemplary information network that is based on a real-world setting oriented on a matrix production principle of a leading robotics manufacturer (cf. Fig. 12) and that is affected by different threats. For this, we model the information network of a production environment consisting of five robotic cells that are a section of a larger smart factory.

The information network consists of 211 components (modeling modules) containing servers, IT services, data storage, external interfaces, embedded systems, sensors, and actuators. The exemplary setting is based on a real-world setting of one of the leading robotic manufacturers with its matrix organized production concept for customers for the production of industrial goods and, thus, is geared toward a close-to-reality production infrastructure. There are five robotic cells equipped with four industrial robots on the shop floor of the smart factory. Each industrial robot embraces one embedded system, three sensors (e.g., temperature or ultrasonic sensor), and six actuators (six axis robots) to flexibly perform production tasks. The embedded systems, sensors, and actuators are modeled as components of the information network. Embedded systems control sensors and actuators as well as exchange production and machine data between industrial robots, IT services, and data storage. According to real-time requirements and data volumes, IT services and data storage can be hosted either on on-premise servers (e.g., MES, ERP) or via external interfaces in the cloud (e.g., big data analytics). Thereby, the MES and ERP applications perform traditional production tasks (e.g., production planning and control), whereas big data applications analyze production and machine data to predict, for instance, productivity, quality, and maintenance jobs. Based on these analyses, big data applications give MES and ERP applications feedback to optimize production processes. Further, we assume that a failure of the on-premise server (hosting MES and ERP

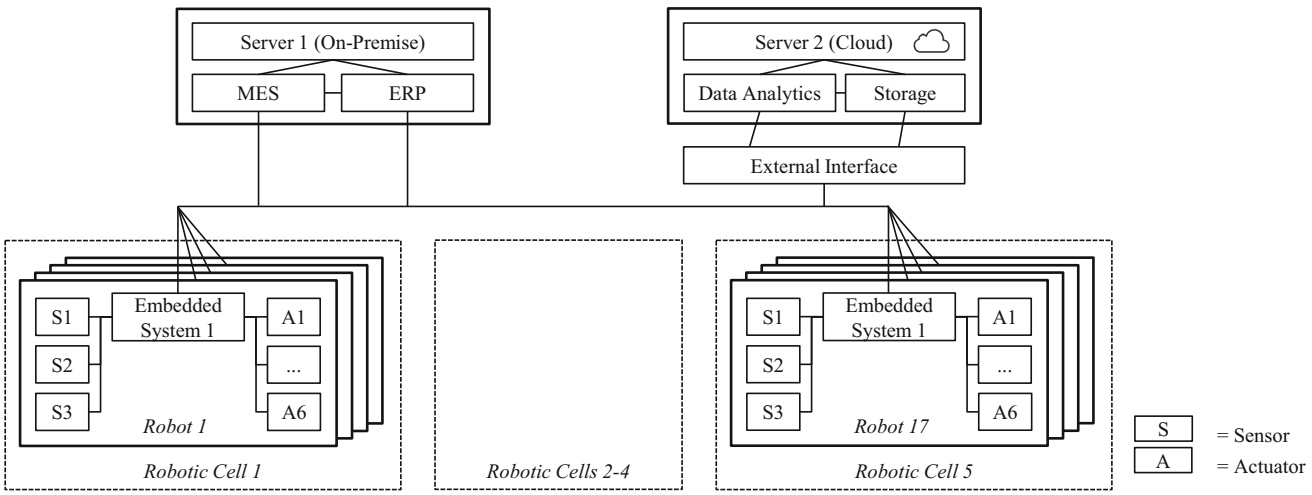


Fig. 12 Exemplary smart factory information network

Table 2 Scenario specifications

	Scenario 1 – attack		Scenario 2 – error	
	Case 1A	Case 1B	Case 2A	Case 2B
Number of simulation runs	1000			
Number of points in time	100			
Number of components	211			
Error rate (λ_E)	0.0001	0.0001	0.0001	0.0001
Error recovery rate (λ_{ER})	0.01	0.01	0.01	0.1
Security level α	0.90	0.99	0.90	0.90

applications) can lead to a standstill of the entire smart factory due to missing necessary information of the MES and ERP. In contrast, a failure of the cloud server (hosting big data applications) affects only the ability of the smart factory to optimize production flows, but the operational capability of production remains unaffected.

Taken this initial setting, we consider two scenarios (i.e., *Scenario 1 – Attack* and *Scenario 2 – Error*) to demonstrate and analyze the impact of different threats on the operational capability of the information network by using the unavailability rate as a measure for the impact of failures. The simulations are based on the following specifications (see Table 2).

We developed an application using MATLAB, which allows us to design, simulate, and analyze generalized stochastic nets. Our application considers immediate and timed transitions. Timed transitions can be deterministic or stochastic. Furthermore, priorities or probabilities can be assigned to conflicting transitions. We use this application to simulate and analyze the information network modeled by means of our PN approach.

We conduct 1000 simulation runs for each scenario. In each simulation run, we observe a time frame of 100 points in time and the states of 211 components of the smart factory information network (see Fig. 12) resulting in 21,100 states. For all simulation runs we define that the start marking was the same (i.e., all of the 211 components are in the state "*operational*"). However, the stochastic effects of the threat events (e.g., probability of a successful attack or the exponentially distributed *time to error*) lead to different results in each simulation run. Thereby, the error failure rate as well as the error and attack recovery rates of all components are set to $\lambda_E = 0.0001$ and $\lambda_{ER} = \lambda_{AR} = 0.01$, meaning that errors occur in one out of 10,000 points in time and that recovery after errors and attacks takes about 100 points in time. Both information are based on technical specifications of IT components and can be gathered from technical data sheets. The maximum acceptable interruption time $L_{k,\hat{k}}$ between components within a robotic cl is set to one (real-time requirement), between robotic cells to 20 points in time, and between IT services and embedded systems to 60 points in time. Further, the $L_{k,\hat{k}}$. between servers and IT services is also set to one depicting functional dependencies.

In **Scenario 1 – Attack**, we assume an adversary that performs a coordinated cyber-attack on all embedded systems of robotic cell 1 via the internet (e.g., via a remote maintenance channel). Thereby, a successful attack can compromise other, directly connected components (e.g., sensors, IT services) according to their security level. First, we assume that the embedded systems run an out-of-date firmware and hence, offer a security level of only 90%. After installing a security update, the security level increases to 99%. Comparing the two security levels, the unavailability rate decreases from 30 to 1% (see Fig. 13). The results indicate that an increased security level dramatically reduces the unavailability rate and, therefore, the impact of an adversary on the operational capability of the information network.

In **Scenario 2 – Error**, we consider a technical defect of the on-premise server leading to failures of the MES and ERP applications. To demonstrate how timing failures affect the operational capability of the smart factory, we analyze different recovery rates of the on-premise server.

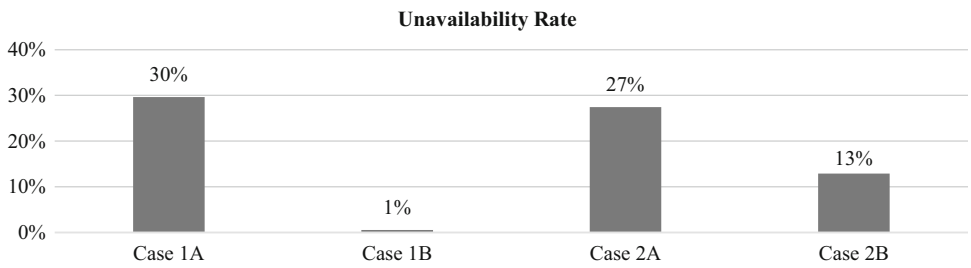


Fig. 13 Simulation results: Unavailability rates for scenario 1 – attack and scenario 2 – error

Table 3 Component states and corresponding state vectors

States	Operational (OP)	On hold (OH)	Failed after attack (FA)	Failed after error (FE)
Function executable	Yes	Yes	No	No
Information accessible	Yes	No	Yes or no	Yes or no
State vector $v^b_{c_k,h}$	$v^b_{c_k,h} = [1;0;0;0]$	$v^b_{c_k,h} = [0;1;0;0]$	$v^b_{c_k,h} = [0;0;1;0]$	$v^b_{c_k,h} = [0;0;0;1]$

First, we assume a recovery time defined by the recovery rate $\lambda_{ER} = 0.01$. After improving the recovery process and fault diagnosis (e.g., by the use of augmented reality) the recovery time decreases ($\lambda_{ER} = 0.1$). Thereby, the unavailability rate decreases from 27 to 13% (see Fig. 13). The results indicate that an improved recovery rate reduces the unavailability rate and, hence, the impact of an error of the on-premise server on the information network.

In summary, the results of the scenario simulation indicate the applicability of the modeling approach to a production environment that is close to real world. In addition, the simulation results demonstrate the application possibilities of our approach for deriving suitable security and prevention measures. Of course, the size of the modeled information network is limited and information networks of smart factories in practice are far more complex because they consist of considerably more components. Nevertheless, the application of our modeling approach to a close-to-real-world scenario within the simulation and its results demonstrate that our approach is principally suitable for more complex scenarios due to the modular structure of our modeling approach. Further, the application demonstrates that there is a need for an adequate modeling approach that enables detailed analysis of IT availability risks (cf. sect. 5.3).

5.3 Application of Key Figures

Besides the simulation results described in Sect. 5.2, the data regarding the components' states and their operational capability (ref. Table 1) generated by the simulation can be used to analyze the information network, its interdependencies, and the propagation behavior of failures over time in more detail. The development of corresponding key figures that are calculated on the basis of the generated data seems promising to support the identification of critical components. Although the elaborated development of such key figures is subject to further research (source left blind due to double-blind review), we briefly describe two potential key figures that can be derived from our approach.

For this, the current state $s \in \{OP, OH, FA, FE\}$ of each component at h is depicted by the state vector $v^b_{c_k,h} = [b^{OP}_{c_k,h}; b^{OH}_{c_k,h}; b^{FA}_{c_k,h}; b^{FE}_{c_k,h}]$, where $b^s_{c_k,h}$ represents a binary variable that takes the value 1 if component c_k is in state s at h, else 0. By means of the state vector $v^b_{c_k,h}$, the state of each component is defined clearly for each point in time h. Table 3 provides an overview over the states, their attributes, and the associated state vector.

Based on the state vector, we develop the key figures *availability* and *operational availability* to analyze the smart factory's information network regarding its operational capability after an attack or error:

Dynamic key figure "Availability": *The availability of the information network $AV_h(\widehat{M}, \widehat{h})$ measures the share of components that are able to provide their function ($s \in \{OP, OH\}$) at h considering that a subset $\widehat{M}$ of the components initially fails[2] at $\widehat{h}$ due to an attack or error (see Eq. 3).*

Dynamic key figure "Operational availability": *The operational availability of the information network $opAV_h(\widehat{M}, \widehat{h})$ measures the share of components that are able to provide their function and access necessary information ($s \in \{OP\}$) at h considering that a subset $\widehat{M}$ of the components initially fails at $\widehat{h}$ due to an attack or error (see Eq. 4).*

$$AV_h((\widehat{M}, \widehat{h}) = \frac{\sum_{c=1}^{C} b^{OP}_{c_k,h} + \sum_{c=1}^{C} b^{OH}_{c_k,h}}{C} \tag{3}$$

$$opAV_h((\widehat{M}, \widehat{h})) = \frac{\sum_{c=1}^{C} b^{OP}_{c_k,h}}{C} \tag{4}$$

To calculate the two key figures, the values of the state vectors obtained from the marking vector resulting from the simulation and fulfilling the respective criteria (for Eq. 3 $s \in \{OP, OH\}$, for Eq. 4 $s \in \{OP\}$) are summed up. By means of the distinction between *availability* and *operational availability*, the information network and its components can be analysed regarding their operational capabilities as well as their informational dependencies to identify critical components. Whereas traditional availability key figures often only cover whether a system is in a functioning condition or not, our approach enables a detailed depiction of four different relevant states. This enables the determination of the extent of non-availability of components that results solely from informational

[2] $\widehat{M}$ is a subset of N ($\widehat{M} \subseteq N$) consisting of one or multiple components (e.g., in case of common cause failures or synchronized attacks) and representing the initial trigger of failures.

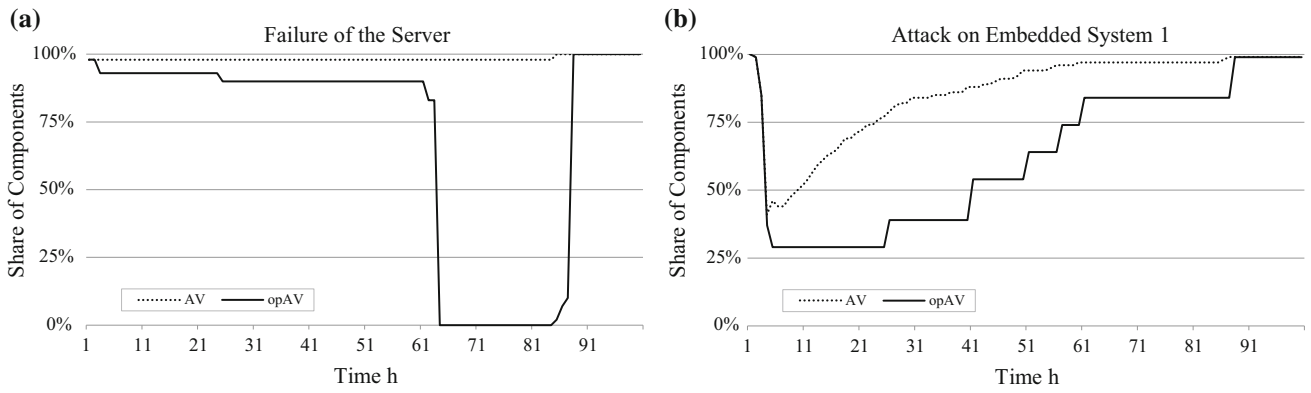


Fig. 14 Illustration of AV and opAV after failure (**a**) and attack (**b**) for an exemplary simulation run

dependencies. They can be applied to analyze an entire information network, a subnetwork, or selected components. Thus, the key figures support the improvement of already existing information networks through targeted security measures as well as the development of a sensible design and configuration of new information networks.

To demonstrate the application of the key figures, Fig. 14 contains the exemplary course of a worst-case simulation run of two different scenarios that resulted both in a significant non-availability of IT components and, thus, a restriction of the production system. For this analysis, we selected two worst-case courses among the generated simulation runs. The worst-case courses show different effects on the information network: (a) a failure of the server (e.g., caused by an incorrect software update) and (b) an attack on one embedded system that can compromise other directly connected components with a given probability.

As shown in Fig. 14a, the *availability* in scenario (a) drops to 98% and remains constantly at this level after the failure of the server at $h = 1$. However, the *operational availability* considerably decreases stepwise, as IT services depend functionally on the server. Consequently, controllers (drop 2 in Fig. 14a), embedded systems, and all dependent sensors and actuators (drop 3 and 4 in Fig. 14a) exhibit the *OH* state due to missing information, resulting in a standstill of the entire smart factory. After the server is repaired, all components restore their operational capability and change their state from *OH* to *OP* as necessary information is accessible, again. Finally, the entire smart factory is restored and fully functional. This worst-case scenario illustrates that a failure of central components, i.e., the server, leads to an inoperability of the entire smart factory and, thus, a significant economic damage.

As shown in Fig. 14b, the attack on the embedded system causes a rapid drop of the components' *availability* to 41%. The rapid drop can be explained by the spread to directly connected components leading to a functional incapacity of these components, too. Thereby, the *operational availability* decreases to 30% as missing information causes further components to interrupt their function ($s \in \{OH\}$). As soon as components begin to restore their operational capability, there is a gradually increase of *availability* and a stepwise increase of *operational availability*. This stepwise increase can be explained by the fact that all components of a production cell have to be restored until the production cell is completely functional, again.

These exemplary worst-case courses of failure propagations within the information network illustrate that our modeling approach can be used as the basis for detailed analyses of information networks and their components and, thus, provides value for practitioners. The analysis of single worst-case courses is especially important as the potentially worst-case courses of propagation effects can cause significant damage to companies and, thus, represent extreme risk potentials for companies like complete production downtimes or a loss of operations that result in significant economic damage. These worst-case courses would not be observable if the data of simulation runs is accumulated, for instance, to average values. Thus, our modeling approach and the application of key figures such as the described ones enable the profound analysis of different structural designs of information networks and the targeted derivation of IT security measures to avoid or soften worst-case courses. Accordingly, the identification of beneficial design features such as precise and highly effective air gaps between components of the information network or the implementation of redundant IT components is facilitated.

5.4 Expert Interviews

To complement the evaluation from a naturalistic perspective, we interviewed experts from two companies to cover different views and an academic PN expert. Thereby,

we discussed our modeling approach with the experts in-depth and based on the exemplary application in the close-to-reality structure from Sect. 5.2 and the application of key figures in Sect. 5.3. The interviews with the experts from practice, who deal with our research context on a daily basis in detail, focused on the first two phases of the DSR methodology (problem identification and design objectives) and helped to validate the usability and real-world fidelity of our modeling approach.

First, we interviewed the chief information officer of PACKAGING, one of the world's leading manufacturers of flexible packaging with 10,000 employees in 23 countries and sales of €1.9 billion in 2015. PACKAGING extensively applies automation technologies in their production facilities and, thus, provides great experience with comprehensive information networks and digital technologies within production facilities. The expert confirmed the need for a modeling approach that depicts information networks in smart factories to analyze both attacks and errors in a separated and integrated manner as, till date, corresponding approaches are missing. Further, he considered our abstraction of a smart factory network, the categorization of threats, and the proposed design objectives and requirements of our research as useful and sensible. For further research, he remarked that employees might not be familiar with the graphical representation of a modeled information network component due to the specific notation of PN. Further, the graphical representability of the entire modeled information network might suffer in large information networks and become rather complex and confusing. Both limitations could be addressed by an user-friendly graphical user interface in combination with drill down functions and a defined hierarchical structure that is able to condense large information networks on customizable granularity levels. For instance, these hierarchy levels could be defined on a component level, production cell level, or production area level.

The second organization ROBOTIC is a manufacturer of industrial robots and intelligent automation solutions. ROBOTIC has about 12,300 employees and sales of €3 billion. We interviewed the vice president of digital strategy of ROBOTIC, who holds a doctorate in business & information systems engineering and has several years of experience in the field of automation and robotics. This expert also confirmed the need for modeling and analyzing IT availability risks in smart factory information networks and the lack of corresponding approaches, till date. He highlighted that the modularization of our PN approach is helpful in managing the increasing size and complexity of information networks. Further, he remarked that the development of key performance indices is necessary to enable employees of the IT department to analyze and improve the security of smart factory information networks. This important remark was integrated in our research and led to the development of the key figures presented in Sect. 5.3. Moreover, he pointed out that the consideration of a dynamic failure rate would be beneficial, as failure rates of technical applications generally change during service life (cf. Weibull distribution). Since the application of our modeling approach in the paper at hand is steered towards an already installed smart factory network that is in an established, running operational mode, the consideration of life cycle effects such as set-up difficulties or wear-out of components is not necessary. However, this would be possible through an appropriate parametrization and the use of suitable distributions. Further remarks from these experts were used as orientation for the parametrization of the exemplary simulation in Sect. 5.2 (for instance, regarding the security level of components or the error recovery rate).

Lastly, we interviewed a professor for electrical engineering with a background in mechatronic and control engineering as an expert for PN to evaluate our modeling approach from a methodological perspective. The interviewed expert focuses in his research on flexible automation and cooperative robotics in the field of Industry 4.0 and, thus, besides the methodological knowledge about PN he possess relevant practical knowledge about smart factories and their information networks. This expert confirmed that our developed modeling approach addresses a highly relevant research topic as the analysis of IT availability risks in complex smart factory information networks requires the development of appropriate approaches. In the opinion of the expert, our approach can serve as a basis for the analysis of different interconnection patterns of information networks and for failure analysis, for instance, of common-cause failures. Further, he confirmed that our design objectives and requirements derived from literature are decisive and plausible. He highlighted, that our approach by means of stochastic PN approach is highly valuable for the structured modeling of complex information networks and that our modeling approach is plausible and comprehensible. Further, he emphasized that the data necessary for the parametrization of our modeling approach in real-world application scenarios can be gathered through different sources relating to functional safety such as technical data sheets of component manufacturers. The expert also suggested that the consideration of functional safety and its impairment by IT availability risks would have been another interesting element. Since we focused our research on IT availability risks and their direct effects in the information network, this represents an interesting opportunity for further research.

6 Conclusion, Limitations, and Future Work

The digitalization and interconnection of production infrastructures lead to new challenges for companies (Amin et al. 2013). In particular, the flawless functioning of information networks and the exchange of information in real-time are prerequisites for the operational capability of smart factories. Therefore, in this paper we have presented a stochastic PN approach to model and simulate information networks of smart factories considering different threats. The key benefits of our modeling approach are:

- Increased transparency and controllability of complexity as the modularization of the modeling approach enables the depiction and simulation of increasingly complex and dynamic information network settings;
- Analysis of different threat scenarios and derivation of valuable recommendations towards sensible design patterns for smart factory information networks and degree of interconnectivity;
- Identification of weak spots in the information network and basis for the derivation of appropriate countermeasures against IT availability risks that is subject to further research.

To validate the developed modeling approach, we have simulated different threats compromising an artificial information network setting and interviewed experts from two global leading companies and an academic PN expert. The results indicate that the developed approach is appropriate for the modeling of information networks in smart factories and the analysis of associated IT availability risks. Considering the examples of Stuxnet, locky, WannaCry, or the steel mill provided in the introduction, our modeling approach can support companies in their preventive risk management by modeling, simulating, and analyzing the information network and by identifying weak spots and critical dependencies through the qualitative comparison of different threat scenarios. For this, our modeling approach provides the starting points for a profound comparison of different threat scenarios by creating transparency and providing a structured modeling approach. In addition to quantitative key figures, a more qualitative analysis, e.g., on the basis of expert assessments and expert discussions (see also our expert interviews in Sect. 5.4), should also be conducted in any case, since pure key figure-based comparisons are not sufficient, e.g., due to uncertainties in parameterization. However, these discussions are made possible or are really effective only through the transparency created by structured approaches such as our modeling approach. Accordingly, the insights gained by our approach can be used as a starting point to investigate targeted IT-security measures to reduce risks associated with IT availability. Accordingly, the insights imply that our approach can be beneficial for practice and further research to derive valuable recommendations towards the design of information networks from a risk management perspective. Hence, our approach is the basis for the (further) development and protection of information networks and dependent production systems.

Our developed modeling approach entails both the challenge of gathering the necessary data by companies and the challenge of the identification of a sensible parametrization (e.g., security level) for accurate modeling and simulation. In this regard, our approach can serve as a blueprint that helps companies to identify which data they should gather to be able to analyze availability risk of their information network. Potential sources for these data may include maintenance data and technical data sheets of components, historical data, expert estimates, or reports from IT security authorities like the German BSI. In addition, the composition of the single modules of large, complex smart factory information networks is time-consuming for the initial modeling. To support this, further research could develop a formal definition for the model composition that performs place superposition based on corresponding labels and, thus, automates the composition process.

Our approach is restricted to the analysis of information network components. However, extensions such as modules for the depiction of information flows and threats that can affect information flows (e.g., broken cables) can be applied due to the modular approach. Further, currently, our modeling approach can only model intentional attacks caused by virus attacks and technical errors. Thus, further research could develop modeling extensions to incorporate other kinds of attacks like data leakage. Pointing into the same direction, our approach is constrained by the defined operational states and, thus, is not able to depict components with reduced functionality. The consideration of different threat intensities and propagation velocities of threats representing, for instance, the skills of an adversary are subject to further research. Besides, the insights provided by our approach regarding IT availability risks could be used to improve existing Unified Modeling Language (UML) models that are suitable to visualize the structure and behavior of the smart factory. As UML (reference) models lack the possibility to analyze dynamic effects such as stochastic cascading failures and propagation effects, our modeling approach can be used as a suitable extension.

Considering that the comprehensive interconnection in smart factories provides both positive (e.g., increased flexibility and efficiency of production) and negative effects (e.g., increased vulnerability to IT availability risks), companies face the challenge of deciding whether an extensive or deliberate interconnection of the information

network is sensible. In this regard, the identification of the sensible degree of interconnection in smart factories represents one of the most challenging topics. Hence, the goal of our future research is to develop approaches and methods to determine the sensible degree of interconnection considering risk and return aspects in different production environments. Here, the analysis of interdependencies between information and production networks and within the production network is especially necessary to enable the monetary valuation of business interruptions.

To solve this research endeavor, we see four consecutive research areas. Based on the modeling approach presented in the paper at hand (area 1), the identification of critical components (area 2) within information networks represents a subsequent step for deciding on appropriate countermeasures, e.g., by means of key figures. To consider risk and return aspects of interconnectivity and to assess the sensible degree of interconnection in smart factories, methods for the quantification of economic loss potentials (area 3) and expected benefits (area 4) resulting from extensive interconnectivity are necessary. These capabilities should empower companies to assess the sensible degree of interconnection in information networks and to derive adequate IT security measures.

References

Acatech (2013) Recommendations for implementing the strategic initiative Industrie 4.0. http://www.acatech.de/fileadmin/user_upload/Baumstruktur_nach_Website/Acatech/root/de/Material_fuer_Sonderseiten/Industrie_4.0/Final_report__Industrie_4.0_accessible.pdf. Accessed 17 Apr 2017

Albert R, Jeong H, Barabasi A-L (2000) Error and attack tolerance of complex networks. Nature 406(6794):378–382. https://doi.org/10.1038/35019019

Amin S, Schwartz GA, Hussain A (2013) In quest of benchmarking security risks to cyber-physical systems. IEEE Netw 27(1):19–24. https://doi.org/10.1109/MNET.2013.6423187

Amiri AK, Cavusoglu H, Benbasat I (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, New Zealand, pp 1–11

Arns M, Fischer M, Kemper P, Tepper C (2002) Supply chain modelling and its analytical evaluation. J Oper Res Soc 53(8):885–894. https://doi.org/10.1057/palgrave.jors.2601381

Arshad N, Heimbigner D, Wolf AL (2006) Dealing with failures during failure recovery of distributed systems. Comput Sci Tech Rep 943:1–12. https://doi.org/10.1145/1082983.1083067

Ash J, Newth D (2007) Optimizing complex networks for resilience against cascading failure. Phys A 380:673–683. https://doi.org/10.1016/j.physa.2006.12.058

Balbo G, Silva M (1998) Performance models for discrete event systems with synchronizations: formalisms and analysis techniques, vol 1. Kronos, Zaragoza

Brettel M, Friederichsen N, Keller M, Rosenberg M (2014) How virtualization, decentralization and network building change the manufacturing landscape: an industry 4.0 perspective. Int J Mech Aerosp Ind Mech Manuf Eng 8(1):37–44

Broy M, Cengarle MV, Geisberger E (2012) Cyber-physical systems: imminent challenges. In: Hutchison D, Kanade T, Kittler J, Kleinberg JM, Mattern F, Mitchell JC et al (eds) Large-scale complex IT systems. Development, operation and management, LNCS Bd. 7539. Springer, Heidelberg, pp 1–28

BSI (2014) Die Lage der IT-Sicherheit in Deutschland 2014. Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2014.pdf?__blob=publicationFile&v=2. Accessed 17 Apr 2017

BSI (2016) Die Lage der IT-Sicherheit in Deutschland 2016. Bundesamt für Sicherheit in der Informationstechnik. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2016.pdf?__blob=publicationFile&v=5. Accessed 17 Apr 2017

BSI (2017) Cyber-Sicherheits-Umfrage 2017—Cyber-Risiken, Meinungen und Maßnahmen. https://www.bsi.bund.de/SharedDocs/Downloads/ACS/cyber-sicherheits-umfrage_2017.pdf?__blob=publicationFile&v=3. Accessed 2 Jun 2018

Buhl HU, Penzel H-G (2010) The chance and risk of global interdependent networks. Bus Inf Syst Eng 2(6):333–336. https://doi.org/10.1007/s12599-010-0131-7

Buldyrev SV, Parshani R, Paul G, Stanley HE, Havlin S (2010) Catastrophic cascade of failures in interdependent networks. Nature 464(7291):1025–1028. https://doi.org/10.1038/nature08932

Cardenas A, Amin S, Sinopoli B, Giani A, Perrig A, Sastry S (2009) Challenges for securing cyber physical systems. In: Workshop on future directions in cyber-physical systems security, pp 1–4

Colombo AW, Karnouskos S (2009) Towards the factory of the future: a service-oriented cross-layer infrastructure. ICT Shap World Sci View 65:65–81

Common Criteria (2006) Common criteria for information technology security evaluation: part 1: introduction and general model. Version 3.1, Revision 1, CCMB-2006-09-001, pp 1–86, https://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R1.pdf. Accessed 17 Apr 2017

Danziger MM, Shekhtman LM, Bashan A, Berezin Y, Havlin S (2016) Vulnerability of interdependent networks and networks of networks. In: Garas A (ed) Interconnected networks. Springer, Cham, pp 79–99

Eden P, Blyth A, Jones K, Soulsby H, Burnap P, Cherdantseva Y, Stoddart K (2017) SCADA system forensic analysis within IIoT. In: Thomas L, Schaefer D (eds) Cybersecurity for industry 4.0 – analysis for design and manufacturing. Springer, Cham, pp 73–101

Faisal MN, Banwet DK, Shankar R (2007) Information risks management in supply chains. an assessment and mitigation framework. J Enterp Inf Manag 20(6):677–699. https://doi.org/10.1108/17410390710830727

Fridgen G, Stepanek C, Wolf T (2014) Investigation of exogenous shocks in complex supply networks – a modular petri net approach. Int J Prod Res 53(5):1387–1408. https://doi.org/10.1080/00207543.2014.942009

Gao J, Buldyrev SV, Stanley HE, Havlin S (2012) Networks formed from interdependent networks. Nat Phys 8(1):40–48. https://doi.org/10.1038/NPHYS2180

Gregor S, Hevner AR (2013) Positioning and presenting design science research for maximum impact. Manag Inf Syst Q 37(2):337–355

Hallikas J, Karvonen I, Pulkkinen U, Virolainen V-M, Tuominen M (2004) Risk management process in supplier networks. Int J Prod Econ 90:47–58

Hao K, Xie F (2009) Componentizing hardware/software interface design. In: Conference on design, automation and test in Europe, Dresden, Germany, pp 232–237

Hermann M, Pentek T, Otto B (2015) Design principles for Industrie 4.0 scenarios – a literature review. In: Technische Universität Dortmund – working paper 01/2015

Hevner AR, March ST, Park J, Ram S (2004) Design science in information systems research. Manag Inf Syst Q 28(1):75–106

Iansiti M, Lakhani KR (2014) Digital ubiquity: how connections, sensors, and data are revolutionizing business. Harv Bus Rev 92(11):91–99

Jensen K (1991) Coloured petri nets: a high level language for system design and analysis. In: Goos G, Hartmanis J, Barstow D, Brauer W, Brinch Hansen P, Gries D et al (eds) Advances in Petri Nets 1990. LNCS. Springer, Heidelberg, pp 342–416

Kaplan S, Garrick BJ (1981) On the quantitative definition of risk. Risk Anal 1(1):11–27. https://doi.org/10.1111/j.1539-6924.1981.tb01350.x

Keller R, König C (2014) A reference model to support risk identification in cloud networks. In: Proceedings of the 35th international conference on information systems, pp 1–19

Lasi H, Fettke P, Kemper H-G, Feld T, Hoffmann M (2014) Industry 4.0. Bus Inf Syst Eng 6(4):261–264. https://doi.org/10.1007/s12599-014-0334-4

Lee J, Bagheri B, Kao H-A (2015) A cyber-physical systems architecture for industry 4.0-based manufacturing systems. Manuf Lett 3:18–23. https://doi.org/10.1016/j.mfglet.2014.12.001

Lucke D, Constantinescu C, Westkämper E (2008) Smart factory – a step towards the next generation of manufacturing. In: The 41st CIRP conference on manufacturing systems

Marsan MA, Conte G, Balbo G (1984) A class of generalized stochastic petri nets for the performance evaluation of multiprocessor systems. ACM Trans Comput 2(2):93–122

Merlin P (1974) A study of the recoverability of computer system. Ph.D. thesis, University of California, Irvine

Merkur (2018) Globaler Angriff mit Erpressungssoftware verursacht Chaos. https://www.merkur.de/welt/ermittlungen-nach-neuer-massiver-cyber-attacke-zr-8438321.html. Accessed 2 Jun 2018

Mertens P, Barbian D (2015) Grand challenges – Wesen und Abgrenzungen. Inf Spektr 38(4):264–268. https://doi.org/10.1007/s00287-015-0897-6

Molloy MK (1981) On the integration of delay and throughput measures in distributed processing models. Ph.D. thesis, University of California, Los Angeles

Monostori L (2014) Cyber-physical production systems. roots, expectations and R&D challenges. In: Proceedings of the 47th CIRP conference on manufacturing systems 17, pp 9–13. https://doi.org/10.1016/j.procir.2014.03.115

Murata T (1989) Petri nets – properties, analysis and applications. In: Proceedings of the IEEE 77(4). https://doi.org/10.1109/5.24143

Offermann P, Blom S, Schönherr M, Bub U (2010) Artifact types in information systems design science – a literature review. In: Hutchison D, Kanade T, Kittler J, Kleinberg JM, Mattern F, Mitchell JC et al (eds) Global perspectives on design science research (LNCS). Springer, Heidelberg, pp 77–92

Peffers K, Tuunanen T, Rothenberger MA, Chatterjee S (2007) A design science research methodology for information systems research. J Manag Inf Syst 24(3):45–78. https://doi.org/10.2753/MIS0742-1222240302

Petri CA (1962) Kommunikation mit Automaten. Doctoral Thesis, Technische Universität Darmstadt

PwC (2016a) Industry 4.0 – building the digital enterprise. https://www.pwc.com/gx/en/industries/industries-4.0/landing-page/industry-4.0-building-your-digital-enterprise-april-2016.pdf. Accessed 1 Feb 2017

PwC (2016b) Turnaround and transformation in cybersecurity. Key findings from the global state of information security survey 2016. http://www.pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf. Accessed 17 Apr 2017

Radziwon A, Bilberg A, Bogers M, Madsen ES (2014) The smart factory. Exploring adaptive and flexible manufacturing solutions. Procedia Eng 69:1184–1190. https://doi.org/10.1016/j.proeng.2014.03.108

Ramchandani C (1974) Analysis of asynchronos concurrent systems by timed petri nets. Ph.D. Thesis, Massachusetts Institute of Technology

Sadeghi A-R, Wachsmann C, Waidner M (nd) Security and privacy challenges in industrial internet of things. In: Design automation conference, pp 1–6

Sathanur AV, Haglin DJ (2016) A novel centrality measure for network-wide cyber vulnerability assessment. In: IEEE symposium on technologies for homeland security, pp 1–5

Schuh G, Potente T, Wesch-Potente C, Weber AR, Prote J-P (2014) Collaboration mechanisms to increase productivity in the context of Industrie 4.0. Procedia CIRP 19:51–56. https://doi.org/10.1016/j.procir.2014.05.016

Siemens (2017) Siemens-Elektronikwerk Amberg. https://assets.new.siemens.com/siemens/assets/api/uuid:6faa0567-6d63-4bda-b8f5-ffc2c46af3cb/hintergrund-amberg-d.pdf. Accessed 2 Jun 2018

Simon HA (1996) The sciences of the artificial. MIT Press, Cambridge

Smith GE, Watson KJ, Baker WH, Pokorski I, Jay A (2007) A critical balance. Collaboration and security in the IT-enabled supply chain. Int J Prod Res 45(11):2595–2613. https://doi.org/10.1080/00207540601020544

Sonnenberg C, vom Brocke J (2012) Evaluation Patterns for design science research artefacts. In: Helfert M, Donnellan B (eds) Practical aspects of design science (communications in computer and information science). Springer, Heidelberg, pp 71–83

Sridhar S, Hahn A, Govindarasu M (2012) Cyber–physical system security for the electric power grid. Proc IEEE 100(1):210–224. https://doi.org/10.1109/JPROC.2011.2165269

The New York Times (2011) Israeli test on worm called crucial in Iran nuclear delay. http://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html, Accessed 17 Apr 2017

Tupa J, Simota J, Steiner F (2017) Aspects of risk management implementation for Industry 4.0. Procedia Manuf 11:1223–1230

van der Aalst WMP (1998) The application of petri nets to workflow management. J Circuit Syst Comput 8(01):21–66. https://doi.org/10.1142/S0218126698000043

VDI (2013): Cyber-physical systems: Chancen und Nutzen aus Sicht der Automation. https://www.vdi.de/uploads/media/Stellungnahme_Cyber-Physical_Systems.pdf#. Accessed 15 May 2018

Venable J, Pries-Heje J, Baskerville R (2012) A comprehensive framework for evaluation in design science research. In: Hutchison D, Kanade T, Kittler J, Kleinberg JM, Mattern F, Mitchell JC et al (eds) Design science research in information systems. advances in theory and practice (LNCS). Springer, Heidelberg, pp 423–438

Vladimir AB (2011) On the modularity in petri nets of active resources. In: Proceedings of CompoNet and SUMo, pp 33–48

Wagner SM, Neshat N (2010) Assessing the vulnerability of supply chains using graph theory. Int J Prod Econ 126(1):121–129. https://doi.org/10.1016/j.ijpe.2009.10.007

Wan J, Yan H, Liu Q, Zhou K, Lu R, Di L (2013) Enabling cyber-physical systems with machine-to-machine technologies. Int J Ad Hoc Ubiquitous Comput 13(3/4):187–196. https://doi.org/10.1504/IJAHUC.2013.055454

Wang S, Wan J, Li D, Zhang C (2016) Implementing smart factory of Industrie 4.0: an outlook. Int J Distrib Sens Netw 12(1):1–10

Washington Post (2008) Cyber incident blamed for nuclear power plant shutdown. By Brian Krebs. http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html. Accessed 17 Apr 2017

Weill P, Vitale M (2002) What IT infrastructure capabilities are needed to implement e-business models? MIS Q 1(1):17–34

Wengert A, Graham J, Ribble E (2016) A new approach to cyberphysical security in industry 4.0. In: Thomas L, Schaefer D (eds) Cybersecurity for industry 4.0 – analysis for design and manufacturing. Springer, Cham, pp 59–72

Wu T, Blackhurst J, O'grady P (2007) Methodology for supply chain disruption analysis. Int J Prod Res 45(7):1665–1682. https://doi.org/10.1080/00207540500362138

Yoon JS, Shin SJ, Suh SH (2012) A conceptual framework for the ubiquitous factory. Int J Prod Res 50(8):2174–2189. https://doi.org/10.1080/00207543.2011.562563

Zambon E, Etalle S, Wieringa RJ, Hartel P (2011) Model-based qualitative risk assessment for availability of IT infrastructures. Softw Syst Model 10(4):553–580

Zuehlke D (2010) Smart factory – towards a factory-of-things. Annu Rev Control 34(1):129–138. https://doi.org/10.1016/j.arcontrol.2010.02.008