Spring 6-10-2017

DEVELOPMENT OF DYNAMIC KEY FIGURES FOR THE IDENTIFICATION OF CRITICAL COMPONENTS IN SMART FACTORY INFORMATION NETWORKS

Björn Häckel
University of Applied Sciences Augsburg, bjoern.haeckel@fim-rc.de

Daniel Miehle
University of Augsburg, daniel.miehle@fim-rc.de

Stefan Pfosser
University of Augsburg, stefan.pfosser@fim-rc.de

Jochen Übelhör
University of Augsburg, jochen.uebelhoer@fim-rc.de

Recommended Citation

Häckel, Björn; Miehle, Daniel; Pfosser, Stefan; and Übelhör, Jochen, (2017). "DEVELOPMENT OF DYNAMIC KEY FIGURES FOR THE IDENTIFICATION OF CRITICAL COMPONENTS IN SMART FACTORY INFORMATION NETWORKS". In Proceedings of the 25th European Conference on Information Systems (ECIS), Guimarães, Portugal, June 5-10, 2017 (pp. 2767-2776). ISBN 978-0-9915567-0-0 Research-in-Progress Papers.
http://aisel.aisnet.org/ecis2017_rip/27

DEVELOPMENT OF DYNAMIC KEY FIGURES FOR THE IDENTIFICATION OF CRITICAL COMPONENTS IN SMART FACTORY INFORMATION NETWORKS

Research in Progress

Björn Häckel, Project Group Business & Information Systems Engineering of the Fraunhofer FIT, Professorship for Digital Value Networks, University of Applied Sciences Augsburg, Germany, bjoern.haeckel@fim-rc.de

Daniel Miehle, University of Augsburg, Augsburg, Germany, daniel.miehle@fim-rc.de

Stefan Pfosser, Research Center Finance & Information Management, University of Augsburg, Germany, stefan.pfosser@fim-rc.de

Jochen Übelhör, Project Group Business & Information Systems Engineering of the Fraunhofer FIT, Research Center Finance & Information Management, University of Augsburg, Germany, jochen.uebelhoer@fim-rc.de

Abstract

Informational risks in smart factories arise from the growing interconnection of its components, the increasing importance of real-time accessibility and exchange of information, and highly dynamic and complex information networks. Thereby, physical production more and more depends on functioning information networks due to increasing informational dependencies. Accordingly, the operational capability of smart factories and their ability to create economic value heavily depend on its information network. Thus, information networks of smart factories have to be evaluated regarding informational risks as a first prerequisite for subsequent steps regarding the management of a smart factory. In this paper, we focus on the identification of critical components in information networks based on key figures that quantitatively depict the availability of the information network. To enable analyses regarding dynamic effects, the developed key figures cover dynamic propagation and recovery effects. To demonstrate their applicability, we investigate two possible threat scenarios in an exemplary information network. Further, we integrated the insights of two expert interviews of two global companies in the automation and packaging industry. The results indicate that the developed key figures offer a promising approach to better analyse and understand informational risks in smart factory information networks.

Keywords: Smart Factory, Information Network, Informational Risk, Dynamic Key Figures.

1 Introduction

Production is on the move towards the fourth industrial revolution, i.e., the advanced digitalization of production facilities. This development is mainly enabled by concepts such as the Internet of Things (IoT) and emerging information and communication technologies (ICTs) such as embedded systems, cloud computing, and big data applications (Jing et al., 2014; Wang et al., 2016; Xu, 2012; Zuehlke, 2010; Schuh et al., 2014). Thereby, the extensive interconnection and integration of ICTs into physical production create smart factories with highly dynamic and complex information networks in which smart machines and smart products are able to control and monitor production processes collaboratively (Kagermann et al., 2013). Thus, in contrast to traditional facilities, smart factories are able to self-organize and self-control production processes, respond context-specific to turbulences in real-time, and flexibly produce small-quantity orders of highly customized products (lot-size one) at costs comparable to mass production (Brettel et al., 2014; Radziwon et al., 2014). However, despite these benefits, smart factories face the growing challenge of informational dependencies that arise from (1) the enormous number of interconnected components and (2) the increasing use of real-time information. These informational dependencies lead to informational risks (e.g., loss of availability) that can not only affect the information network, but also physical production processes (Broy et al., 2012). In this context, informational risks are caused through local threat events in the information network such as errors (e.g., technical defects) and attacks (e.g., cyber-attacks) and can propagate within the information network even independent of physical connections resulting in cascading failures. Additionally, information networks of smart factories are integrated within inter-corporation value networks (e.g., with vendors and customers), which facilitates a highly automated and flexible production on the one hand, but reinforces the vulnerability of smart factories to informational risks on the other hand (Wang et al., 2016).

Given this development and considering the increasing interdependency of physical production and information networks (Broy et al., 2012), such threat scenarios are highly relevant for the proper functioning of smart factories and thus, for the process of economic value creation. Prominent examples are *Slammer*, a worm that infected critical monitoring systems of a nuclear power plant in the U.S., *Stuxnet*, that targeted programmable logic controllers at an Iranian nuclear facility (Cardenas et al., 2009), or, most recently, the attack on routers of a German internet provider (Fitzgerald, 2016). Considering such events, appropriate methods and approaches for the identification and economic evaluation of informational risks in smart factories and their propagation behaviour over time are needed to lay the basis for the meaningful derivation of corresponding countermeasures. As this is a quite young field of research, approaches are, to the best of our knowledge, virtually absent. Therefore, we state our research question:

RQ: What are appropriate dynamic key figures to identify critical components in smart factory information networks?

We develop dynamic key figures that enable the identification of critical components in information networks by depicting the dynamic behaviour of threats (e.g., propagation effects) and the resulting operational capability of the smart factory quantitatively. We follow the Design Science Research (DSR) paradigm (Hevner et al., 2004) and provide first insights into the applicability of dynamic key figures to better analyse and understand informational risks.

The remainder of this paper is structured as follows. We provide a brief overview on related work in section 2. In section 3, we develop and describe the dynamic key figures. In section 4, we apply the developed figures to an exemplary smart factory information network based on a real-world setting providing first results and integrate insights of expert interviews with two global leading companies in the robotic automation and flexible packaging industry confirming the identified research gap. Finally, section 5 presents conclusions, reveals limitations, and gives an outlook on ongoing and further research.

2 Related Work

In the following section, we review literature on smart factories and methods for criticality analysis. Based on this literature we define requirements (R.1 – R.5) for the adequate development of key figures. As the digitalization of physical production increasingly gains importance, scientific literature (e.g., Fleisch and Thiesse, 2007; Haller et al., 2009; Iansiti and Karim, 2014) and application-oriented studies (e.g., Radziwon et al., 2014; Yoon et al., 2012; Zuehlke, 2010; Lucke et al., 2008) deal with the development of smart factories. Thereby, the term smart factory is not clearly defined and is also known, for instance, as a U-factory (Yoon et al., 2012) or a factory-of-things (Zuehlke, 2010). Based on a literature review, Radziwon (2013) describes a smart factory as a *"manufacturing solution that provides such flexible and adaptive production processes that will solve problems arising on a production facility with dynamic and rapidly changing boundary conditions in a world of increasing complexity"*. In this vein, there is research that deals with characteristics such as modularization, distributed control, and self-optimization (Brettel et al., 2014) as well as challenges such as safety and security issues of smart factories (Amin et al., 2013; Broy et al., 2012). However, as physical production and thus, economic value creation increasingly depend on the flawless functioning of information networks, one remaining challenge is the identification of critical components to ensure the operational capability of smart factories. This challenge was also confirmed by our interviewed experts, who are concerned with the design of information networks in digital production environments. Hence, the identification of critical components represents an indispensable prerequisite to economically evaluate informational risks and to implement corresponding countermeasures. The criticality of a component depicts its threat potential to the operational capability of the information network in case of a failure. Thus, key figures should enable the identification of *critical components* in information networks in case of a failure (R.1). A failure of a component can be caused by attacks or errors (Amin et al., 2013). Hence, key figures should consider different threats (R.2). Additionally, due to increasing informational dependencies in smart factories, a failure of a component can spread within the information network affecting other components (Sadeghi et al., 2015; Sathanur and Haglin, 2016). To analyse the dynamic behaviour of propagation and recovery effects, key figures should consider timing aspects (R.3). Moreover, to determine the operational capability of a smart factory, key figures should consider different states regarding the availability of components (R.4) (cf. Arshad et al., 2005). Finally, key figures should be *easy to apply and interpret* (R.5).

Despite the theoretical and practical relevance, research on the identification of critical components in smart factory information networks remains insufficient until today. Hence, we provide an overview of approaches that assess informational risks in general as they may provide adequate starting points for our research. For instance, Silva et al. (2014) develop a multi-dimensional risk model based on *Failure Mode and Effect Analysis* and *fuzzy theory* providing information regarding the criticality of investigated failures. Another risk framework developed by Jaisingh and Rees (2001) uses the risk measure *Value at Risk* to assess informational risks. Zambon et al. (2011) developed a risk assessment method for business processes that considers the IT architecture and dependencies between IT components. Other methods in *graph theory* and *network analysis* include centrality measures such as *degree measure* (Freeman, 1978) and *alpha centrality* (Bonacich and Lloyd, 2001). Thereby, 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, the approaches only allow a static analysis and thus, neglect dynamic effects within information networks. Further, Nikoletseas et al. (2003) develop a model for attack propagation in networks considering the number of captured nodes. Other research analyses informational risks that exist in the context of supply chain networks and critical infrastructures. For instance, Faisal et al. (2007) introduce a method for the quantification of informational risks in static supply chains, whereas Wagner and Neshat (2010) develop an index to evaluate the vulnerability of supply chain processes to informational risks. Once again, these approaches focus on a static analysis and do not explicitly consider propagation effects in smart factories. In addition, they analyse the vulnerability of the overall network and do not focus on the criticality of single components - what is the basis for the identification of appropriate countermeasures. Since propagation effects are interdependent and dynamic, Buldyrev et al. (2010) consider the spread of information risks within interdependent networks analysing the criticality of nodes for network stability. Although this approach meets several of the requirements stated above, it does not take into account different component states. Thus, to the best of our knowledge there is no approach that develops dynamic key figures for the identification of critical components and considers adequately network structures and inherent (informational) dependencies.

3 Development of Dynamic Key Figures

3.1 Research Approach

To answer the stated research question, we follow the research guidelines for DSR by Hevner et al. (2004) to develop a metric as our design artefact (Offermann et al., 2010). Thereby, the DSR approach helps to clearly structure research activities in the context of information systems research to successfully develop theoretical artefacts (cf. Peffers et al., 2007). In this paper, we apply a two-step approach. First, we develop dynamic key figures that enable the identification of critical components of information networks in smart factories in an observed time frame. Second, we apply the dynamic key figures in an exemplary smart factory setting based on several simulations. In doing so, we are able to demonstrate the feasibility and applicability of our dynamic key figures (Sonnenberg and Vom Brocke, 2012). Hence, we follow a well-known framework of evaluation activities in DSR by means of an evaluation in an artificial environment using a simulation to show that the developed dynamic key figures "*progress to a solution of the stated problem*" (Sonnenberg and Vom Brocke, 2012).

3.2 Dynamic Key Figures for Informational Risks

We basically consider a company that runs a smart factory and thus, faces the challenge of highly interconnected and interdependent production and information networks. Since our approach cannot depict all real world complexities entirely, we state the following two assumptions. First of all, to be able to identify critical components within the information network by means of dynamic key figures, relevant data regarding the information network and its components has to be available.

Assumption 1 – Data about the information network: *The information network of the smart factory is depicted by an adequate modelling method that covers relevant characteristics (e.g., states of a component, dependencies between components) and provides all necessary data for the application of dynamic key figures to identify critical components of the information network (e.g., servers, embedded systems).*

Second, to determine whether single components are in a functioning condition, and thus, to determine the current operational capability of the information network, possible component states have to be defined. These states have to be distinct without overlaps to enable a clear calculation of dynamic key figures. Hence, a component should only exhibit one state at a certain point in time.

Assumption 2 – States of the information network's components: *An information network's component can exhibit the states $s \in \{$operational (OP); on hold (OH); failed after attack (FA); failed after error (FE)$\}$ at one point in time $t \in \{1; 2; \ldots; T\}$ of the observed time frame.*

We consider a component to be *OP* if it can perform its assigned function, i.e., the component provides its function and all necessary information is accessible. In contrary, a component is *OH* if it still provides its function, but the transmission of necessary information exceeds a certain time limit (e.g., due to a failure of another component). Furthermore, external and internal attacks or errors can lead to a failure of a component. In this case, the component is no longer able to provide its function and to transmit processed information to other components. According to the initial trigger of the failure event, we distinguish between the states FA or FE. The current state $s \in \{OP; OH; FA; FE\}$ of each component $n \in N$ at t is depicted by the state vector $v_{n,t}^{b} = (b_{n,t}^{OP}, b_{n,t}^{OH}, b_{n,t}^{FA}, b_{n,t}^{FE})$, where $b_{n,t}^{s}$ represents a binary variable that takes the value 1 if component n is in state s at t, else 0. Each component n can only exhibit one state s at t. Thus, the following condition applies: $b_{n,t}^{OP} + b_{n,t}^{OH} + b_{n,t}^{FA} + b_{n,t}^{FE} = 1\ \forall t$. By means of the state vector $v_{n,t}^{b}$, the state of each component is defined clearly for each point in time. Table 1 provides an overview over the states, their attributes, and the associated state vector.

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 $v_{n,t}^{b}$	$v_{n,t}^{b} = (1,0,0,0)$	$v_{n,t}^{b} = (0,1,0,0)$	$v_{n,t}^{b} = (0,0,1,0)$	$v_{n,t}^{b} = (0,0,0,1)$

Table 1. Component states and corresponding state vectors

To enable a comprehensive analysis of the smart factory's information network regarding its operational capability after an attack or error, we develop the following dynamic key figures, using the state vectors $v_{n,t}^{b}$. Thereby, we distinguish between *availability* and *operational availability:*

Dynamic key figure 1a – Availability: *The availability of the information network $AV_t^{IN}(\widehat{M},\hat{t})$ measures the share of components that are able to provide their function ($s \in \{OP;OH\}$) at t considering that a subset $\widehat{M}$ of the components initially fails[1] at $\hat{t}$ due to an attack or error (see eq. 1a).*

Dynamic key figure 1b – Operational availability: *The operational availability of the information network $opAV_t^{IN}(\widehat{M},\hat{t})$ measures the share of components that are able to provide their function and access necessary information ($s \in \{OP\}$) at t considering that a subset $\widehat{M}$of the components initially fails at $\hat{t}$ due to an attack or error (see eq. 1b).*

$$AV_t^{IN}(\widehat{M},\hat{t}) = \frac{\sum_{n=1}^{N} b_{n,t}^{OP} + \sum_{n=1}^{N} b_{n,t}^{OH}}{N} \ \forall t \qquad (1a) \qquad\qquad opAV_t^{IN}(\widehat{M},\hat{t}) = \frac{\sum_{n=1}^{N} b_{n,t}^{OP}}{N} \ \forall t \qquad (1b)$$

By means of the distinction between *availability* and *operational availability*, the information network and its components can be analysed regarding their operational capabilities and informational dependencies in order to identify critical components (cf. section 5). Whereas traditional availability key figures often only cover if a system is in a functioning condition or not, our approach enables a detailed depiction of four different relevant states. To analyse the information network's behaviour over time after a failure event, the following key figures describe how the states of components of the information network change between $t-1$ and t. We consider four types of rates comprising *propagation rate, operational propagation rate, recovery rate,* and *operational recovery rate*.

Dynamic key figure 2a and 2b – (Operational) propagation rate: *The propagation rate $pr_t^{IN}(\widehat{M},\hat{t})$ measures the ratio of the information network's components that provided their function at $t-1$ ($s \in \{OP;OH\}$), but malfunction at t ($s \in \{FA;FE\}$) considering that a subset $\widehat{M}$ initially fails at $\hat{t}$ due to an attack or error (see eq. 2a). Analogously, the operational propagation rate $oppr_t^{IN}(\widehat{M},\hat{t})$ measures the change from $s \in \{OP\}$ to $s \in \{OH;FA;FE\}$ (see eq. 2b).*

$$pr_t^{IN}(\widehat{M},\hat{t}) = \frac{\sum_{n=1}^{N} b_{n,t}^{FA} + \sum_{n=1}^{N} b_{n,t}^{FE}}{N} \qquad \forall n \middle| b_{n,t-1}^{OP} = 1 \lor b_{n,t-1}^{OH} = 1;\ \forall t > 1 \qquad (2a)$$

$$oppr_t^{IN}(\widehat{M},\hat{t}) = \frac{\sum_{n=1}^{N} b_{n,t}^{OH} + \sum_{n=1}^{N} b_{n,t}^{FA} + \sum_{n=1}^{N} b_{n,t}^{FE}}{N} \qquad \forall n \middle| b_{n,t-1}^{OP} = 1;\ \forall t > 1 \qquad (2b)$$

The (operational) propagation rate enables the illustration and analysis of propagation effects within the information network (e.g., identification of the start of propagation effects or the velocity of the propagation). To observe the information network's behaviour regarding the recovery of components over time, we define the following rates.

Dynamic key figure 3a and 3b – (Operational) recovery rate: *The recovery rate $rr_t^{IN}(\widehat{M},\hat{t})$ measures the ratio of the information network's components that malfunction at $t-1$ ($s \in \{FA;FE\}$), but are restored at t ($s \in \{OP;OH\}$) considering that a subset $\widehat{M}$ of the components initially fails at $\hat{t}$ due to an attack or error (see eq. 3a). Analogously, the operational recovery rate $oprr_t^{IN}(\widehat{M},\hat{t})$ measures the change from $s \in \{OH;FA;FE\}$ to $s \in \{OP\}$ (see eq. 3b).*

$$rr_t^{IN}(\widehat{M},\hat{t}) = \frac{\sum_{n=1}^{N} b_{n,t}^{OP} + \sum_{n=1}^{N} b_{n,t}^{OH}}{N} \qquad \forall n \middle| b_{n,t-1}^{FA} = 1 \lor b_{n,t-1}^{FE} = 1;\ \forall t > 1 \qquad (3a)$$

$$oprr_t^{IN}(\widehat{M},\hat{t}) = \frac{\sum_{n=1}^{N} b_{n,t}^{OP}}{N} \qquad \forall n \middle| b_{n,t-1}^{OH} = 1 \lor b_{n,t-1}^{FA} = 1 \lor b_{n,t-1}^{FE} = 1;\ \forall t > 1 \qquad (3b)$$

[1] $\widehat{M}$ 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.

The developed key figures can be applied to analyse an entire information network, a subnetwork, or selected components. Thus, the key figures support the improvement of already existing information networks as well as the development of a sensible design and configuration of new information networks. To demonstrate the usability of the developed key figures, in the following section, we implement the key figures in a simulation software and apply them to an exemplary case. Since the development of the formal modelling method is still pending and it is therefore not yet possible to apply our key figures to a real world case, we base our analysis on an exemplary data set in a first step. The data set is deliberately chosen to obtain different network characteristics and present relevant insights.

4 Exemplary Application and Analyses

To analyse the impact of different threats on the information network and to identify critical components, we apply the dynamic key figures in an exemplary information network. The structure of the information network is based on literature (see e.g., Lucke et al., 2008; Yoon et al., 2012; Zuehlke, 2010). Also, the interviewed experts verified that the information network structure depicts the relevant characteristic of the real-world. As depicted in Figure 1, the considered information network consists of 100 components.

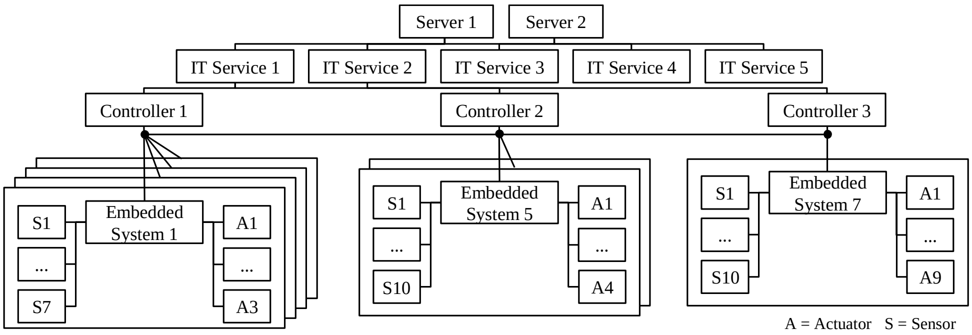

Figure 1. Smart factory information network based on Lucke et al. (2008) and Yoon et al. (2012)

On the first level (shop-floor level), there are seven subnets representing production cells (e.g., machines or industrial robots) consisting of an embedded system, a varying number of sensors (seven or ten), and actuators (three, four, or nine). The embedded systems enable the decentralized control of sensors and actuators, and the communication with other production cells and higher-level controllers. The three controllers are connected to IT services (e.g., enterprise resource planning) hosted on two on-premise servers. The described setting results in a dependency structure including functional (e.g., between server and IT services) and informational dependencies between components. Given this setting, we analyse two threat scenarios to show different effects on the information network. In both scenarios, we observe a time frame of 100 periods and threat events occurring initially at $t = 1$. As components depend on the information and function provided by other components, a functional incapacity of component x can lead after a certain time span, for instance 20 periods, to a functional incapacity of component y due to missing information. Once component x is initially affected by an attack or an error, the time required to repair it and to restore its functional capacity is described by a random variable.

In ***Scenario 1***, we consider a failure of both servers due to a technical defect (e.g., caused by an incorrect software update). We assume that the defect leads to a severely damage of the servers resulting in a repair time of 85 periods. In ***Scenario 2***, we consider a targeted attack by a malicious adversary affecting only embedded system 1. We assume that the executed attack can compromise other directly connected components (e.g., sensors, actuators, and other embedded systems) with a given probability.

Figure 2a shows that the *availability* in scenario 1 drops to 98% after the failure of server 1 and 2 at $t = 1$. However, the *operational availability* considerably decreases stepwise, as IT services depend functionally on the servers. Consequently, controllers ($t = 25$ / drop 2 in figure 2a), embedded systems, and all dependent sensors and actuators ($t = 63$ and $t = 64$ / drop 3 and 4 in figure 2a) exhibit the *OH* state due to missing information, resulting in a standstill of the entire smart factory. In $t = 85$, both servers are repaired. Within the following periods, all components restore their operational capacity and change their state from OH to OP as necessary information is accessible, again. The entire smart factory is restored and fully functional at $t = 88$. This scenario illustrates that a failure of central components, i.e., both servers, leads to an inoperability of the entire smart factory. As shown in Figure 2b, the attack on embedded system 1 in scenario 2 causes a rapid drop of the components' *availability* to 41% at $t = 4$. 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.

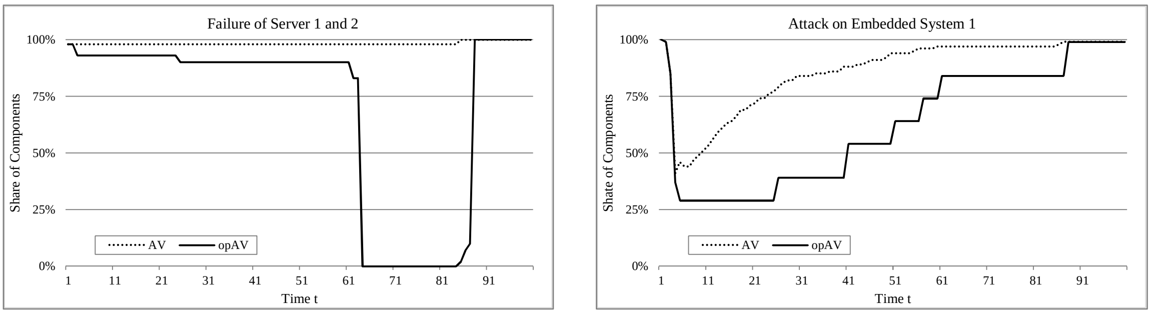

Figure 2. Illustration of AV and opAV after failure (a) and after attack (b)

Monitoring the *propagation rate* and the *operational propagation rate*, we are able to draw further conclusions. We generally can observe that propagation effects due to informational dependencies in case of errors of components start delayed in scenario 1 (Figure 3a). This is due to the different levels of the information network. Thus, cause (technical error) and effect (decrease of *operational availability)* of a component's failure are not synchronized in that scenario. Further, the *propagation rate* shows a small peak in $t = 1$ representing the technical defect of both servers. Whereas, the *operational propagation rate* shows several small peaks, representing the operational incapacity of, for example, IT services and one big peak representing the operational incapacity of the embedded systems, sensors and actuators. In contrast, the *operational propagation rate* in scenario 2 is high right after the attack compromises embedded system 1 and subsequently spreads within the information network compromising other components (Figure 3b). In the following, after the attack affected the majority of production cell, *propagation rate* and *operational propagation rate* show no further peaks after $t = 8$.

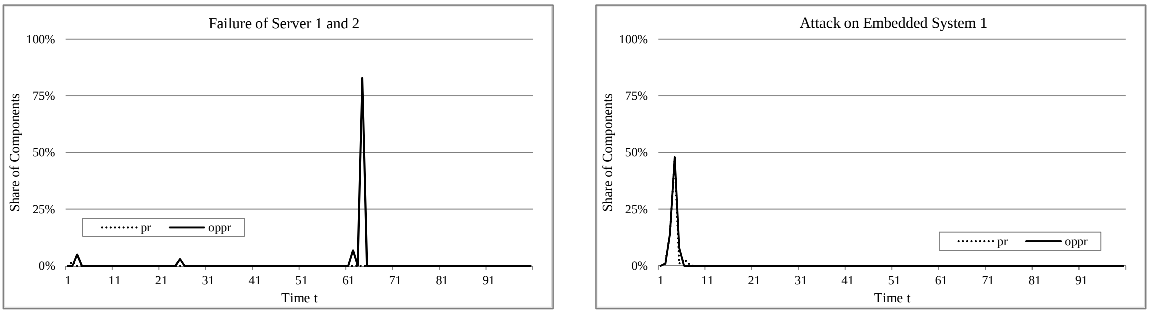

Figure 3. Illustration of pr and oppr after failure (a) and after attack (b)

Further, a detailed analysis of different recovery behaviours is enabled by the *recovery rate* and *operational recovery rate*. The recovery of the network in scenario 1 (Figure 4a) is mainly influenced by the repair of the servers leading to a rapid and complete recovery of the operational capabilities of the entire smart factory in $t = 88$. As the attack on the embedded system 1 in scenario 2 compromised several other components, the recovery in Figure 4b follows a progressive process over time as affected components restore their operational capability gradually.

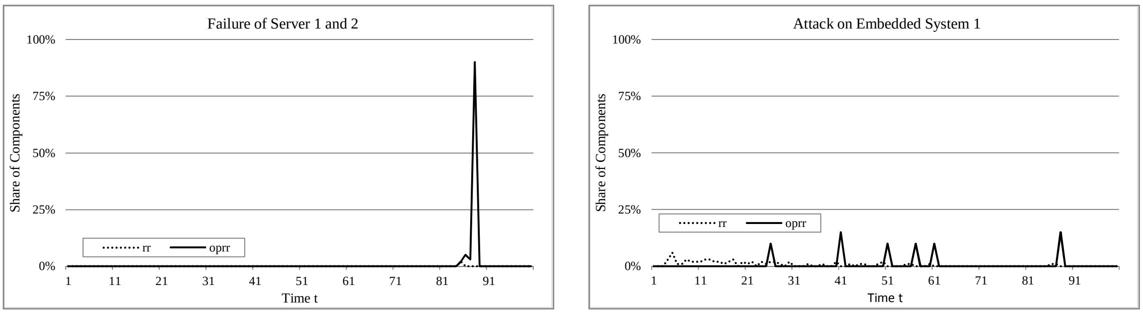

Figure 4. Illustration of rr and oprr after failure (a) and after attack (b)

5 Conclusion, Limitations, and Future Work

The increasing dependency of physical production on information networks and the increasing use of real-time information lead to new challenges for companies, as the proper functioning of components of the information network becomes a factor of upmost importance. Hence, our aim is to identify the most critical components of information networks to derive valuable recommendations towards the design of information networks and especially the identification of adequate countermeasures. Therefore, we developed a set of dynamic key figures that particularly consider dynamic propagation and recovery effects and presented first insights regarding the characteristics of different threats as well as the criticality of different components. Although this first approach cannot provide a complete answer to the stated research question, it constitutes interesting first results that can be beneficial for practice and further research. For instance, the results gained by our current approach reveal detailed information about propagation effects and their progress over time. By refining the key figures, for example in regard to the considered states, even more detailed analyses of failure propagation courses become feasible. This enables the profound analysis of different structural designs of information networks and accordingly, the identification of beneficial design features such as precise and highly effective air gaps between components of the information network. Limitations of our idea include that the development of an adequate modelling approach for informational risks in smart factories is still in process. Further, not all companies are able to provide the required input data for the calculation of the dynamic key figures.

In a next step, we want to perform several simulations to analyse the criticality of all components of the information network after an attack or error in order to define thresholds and patterns that facilitate the automatic identification of critical components. In addition, we aim to investigate stochastic aspects such as frequency and occurrence probability of attacks on specific components in more detail. To enable the comparison of different propagations velocities, we plan to modify the propagation rate to measure the cumulative number of failed components at a certain point in time. Finally, we plan to evaluate the developed dynamic key figures in real world settings in cooperation with companies.

In our opinion, the identification of critical components by means of dynamic key figures contributes to an important overarching research project. The aim of this research project is to provide approaches and methods to determine the optimal level of interconnectedness within and between information and production networks in smart factories. To solve this extensive research project, we see four consecutive research areas: First, a formal modelling approach for the depiction and simulation of informational risks in smart factories is needed (area 1). We address this topic by means of a currently evolving working paper in which we apply stochastic modular petri nets. Second, representing the focus of this paper, the identification of critical components based on dynamic key figures is necessary (area 2). Finally, methods for the quantification of economic loss potentials (area 3) and expected benefits (area 4) that result from the extensive interconnection have to be developed. The developed methods and approaches are supposed to support companies in deciding on adequate countermeasures for informational risks and in determining the optimal level of interconnectedness within smart factory environments.

References

Amin, S., G. A. Schwartz and A. Hussain (2013). "In Quest of Benchmarking Security Risks to Cyber-Physical Systems." *IEEE Network* 27 (1), 19–24.

Arshad, N., D. Heimbigner and A. L. Wolf (2005). "Dealing with Failures During Failure Recovery of Distributed Systems." *ACM SIGSOFT Software Engineering Notes* 30 (4), 1.

Bonacich, P. and P. Lloyd (2001). "Eigenvector-like Measures of Centrality for Asymmetric Relations." *Social Networks* 23 (3), 191–201.

Brettel, M., N. Friederichsen, M. Keller and M. Rosenberg (2014). "How Virtualization, Decentralization and Network Building Change the Manufacturing Landscape: An Industry 4.0 Perspective." *International Journal of Mechanical, Aerospace, Industrial, and Mechatronics Engineering* (8).

Broy, M., M. V. Cengarle and E. Geisberger (2012). "Cyber-Physical Systems: Imminent Challenges." In: *Large-Scale Complex IT Systems. Development, Operation and Management*. Ed. by Calinescu R., Garlan D. Springer Berlin Heidelberg, p. 1–28.

Buldyrev, S. V., R. Parshani, G. Paul, H. E. Stanley and S. Havlin (2010). "Catastrophic Cascade of Failures in Interdependent Networks." *Nature* 464 (7291), 1025–1028.

Cardenas, A., S. Amin, B. Sinopoli, A. Giani, A. Perrig and S. Shankar (2009). "Challenges for Securing Cyber Physical Systems." *Workshop on Future Directions in Cyber-physical Systems Security*.

Faisal, N. M., D. K. Banwet and R. Shankar (2007). "Information Risks Management in Supply Chains: An Assessment and Mitigation Framework." *Journal of Enterprise Information Management* 20 (6), 677–699.

Fleisch, E. and F. Thiesse (2007). "On the Management Implications of Ubiquitous Computing: An IS Perspective." *Proceedings of the 15th European Conference on Information Systems. St. Gallen, Switzerland.*

Freeman, L. C. (1978). "Centrality in Social Networks Conceptual Clarification." *Social Networks* 1 (3), 215–239.

Haller, S., S. Karnouskos and C. Schroth (2009). "The Internet of Things in an Enterprise Context." In: *Future Internet – FIS 2008*. Ed. by J. Domingue, D. Fensel and P. Traverso. Berlin, Heidelberg: Springer Berlin Heidelberg, p. 14–28.

Hevner, A. R., S. T. March, J. Park and S. Ram (2004). "Design Science in Information Systems Research." *Management Information Systems Quarterly (28:1)*, 75–105.

Iansiti, M. and R. L. Karim (2014). "Digital Ubiquity How Connections, Sensors, and Data Are Revolutionizing Business." *Harvard Business Review 92, no. 11*, 90–99.

Jaisingh, J. and J. Rees (2001). "Value at Risk: A Methodology for Information Security Risk Assessment." *Proceedings of the 6th INFORMS Conference on Information Systems and Technology. Miami, USA.*

Jing, Q., A. V. Vasilakos, J. Wan, J. Lu and D. Qiu (2014). "Security of the Internet of Things: Perspectives and challenges." *Wireless Networks* 20 (8), 2481–2501.

Kagermann, H., W. Wahlster and J. Helbig (2013). "Recommendations for Implementing the Strategic Industrie 4.0."

Lucke, D., C. Constantinescu and E. Westkämper (2008). "Smart Factory - A Step towards the Next Generation of Manufacturing." In: *Manufacturing Systems and Technologies for the New Frontier*. Ed. by M. Mitsuishi, K. Ueda and F. Kimura. London: Springer London, p. 115–118.

Nikoletseas, S., G. Prasinos, P. Spirakis and C. Zaroliagis (2003). “Attack Propagation in Networks.” *Theory of Computing Systems* 36 (5), 553–574.

Nishat Faisal, M., D. K. Banwet and R. Shankar (2007). “Information risks management in supply chains: An assessment and mitigation framework.” *Journal of Enterprise Information Management* 20 (6), 677–699.

Offermann, P., S. Blom, M. Schönherr and U. Bub (2010). “Artifact Types in Information Systems Design Science – A Literature Review.” *Global Perspectives on Design Science Research 77-92*.

Peffers, K., T. Tuunanen, M. A. Rothenberger and S. Chatterjee (2007). “A Design Science Research Methodology for Information Systems Research.” *Journal of Management Information Systems* 24 (3), 45–77.

Radziwon, A., A. Bilberg, M. Bogers and E. S. Madsen (2014). “The Smart Factory: Exploring Adaptive and Flexible Manufacturing Solutions.” *Procedia Engineering* 69, 1184–1190.

Sadeghi, A.-R., C. Wachsmann and M. Waidner (2015). “Security and Privacy Challenges in Industrial Internet of Things.” In: *the 52nd Annual Design Automation Conference*. Ed. by Unknown, p. 1–6.

Sathanur, A. V. and D. J. Haglin (2016). “A Novel Centrality Measure for Network-wide Cyber Vulnerability Assessment.” In: *2016 IEEE Symposium on Technologies for Homeland Security*, p. 1–5.

Schuh, G., T. Potente, C. Wesch-Potente, A. R. Weber and J.-P. Prote (2014). “Collaboration Mechanisms to Increase Productivity in the Context of Industrie 4.0.” *Procedia CIRP* 19, 51–56.

Silva, M. M., A. P. H. de Gusmão, T. Poleto, L. C. e. Silva and A. P. C. S. Costa (2014). “A Multidimensional Approach to Information Security Risk Management Using FMEA and Fuzzy Theory.” *International Journal of Information Management* 34 (6), 733–740.

Sonnenberg, C. and J. Vom Brocke (2012). “Evaluations in the Science of the Artificial – Reconsidering the Build-Evaluate Pattern in Design Science Research.” *Design Science Research in Information Systems. Advances in Theory and Practice*, 381–397.

Wagner, S. M. and N. Neshat (2010). “Assessing the Vulnerability of Supply Chains Using Graph Theory.” *International Journal of Production Economics* 126 (1), 121–129.

Wang, S., J. Wan, Di Li and C. Zhang (2016). “Implementing Smart Factory of Industrie 4.0: An Outlook.” *International Journal of Distributed Sensor Networks* 2016, 1–10.

Xu, X. (2012). “From Cloud Computing to Cloud Manufacturing.” *Robotics and Computer-Integrated Manufacturing* 28 (1), 75–86.

Yoon, J.-S., S.-J. Shin and S.-H. Suh (2012). “A Conceptual Framework for the Ubiquitous Factory.” *International Journal of Production Research* 50 (8), 2174–2189.

Zambon, E., S. Etalle, R. J. Wieringa and P. Hartel (2011). “Model-based Qualitative Risk Assessment for Availability of IT Infrastructures.” *Software & Systems Modeling* 10 (4), 553–580.

Zuehlke, D. (2010). “Smart Factory—Towards a Factory-of-Things.” *Annual Reviews in Control* 34 (1), 129–138.