Risk and Return Management in Digitized Value Networks

Kumulative Dissertation

der Wirtschaftswissenschaftlichen Fakultät

der Universität Augsburg

zur Erlangung des Grades eines

Doktors der Wirtschaftswissenschaften

(Dr. rer. pol.)

Vorgelegt von

Jochen Übelhör

(Master of Science & Master of Business Administration)

Erstgutachter: Prof. Dr. Hans Ulrich Buhl

Zweitgutachter: Prof. Dr. Axel Tuma

Vorsitzende der mündlichen Prüfung: Prof. Dr. Jennifer Kunz

Tag der mündlichen Prüfung: 20.11.2018

„The best way to predict the future is to create it."

Peter F. Drucker

US-American Consultant and Publicist (1909–2005)

Table of Contents

Please note: Tables and figures are consecutively numbered per chapter, and within Chapters II, III, and IV per section (each representing one research paper). References are provided at the end of each section and each research paper, respectively.

Index of Research Papers

This doctoral thesis contains the following research papers:

Research Paper P1: Übelhör J (2019) Industrieunternehmen und die Transformation von Geschäftsmodellen im Kontext der Digitalisierung – Eine empirische Studie über die Auswirkungen anhand des Business Model Canvas.

In: *HMD - Praxis der Wirtschaftsinformatik,* 2019, 56 (2), pp. 453-467 *(VHB-JOURQUAL 3: category D)*

Research Paper P2: Geißler A, Häckel B, Übelhör J, Voit C (2019) Structuring the Anticipated Benefits of the Fourth Industrial Revolution.

In: Proceedings of the *25th Americas Conference on Information Systems*, 2019, Cancun, Mexico *(VHB-JOURQUAL 3: category D)*

Research Paper P3: Freitag B, Häfner L, Pfeuffer V, Übelhör J (2020) Evaluating Investments in Flexible On-Demand Production Capacity – A Real Options Approach.

In: *Business Research,* 2020, 13 (1), pp. 133-161 *(VHB-JOURQUAL 3: category B)*

Research Paper P4: Miehle D, Häckel B, Pfosser S, Übelhör J (2019) Modeling IT Availability Risks in Smart Factories – A Stochastic Petri Nets Approach.

In: *Business & Information Systems Engineering*, 2019 *(VHB-JOURQUAL 3: category B)*

Research Paper P5: Häckel B, Hänsch F, Hertel M, Übelhör J (2019) Assessing IT Availability Risks in Smart Factory Networks.

In: *Business Research,* 2019, 12 (2), pp. 523-558 *(VHB-JOURQUAL 3: category B)*

Research Paper P6: Häckel B, Häfner L, Übelhör J (2018) Toward Strategic Decision Support Systems for Systemic Risk Management.

Under Review in: *Journal of the Association for Information Systems (VHB-JOURQUAL 3: category A)*

I Introduction

Digitalization is one of the megatrends of our days (Collin 2015) affecting all areas of society in an unprecedented speed and embracing all aspects of private and professional lives (Legner et al. 2017). Besides other areas like education or public services, especially the business world experiences significant and rapid changes as technological advancements and technologically driven competition forces companies to innovate constantly to satisfy changing customer demands that shift toward highly individualized offerings (Gimpel and Röglinger 2017; Porter and Heppelmann 2015; Priem et al. 2013; Turber and Smiela 2014). Today, customers are, for instance, able to purchase products with only a few clicks from Amazon or Alibaba, to book accommodation via smartphone applications of AirBnB or trivago, or to conduct financial transactions online offered from N26 or Scalable Capital. For this, companies are engaged in digitized value networks, utilize digital technologies, massive amounts of data, and innovative IT infrastructures, and apply digital business models. Besides industries like online retailing or banking, especially the industrial sector is subject to a dynamic digital transformation induced by "the convergence of the so-called IT megatrends (social, mobile, big data, cloud, smart)" (Legner et al. 2017, p. 303). These offer new opportunities for innovative production processes and disruptive business models as "economy [shifts] from a goods-based to a service-based economy" (Barrett et al. 2012, p. 434) resulting "in a new fundamental paradigm shift in industrial production" (Lasi et al. 2014, p. 239). Examples include, for instance, smart manufacturing concepts, data-based product-service bundles, usage-based provider business models, and digital platforms changing long-established success mechanism in entire industries (Porter and Heppelmann 2015). In response to this dynamic digital transformation, companies have to adapt their business models, invest in digital technologies, develop new service offerings based on hybrid value creation, and engage in digitized value networks to retain competitiveness in highly competitive global markets, to exploit revenue potentials, and to open up new markets (Geisberger and Broy 2015). Along with the adaption of their return management, companies have to consider new risk associated with digital technologies, digitized value networks and digital business models in the course of their risk management due to the increase of information-based, complex dependencies and opaque structures (Broy et al. 2012; Gimpel and Röglinger 2017; Tupa et al. 2017). As digitalization and digital transformation affect all levels of the enterprise architecture and are characterized by high complexity and fast development cycles of digital technologies, companies engaged in digitized value networks

require appropriate methods and processes for risk and return management. Only in this way are they able to exploit the opportunities offered by digitalization, for instance, in the context of hybrid value creation, while at the same time keeping the associated risks manageable.

Despite the omnipresence and relevance of *digitalization* in both academia and practice, there are various ambiguities and opinions regarding its definition, especially in relation to the related term *digitization* (e.g., Legner et al. 2017; Mertens and Wiener 2018; Riedl et al. 2017). Therefore, in this doctoral thesis, these are differentiated according to the majority opinion as follows: While the term *digitization* describes the "technical process of converting analog signals into a digital form, and ultimately into binary digits" in a more narrow sense (Legner et al. 2017, p. 301) and origins from computer science (Tilson et al. 2010; Hess 2016), the term *digitalization* describes "the manifold sociotechnical phenomena and processes of adopting and using […] technologies in broader individual, organizational, and societal contexts" (Legner et al. 2017, p. 301). Focusing on the economic perspective, *digitalization* can also be described as the "ever more intensive and rapid penetration of the economy and society with information and communication technologies and the associated changes with regard to the interconnection of individuals, companies and physical objects" (Gimpel and Röglinger 2017, p. 9). Due to its broader scope, the term *digitalization* is applied in this doctoral thesis in accordance with Legner et al. (2017) to describe the comprehensive transformation of businesses and value networks by adopting and leveraging digital technologies. Since the participle is derived from the verb *to digitized*, the participle *digitized* is applied in the context of value networks, i.e., *digitized value networks*.

Despite its current hype, digitalization is not a new phenomenon (Legner et al. 2017). After previous developments including the dissemination of computers and the internet as a global communication infrastructure, today, we are experiencing a third wave of digitalization (Legner et al. 2017). Thereby, the so-called SMAC technologies (social, mobile, analytics, and cloud), miniaturization, increased processing power, storage capacity, and communication bandwidth enable smart manufacturing environments, data-based product-service bundles, and the development of new digital business models (Lasi et al. 2014; Legner et al. 2017; Porter and Heppelmann 2015). These developments within the industrial sector are referred to under various terms like the Industrial Internet of Things (IIoT), Industry 4.0, Industrial Internet, or Advanced Manufacturing (Lasi et al. 2014). While they differ in their exact definitions, all terms comprise in their inner kernel the comprehensive application of digital technologies in the industrial sector and the extensive integration and internet-based interconnection of intelligent products, processes, and services that are able to communicate

with each other and with people over the Internet (Kagermann et al. 2013, p. 23). Thereby, products and production components generate, share, and process massive amounts of production and product-related data that present an unprecedented potential to optimize production processes and to develop innovative digital services and new digital business models.

Consequently, digitalization promises great economic potentials for industrial companies with respect to digital hybrid value creation. Thereby, *digital hybrid value creation* can be defined as the creation of added value by companies through the combination of specific resources, capabilities, intelligent digital technologies, and the internet-based interconnection of companies and customers through integrated, data-based product-service bundles (Böhmann and Krcmar 2006; Fleisch et al. 2017; Porter and Heppelmann 2015). For instance, a study by Accenture estimates that predictive asset maintenance of machinery enabled by advanced analytics can reduce overall maintenance costs by up to 30% and result in up to 70% fewer breakdowns (Accenture 2015). Further, another study by McKinsey estimates the economic impact of the Internet of Things of $2.7 trillion to 6.2 trillion per year by 2025 (Manyika et al. 2013). These vast economic potentials are of utmost importance for industrial companies as they experience increasing pressure from three sides. First, industrial companies face declining margins in core businesses as competitors from formerly low-wage countries, which used to serve as extended workbenches, are constantly further developing their technological capabilities enabling them to offer competitive products (Kindström 2010). This can be observed in the example of China and its industrial masterplan “Made in China 2025” which strives for technological leadership in various key industries like machinery, robotics, and information technology through concentrated efforts (Wübbeke et al. 2016). Second, market and customer demands increasingly shift towards individualized products, ever decreasing time-to-market, and highly customized solution offerings increasing the importance of highly flexible and efficient production processes and innovative, individualized services and products (Brettel et al. 2014; Römer et al. 2017). Third, there is an intense innovation pressure induced by market entries of start-ups and non-traditional competitors who offer innovative digital services and operate highly agile as they are not bound to traditional business models and complex organizational structures of large firms (Gimpel et al. 2018; Röglinger and Urbach 2017; Römer et al. 2017).

Against this backdrop and to retain competitiveness in dynamically changing markets, companies in all industrial sectors have to undergo a targeted digital transformation evolving their business models, processes, and IT infrastructures to enable digital hybrid value creation.

In this regard, *digital transformation* can be defined as the "socio-technical transformation that affects organizational structures, strategies, IT architectures, methods, and business models" (Legner et al. 2017, p. 303) referring to "the changes imposed by information technologies in the sense of digitization" (Hess 2016). Besides other key areas like *digital leadership* or *customer and partner engagement* (Böhmann et al. 2015), digital transformation requires investments in digital technologies and the development of digitized value networks causing adjustments on every level of the enterprise architecture. The enterprise architecture of a company can be differentiated into five levels as depicted in Figure I.1-1: *Business Model*, *Business Processes*, *People and Application Systems*, *Data and Information*, and *Infrastructure* (Gimpel and Röglinger 2017; Buhl and Kaiser 2008).

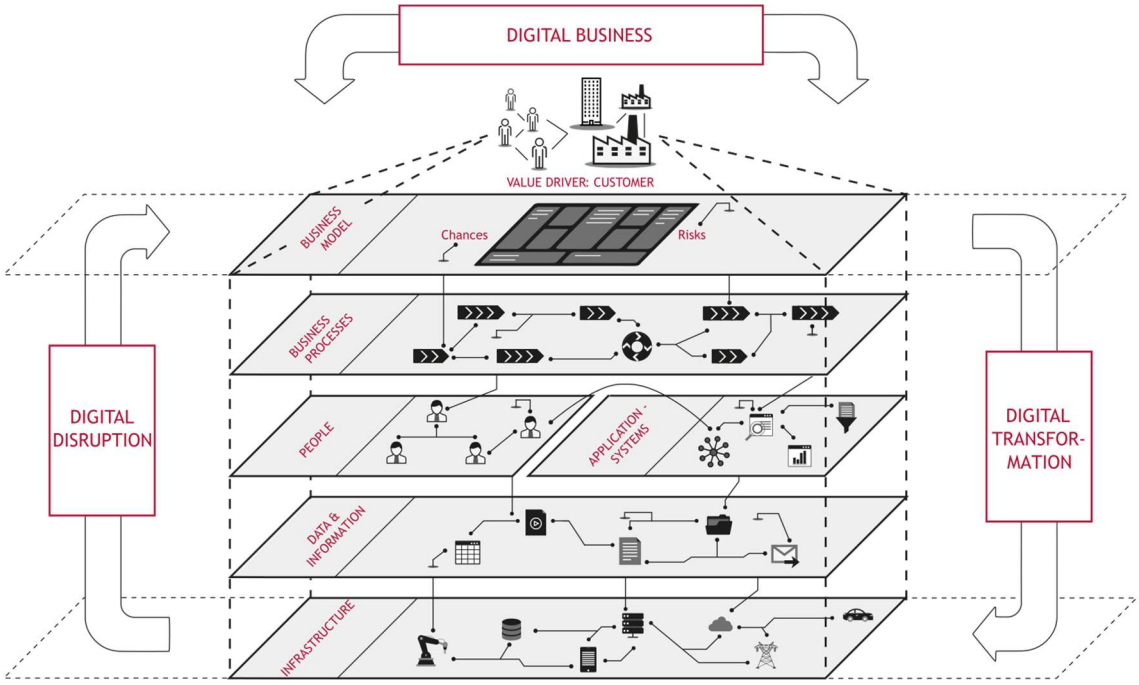


Figure I.1-1: Enterprise Architecture Model for Digital Businesses – Source: Gimpel and Röglinger (2017), building on Buhl and Kaiser (2008)

- *Business Model*: As customers represent the central value drivers for any company, the business model serves to align value creation with company strategy to effectively exploit market potentials. Thereby, digital value creation requires a consistent focus on customer needs. For this, the business model defines the "basic principle according to which an organization creates, conveys and captures values" (Osterwalder and Pigneur 2010, p. 18).
- *Business Processes*: Taking a process-oriented and cross-functional view of companies, business processes specify which tasks must be carried out and how they

are intertwined to fulfil corporate tasks. Thereby, traditional, rather static process concepts must be complemented by agile processes due to the dynamic of digitized value networks (Gimpel et al. 2018).

- *People and Application Systems*: Tasks generated by business processes can be carried out manually by people (internal or external), automatically by application systems (e.g., ERP, MES, CRM) or by a cooperation of both types of task carriers. Thereby, especially the cooperation between humans and machines has to be further developed in the course of digital transformation (Gimpel and Röglinger 2017).
- *Data and Information*: To be able to carry out tasks, data and information are required. These include structured and unstructured data, whose available volume is increasing rapidly due to the comprehensive dissemination and interconnection of intelligent objects generating massive amounts of data (Kiel et al. 2016).
- *Infrastructure*: To exploit the potentials of digital technologies, a suitable infrastructure is required including all hardware components and system software required for technical implementation. Through the use of digital technologies, the traditional information and communication infrastructure is increasingly integrated with the production infrastructure (e.g., machines and workpieces) to so-called *cyber-physical production systems* (CPPS) (Penas et al. 2017).

In the course of digital transformation, companies need to "master the interaction of these levels and to establish structures and processes […] which help to further develop the levels in a coordinated and dynamic manner" (Gimpel and Röglinger 2017, p. 10). This is especially important in digitized value networks as these are characterized by a highly dynamic composition and complex interconnections between value chain partners. Further, the fast development cycles of digital technologies confront companies with the challenge to make fast and reliable strategic decisions regarding the application of digital technologies on all levels of the enterprise architecture (Gimpel and Röglinger 2017). In this regard, there are three fields of action: First, *digital disruption* deals with the assessment of chances and risks of disruptive technologies to differentiate between real opportunities and short-term hypes. Second, *digital business* deals with the development and evaluation of new business models based on digital technologies. And third, *digital transformation* seeks to adapt the underlying levels of the enterprise architecture that new, digitally enhanced value propositions can be delivered (Gimpel and Röglinger 2017). Thereby, companies are in all three fields of action

required to adequately analyze and adjust all levels of the enterprise architecture under consideration of risk and return aspects by means of appropriate methods and processes.

Accordingly, the research work carried out in this doctoral thesis attempts to investigate specific aspects of risk and return management in digitized value networks affecting the different levels of the enterprise architecture under consideration of the three fields of action: digital business, digital transformation, and digital disruption. This includes particularly the analysis of effects of digitalization and digitized value networks on industrial companies, such as their business model, as well as corresponding risks, such as information-based systemic risks in smart factory environments. In order to contribute to the knowledge at the interface between the disciplines of Finance and Information Management, challenges and methods of return management (Chapter II) and risk management (Chapter III) are addressed, evaluated, and adapted in the context of digitized value networks.

Regarding return management: In the course of digital transformation, companies focus first on return management in terms of business model level and particularly revenue side to exploit the potentials enabled by digitalization (Porter and Heppelmann 2015). Thereby, two target dimensions can be distinguished (Kagermann et al. 2013): (i) user dimension and (ii) provider dimension. Considering the user dimension, digital technologies and smart manufacturing concepts applied in production infrastructures and the vertical integration of information systems turn traditional factories into intelligent production facilities, so-called smart factories (Radziwon et al. 2014; Zuehlke 2010). This enables a variety of potential benefits like optimized production processes, increased efficiency and flexibility, improved product quality, and improved supply chain cooperation (Lasi et al. 2014). In the context of digital hybrid value creation, value networks are becoming increasingly distributed among several highly specialized value chain partners, resulting in complex ecosystems (Martín-Peña et al. 2018). Additionally, the improvement of inter-organizational cooperation with value chain partners by means of digital technologies and the horizontal integration of information systems cause an increasing digitalization of value networks (Bharadwaj et al. 2013). From a provider perspective, digital technologies and the generation and sharing of massive amounts of data enable the development of innovative data-based services and new digital business models (Iansiti and Lakhani 2014; Porter and Heppelmann 2015). Thereby, physical functions of products can be enhanced with digital services to integrated, data-based product-service bundles to offer highly individual, customer-centric solution offerings (Fleisch et al. 2017). Through this, companies are able to target new customer segments, to exploit resulting revenue potentials, to open up new markets, and to gain competitive advantages through

differentiation from competitors (Porter and Heppelmann 2014). Accordingly, digital transformation and the comprehensive digitalization of value creation promises a variety of potential benefits for industrial companies both internally and externally. However, digital transformation and the investments in digital technologies confront companies with various challenges regarding their return management. For instance, the development of data-based product-service bundles causes various effects and requires targeted adjustments on every level of the enterprise architecture as the core of value creation shifts from physical products towards digital services. This includes, for example, the development of new value propositions in response to changing customer demands like individual solution offerings instead of product sales, the development of new capabilities like software engineering and data analytics, the engagement with new partners in digital ecosystems like cloud providers, as well as the development of new revenue models like pay-per-use or gain-share to monetarize on the values generated by digital services. Further, companies must evaluate ex-ante their investments into specific technologies under consideration of the involved costs, risks, and benefits. Thereby, especially the evaluation of benefits remains a major obstacle for value-based investment decisions as the variety, complexity, and the fast development cycles of digital technologies complicate the identification and quantification of associated benefits. Thus, companies developing a sound digitalization strategy require guidance and appropriate methods to ensure a comprehensive return management that enables exploiting the benefit potential of digitalization. This challenge is addressed in Chapter II of this doctoral thesis.

Regarding risk management: The digital transformation of business models, processes, and IT infrastructures, the application of digital technologies and the comprehensive interconnection of production infrastructures, products, customers, and value chain partners within digitized value networks creates a variety of new risks. For instance, the application of digital technologies bears considerable investment risks, especially considering the fast development cycles of digital technologies. Further, the development of new digital business models confronts companies with additional risks as companies open up new, unknown markets and customers segments, and act as first movers. Additionally, companies face an increased complexity of their overall value network and increasingly complex, information-based dependencies (Geisberger and Broy 2015; Tupa et al. 2017). Thereby, especially information-based risks are of utmost importance as the proper functioning of information systems and the reliable flow of information have become a prerequisite for the reliable operation of production infrastructures and digital services (Tupa et al. 2017; Yoon et al. 2012; Zuehlke 2010). Consequently, risk management is confronted with a variety of different

aspects in the context of digitalization and digitized value networks. As the increasing vulnerability of production infrastructures to IT security breaches represent a central challenge for risk management, this doctoral thesis focusses on information-based risks in relation to IT security breaches in smart manufacturing environments. This represents a highly relevant topic as formerly isolated production facilities become increasingly connected to external information systems over the internet due to external services like remote maintenance and inter-organizational information systems (Smith et al. 2007; Tupa et al. 2017; Yoon et al. 2012). Thereby, due to informational interdependencies within digitized value networks, single point failures can spread into the entire value network and may result in its complete breakdown. These threat scenarios can be observed on various incidents like the cyber-attacks *WannaCry*, *Petya*, or *Locky*, that resulted in production downtimes and affected numerous companies like Beiersdorf, Honda, Maersk, Merck, Mondelez, Nissan, Renault, Rosneft (Handelsblatt 2018; Spiegel Online 2017; Forbes 2017). The relevance of such threat scenarios was also confirmed by a study of the German Federal Office for Information Security that revealed that 70% of 900 surveyed companies have been exposed to cyber-attacks in the past two years. Thereby, every second successful attack resulted in production downtime or a failure of operations (BSI 2017). Another study by PwC revealed that the number of cyber-attacks on businesses rose by 38% in 2015 (PwC 2016). At the same time, the complexity and dynamics of digitized value networks and the inherent dependency structures complicate risk management for companies as appropriate methods are often times missing. Against this backdrop, companies have to deal with the new risks associated with digitized value networks and digital businesses in the course of their risk management as part of their business activities in a proactive manner. For this, risk management can be structured along the risk management cycle into the four phases (1) identification, (2) quantification, (3) controlling, and (4) monitoring (Hallikas et al. 2004). Only by identifying the most critical points of digitized value networks, economically sound security investments can be derived. For this, companies require appropriate methods and processes for their risk management in digitized value networks. This challenge is addressed in Chapter III of this doctoral thesis.

In summary, the digital transformation of companies and investments in digitized value networks poses challenges regarding risk and return management under consideration of all levels of the enterprise architecture, which are addressed in this doctoral thesis. The following Section I.1 illustrates the objectives and structure of the doctoral thesis. In the subsequent Section I.2, the corresponding research papers are embedded in the research context and the fundamental research questions are highlighted.

I.1 Objectives and Structure of this Doctoral Thesis

The main objective of this doctoral thesis is to contribute to the field of Finance and Information Management by focusing on the developments of digitized value networks and by addressing specific challenges regarding risk and return management as introduced above. Table I.1-1 provides an overview of the pursued objectives and the structure of the doctoral thesis.

I Introduction	
Objective I.1:	Outlining the objectives and the structure of the doctoral thesis
Objective I.2:	Embedding the included research papers into the context of the doctoral thesis and formulating the fundamental research questions
II Return Management in Digitized Value Networks (Research Papers 1–3)	
Objective II.1:	Determining the effects and challenges resulting from the development of digital business models in the context of digital, hybrid value creation
Objective II.2:	Identifying and structuring the anticipated benefits of digital technologies in the context of digitalization of the industrial sector
Objective II.3:	Developing an approach to evaluate investments in flexible on-demand production capacity in digitized production infrastructures
III Risk Management in Digitized Value Networks (Research Papers 4–6)	
Objective III.1:	Developing a novel approach to model smart factory information networks and simulate IT availability risks
Objective IIII.2:	Developing a risk assessment model to model interdependencies between the information network and production network of smart factories and to quantify IT availability risks for the identification of critical nodes
Objective IIII.3:	Developing a generic architecture for an information system to identify and analyze systemic risks and to provide strategic decision support in digitized value networks
IV Results and Future Research	
Objective IV.1:	Presenting the key findings of the doctoral thesis
Objective IV.2:	Identifying and highlighting areas for future research

Table I.1-1: Objectives and structure of the doctoral thesis

I.2 Research Context and Research Questions

In the following, the research questions of chapters II and III including research papers P1 to P6 are motivated. As digital transformation affects all levels of the enterprise architecture in regard to aspects related to risk and return management, this doctoral thesis distinguishes between return management (Chapter II) and risk management (Chapter III).

In Chapter II, research paper P1 is set up on the *business model level* and deals with the impacts and challenges resulting from the development of digital business models in the context of digital hybrid value creation. Research paper P2 can be assigned to *digital disruption* and investigates the anticipated benefits of the application of digital technologies in the context of smart manufacturing environments enabling new, innovative business models. Research paper P3 with the evaluation of investments for flexible on-demand capacity as a means for increased production flexibility addresses a topic concerning *digital transformation*. In Chapter III, research papers P4 and P5 address the modeling of IT infrastructures, production environments, and informational dependencies in smart factory environments and the subsequent analysis of information-based risk. Research paper P6 addresses processes and systems for risk management and develops a generic architecture for systemic risk management. Figure I.2-1 provides an overview of the papers included in this doctoral thesis.

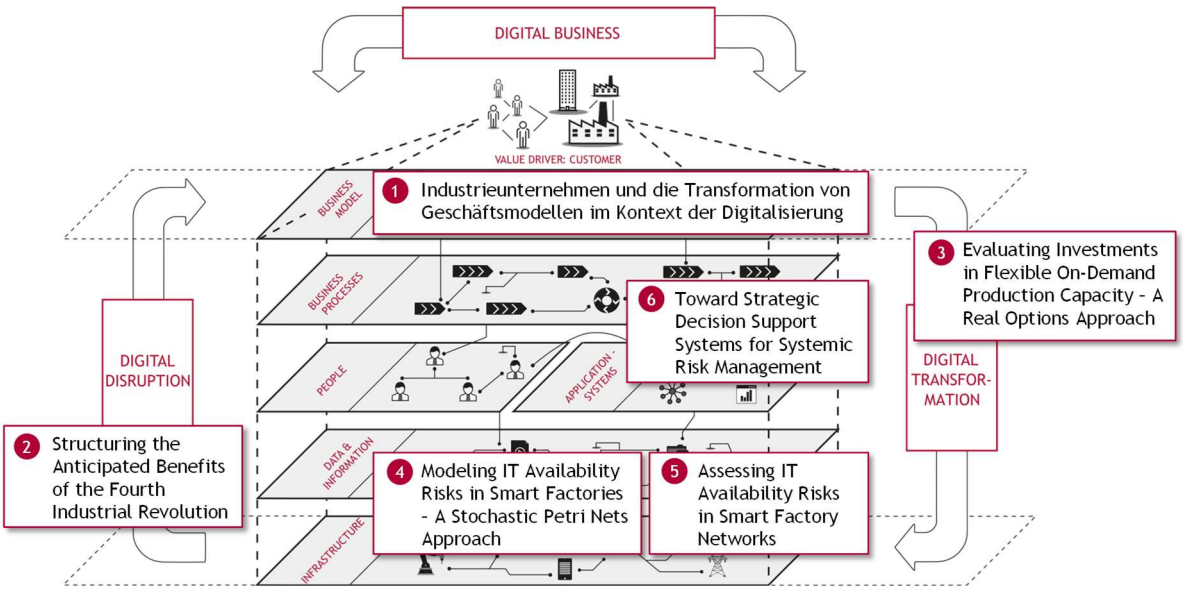


Figure I.2-1: Research papers included in the doctoral thesis – Own illustration, building on Gimpel and Röglinger (2017) and Buhl and Kaiser (2008)

In the following, the research papers included in this doctoral thesis are embedded in the research context, and the research questions are motivated with respect to the above stated objectives.

I.2.1 Chapter II: Return Management in Digitized Value Networks

Research Paper P1: *"Industrieunternehmen und die Transformation von Geschäftsmodellen im Kontext der Digitalisierung – Eine empirische Studie über die Auswirkungen anhand des Business Model Canvas"*

Research Paper P2*: "Structuring the Anticipated Benefits of the Fourth Industrial Revolution"*

Research Paper P3*: "Evaluating Investments in Flexible On-Demand Production Capacity – A Real Options Approach"*

The comprehensive digital transformation and application of digital technologies promises great potentials for companies in the industrial sector (Iansiti and Lakhani 2014; Lasi et al. 2014). To exploit new market potentials and to generate competitive advantages, companies focus first on return management in terms of their business model and revenue side. Regarding the provider perspective, digital hybrid value creation by means of innovative, data-based product-service bundles present a promising option as the generation, collection, and analysis of massive amounts of data enable highly individualized services for customers. For this, companies are required to adapt all aspects of their business model including the application of innovative digital technologies as key resources like cloud computing, big data analytics, or blockchain, and the development of new capabilities like software development as the focus of value creation shifts from physical products towards digital services. At the same time, digital technologies and smart manufacturing approaches are applied internally and within the value network to optimize value creation. However, the variety of digital technologies, their fast development cycles, and countless application possibilities on both the provider side and the user side complicate the evaluation of potential effects and subsequent investment decision processes. Besides transformational effects like the development of new capabilities or the cooperation with new partners, this applies in particular for potential benefits of digital technologies. While much research deals with effects and benefits of specific digital technologies (e.g., Herterich et al. 2015; Michniewicz and Reinhart 2016; Yang et al. 2016), a holistic perspective on the effects of digital transformation and digital technologies has been rather neglected in scientific literature. Accordingly, as companies face various challenges regarding an appropriate return management, this doctoral thesis contributes to closing this gap by investigating the effects of digital transformation and digital technologies, especially regarding the overall business model level, and the effects of digital technologies within smart manufacturing environments, and by providing an approach for the economically sound

evaluation of investments in digital technologies, especially regarding investments enabling the commissioning of flexible on-demand capacity that becomes feasible in digitized production infrastructures.

Research paper P1 provides results from an empirical study in which the effects and challenges of digital hybrid value creation on business models of industrial companies were investigated. In order to structure the effects and challenges, the Business Model Canvas (BMC) developed by Osterwalder and Pigneur (2010) was applied as an established method for business model development. On the basis of a literature review, real-world examples, and five interviews with experts from companies in different key industries, the paper presents key impacts and resulting challenges for every segment of the BMC. To demonstrate the developments associated with digitalization, research paper P1 presents a case study based on the example of Mitsubishi Electric. Furthermore, practical recommendations are introduced as starting points for the targeted transformation of business models. In sum, research paper P1 mainly focuses on the overall business model level, as depicted in Figure I.2-1. By addressing the following research questions, research paper P1 provides practical guidance for the targeted development of hybrid, data-based product-service bundles in the context of digital hybrid value creation:

- What effects and challenges are associated with the development of digital business models in the context of digital hybrid value creation?
- Which practical recommendations for action can be derived for companies?

Research paper P2 investigates the anticipated benefits of digital technologies in the context of smart manufacturing as companies face a fierce pressure to transform their business practices and success models in a proactive manner. To lay the ground for the subsequent economic evaluation of investments into digital technologies including the identification and quantification of potential benefits, scientific literature was analyzed based on a structured literature review and identified benefits were structured and categorized by means of an established framework for information systems (IS) benefits. By presenting 21 benefits within the four dimensions *operational*, *managerial*, *strategic*, and *organizational*, a comprehensive overview of benefits of digital technologies in the context of smart manufacturing is provided. Further, managerial implications resulting from the variety of benefits and their dependencies are presented. Accordingly, research paper P2 can be assigned to digital disruption, as depicted in Figure I.2-1. By addressing the following research questions, research paper P2 provides an

essential first step towards the economically sound evaluation of digital technologies in accordance with value-based management principles:

- Which benefits of Industry 4.0 are anticipated in scientific literature?
- How can the benefits of Industry 4.0 be categorized?

Research paper P3 deals with investments of manufacturing companies enabling the usage of flexible on-demand production capacity provided by external capacity providers. As development and lifecycles of products accelerate and customer preferences shift towards highly individualized products that cannot be economically produced for stock, customer demand becomes increasingly volatile requiring manufacturing companies to apply flexible make-to-order-concepts. For this, the commissioning of external capacity providers represents an interesting option for volume flexibility in terms of capacity planning to expand the rather rigid internal production capacity as needed. However, significant upfront investments, for instance, for inter-organizational information systems, are required to enable the flexible commissioning of on-demand production capacity. To consider these costs as well as uncertainty of volatile customer demand, research paper P3 presents an Expanded Net Present Value approach based on real options analysis in a discrete-time binomial tree model that is able to capture flexibility of action and to evaluate investments under uncertainty. The model is evaluated by means of a simulation and sensitivity analyses. Accordingly, research paper P3 can be assigned to digital transformation as it enables investments in digital technologies that contribute to the flexibility of production as part of innovative business models (cf. Figure I.2-1). By addressing the following research question, research paper P3 provides a model for the evaluation of upfront investments for the derivation of a profound economical basis for investment decisions:

- How can an industrial company evaluate investments in flexible on-demand production capacity considering flexibility of action and uncertainty?

I.2.2 Chapter III: Risk Management in Digitized Value Networks

Research Paper P4: *"Modeling IT Availability Risks in Smart Factories – A Stochastic Petri Nets Approach"*

Research Paper P5: *"Assessing IT Availability Risks in Smart Factory Networks"*

Research Paper P6: *"Toward Strategic Decision Support Systems for Systemic Risk Management"*

Due to the importance of information systems in digitized value networks, information-based risks are a major challenge for risk management in the context of digitalization of the industrial sector as digitized value networks are increasingly vulnerable to IT security risks (Tupa et al. 2017). Reasons for this are the increasing interconnection within digitized value networks with a large number of intelligent products and production components that are connected via the internet with cloud-based applications for the centralized analysis of data, opening further entry points for malicious attacks. Further, digitized production infrastructures, i.e., smart factories, are increasingly interconnected to value chain partners opening numerous entry points to formerly isolated information systems. Thereby, the informational dependencies among products, production components and value chain partners result in the occurrence of value network instabilities, as single point failures caused by unintentional errors or intentional attacks can spread into the entire value network without any physical connection. Ultimately, the resulting cascading failures can cause a complete breakdown of the value network. Concurrently, the increasing complexity of smart factory environments and digitized value networks complicate the corresponding risk management, especially regarding the identification and quantification of information-based risks. Thereby, complex network structures and the ever stronger dependencies between information systems and the physical production and product environment as well as the numerous active components involved result in highly complex information-based dependency structures complicating risk management in digitized value networks. Accordingly, as companies face various challenges regarding an appropriate risk management, this doctoral thesis contributes to research by developing appropriate approaches for the modeling of smart information networks and the analysis of information-based risk, especially regarding IT availability risks, and by developing a generic architecture for a strategic decision support system for systemic risk management.

Research paper P4 deals with the modeling of smart factory information networks as digitized production infrastructures are increasingly intertwined with information and communication

technology and depend on the availability of information networks. Due to informational interdependencies between its components, single point failures caused by attacks or errors can propagate in the entire network resulting in cascading failures that ultimately jeopardize the operational capability of the information network and, consequently, the functionality of the entire smart factory. Against this backdrop, research paper P4 presents a novel modeling approach based on generalized stochastic petri nets for the modeling of complex information networks, its components, and inherent informational dependencies enabling the simulation and analysis of IT availability risks and their propagation within the information network. To demonstrate the feasibility and usability of the developed approach, different worst-case threat scenarios are investigated regarding their impact on the operational capability of an information network. Further, interviews with experts from both practice and academia are conducted to complement the evaluation. Regarding the enterprise architecture depicted in Figure I.2-1, research paper P4 can be allocated on the infrastructure and information level. By addressing the following research questions, research paper P4 provides a modeling approach for the analysis of IT availability risks, cascading failures, and propagation effects in information networks in digitized production environments:

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

Research paper P5 is concerned with informational dependencies in complex smart factory networks, which are increasingly vulnerable to IT security risks due to the central role of information systems. This includes especially IT availability risks as smart factory networks and the proper functioning of the production infrastructure rely on communication and real-time information synchronization and, thus, depend on the underlying IT systems. However, complex network structures of information network and production networks, the magnitude of involved components as well as inherent dependency relations complicate investment decisions in targeted IT security measures. Against this backdrop, research paper P5 presents a risk assessment model based on graph theory, matrix notation and Value at Risk for the modeling of interdependencies between the information network and production network of smart factories and for the quantification of IT availability risks. In contrast to research paper P4 that focusses on the modeling of an information network, the risk assessment model presented in research paper P5 considers both the information network and the production network as well as their interdependencies. However, research paper P5 addresses also the infrastructure and information level of the enterprise architecture, as depicted in Figure I.2-1.

By addressing the following research questions, research paper P5 provides a profound economic basis for investment decision on IT security measures in complex smart factory networks:

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

Research paper P6 deals with the comprehensive management of systemic risk as companies are increasingly vulnerable to systemic risk due to the increasing interdependencies and complexities of digitized value networks. Thereby, risks that occur at local parts of value networks have the potential to spread into the entire value network and to threaten the business operations of distant business partners. However, the complexity of value networks and the lack of transparency complicate risk management. Thus, companies are often times not able to comprehensibly assess their embeddedness and interconnectedness within value networks that would be necessary for managerial decisions, e.g. regarding sourcing decisions. Accordingly, companies require appropriate decision support systems and the assistance of IS technology that gather, process, and interpret information from diverse sources. For this, research paper P6 develops a generic architecture for a strategic decision support system for systemic risk management. Furthermore, to show potentials for future research, challenges are discussed and research question are presented that have to be solved for the implementation of an appropriate decision support system. Accordingly, research paper P6 addresses processes and systems for risk management, as depicted in Figure I.2-1. By addressing the following research questions, research paper P6 supports the realization of a strategic decision support system for systemic risk management:

- What is an appropriate generic architecture for a DSS that is capable of identifying systemic risks, analyzing those risks, and providing strategic decision support in digitized value networks?

I.2.3 Chapter IV: Results and Future Research

After this introduction, which aims at outlining the objectives and the structure of the doctoral thesis as well as at motivating the research context and formulating the research questions, the research papers are presented in chapters II and III. Subsequently, Chapter IV presents the key findings and highlights areas for future research in the fields of risk and return management in digitized value networks.

I.3 References

Accenture (2015): Smart Production – Finding a Way Forward: How Manufacturers can make the most of the Industrial Internet of Things. Accenture. Available online at https://www.accenture.com/_acnmedia/PDF-5/Accenture-804893-Smart-Production-POV-Final.pdf, checked on 8/12/2018.

Barrett, Michael; Davidson, Elizabeth; Fayard, Anne Laure; Vargo, Stephen L.; Yoo, Youngjin (2012): Being Innovative about Service Innovation: Service, design and digitalization. In *Proceedings of the 33rd International Conference on Information Systems*, Orlando, Florida, United States, pp. 433–438.

Bharadwaj, Anandhi; El Sawy, Omar A.; Pavlou, Paul A.; Venkatraman, N. Venkat (2013): Digital Business Strategy: Toward a Next Generation of Insights. In *MIS Quarterly* 37 (2), pp. 471–482.

Böhmann, Tilo; Drews, Paul; Meyer-Blankart, Corvin (2015): Digitale Exzellenz – Eine Bestandsaufnahme zur Digitalisierung deutscher Unternehmen und Behörden. Research Report. Universität Hamburg. Available online at https://www.soprasteria.de/docs/librariesprovider33/Studien/digitale-exzellenz-2015-expose-steria.pdf?sfvrsn=4, checked on 8/2/2018.

Böhmann, Tilo; Krcmar, Helmut (2006): Komplexitätsmanagement als Herausforderung hybrider Wertschöpfung im Netzwerk. In Franz Wojda, Alfred Berth (Eds.): Innovative Kooperationsnetzwerke. 1. Aufl.: DUV Deutscher Universitäts-Verlag (Schriftenreihe der Hochschulgruppe für Arbeits- und Betriebsorganisation), pp. 81–105.

Brettel, Malte; Friederichsen, Niklas; Keller, Michael; Rosenberg, Marius (2014): How Virtualization, Decentralization and Network Building Change the Manufacturing Landscape: An Industry 4.0 Perspective. In *International Journal of Information and Communication Engineering* 8 (1), pp. 37–44.

Broy, Manfred; Cengarle, María Victoria; Geisberger, Eva (2012): Cyber-Physical Systems. Imminent Challenges. In Radu Calinescu, David Garlan (Eds.): Large-scale complex IT systems. Development, operation and management; 17th Monterey Workshop 2012, Oxford, UK, March 19–21, 2012; revised selected papers, vol. 7539. Berlin: Springer (Lecture Notes in Computer Science, 7539), pp. 1–28.

BSI (2017): Cyber-Sicherheits-Umfrage 2017 – Cyber-Risiken, Meinungen und Maßnahmen. Bundesamt für Sicherheit in der Informationstechnik. Available online at

https://www.bsi.bund.de/SharedDocs/Downloads/ACS/cyber-sicherheits-umfrage_2017.pdf;jsessionid=E8E33481F32B0BA6F63A0ADD24736BAF.1_cid341?__blob=publicationFile&v=3, checked on 8/2/2018.

Buhl, Hans Ulrich; Kaiser, Marcus (2008): Herausforderungen und Gestaltungschancen aufgrund von MiFID und EU-Vermittlerrichtlinie in der Kundenberatung. In *Zeitschrift für Bankrecht und Bankwirtschaft* 20 (1), pp. 43–52.

Collin, Jari (2015): Digitalization and Dualistic IT. In Jari Collin, Kari Hiekkanen, Janne J. Korhonen, Marco Halén, Itälä, timo, Mika Helenius (Eds.): IT Leadership in Transition – The Impact of Digitalization on Finnish Organizations, pp. 29–34.

Fleisch, Elgar; Weinberger, Markus; Wortmann, Felix (2017): Geschäftsmodelle im Internet der Dinge. In Stefan Reinheimer (Ed.): Industrie 4.0. Herausforderungen, Konzepte und Praxisbeispiele. Wiesbaden: Springer Vieweg (Edition HMD), pp. 1–16.

Forbes (2017): Cyber Attack at Honda Stops Production After WannaCry Worm Strikes. Edited by Forbes. Forbes. Available online at https://www.forbes.com/sites/peterlyon/2017/06/22/cyber-attack-at-honda-stops-production-after-wannacry-worm-strikes/#463c8fc5e2b7, updated on 6/22/2017, checked on 8/12/2018.

Geisberger, Eva; Broy, Manfred (2015): Living in a networked world: Integrated research agenda Cyber-Physical Systems (agenda CPS): Herbert Utz Verlag.

Gimpel, Henner; Röglinger, Maximilian (2017): Disruptive Technologien — Blockchain, Deep Learning & Co. In *Wirtschaftsinformatik & Management* 9 (5), pp. 8–15.

Gimpel, Henner; Sabiölla, Hosseini; Huber, Rocco; Probst, Laura; Röglinger, Maximilian; Faisst, Ulrich (2018): Structuring Digital Transformation – A Framework of Action Fields and its Application at ZEISS. In *Journal of Information Technology Theory and Application* 19 (1), pp. 31–54.

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

Handelsblatt (2018): Kleiner Angriff, große Wirkung. Hackerattacken kommen Unternehmen teuer zu stehen. Den Schaden zu berechnen ist schwierig. In *Handelsblatt* 2018, 8/4/2018 (149), p. 16.

Herterich, Matthias M.; Uebernickel, Falk; Brenner, Walter (2015): The Impact of Cyber-physical Systems on Industrial Services in Manufacturing. In *Procedia CIRP* 30, pp. 323–328.

Hess, Thomas (2016): Digitalisierung. Edited by Norbert Gronau, Jörg Becker, Natalia Kliewer, Jan Marco Leimeister, Sven Oberhage (Enzyklopädie der Wirtschaftsinformatik – Online Lexikon). Available online at http://www.enzyklopaedie-der-wirtschaftsinformatik.de/lexikon/technologien-methoden/Informatik--Grundlagen/digitalisierung/index.html/, updated on 11/23/2016, checked on 8/11/2018.

Iansiti, Marco; Lakhani, Karim R. (2014): Digital Ubiquity. How Connections, Sensors, and Data Are Revolutionizing Business. In *Harvard Business Review* 92 (11), pp. 90–99.

Kagermann, Henning; Helbig, Johannes; Hellinger, Ariane; Wahlster, Wolfgang (2013): Recommendations for implementing the strategic initiative Industrie 4.0: Securing the future of German manufacturing industry. Final Report of the Industrie 4.0 Working Group. Munich, Germany.

Kiel, Daniel; Arnold, Chrstian; Collisi, Matthias; Voigt, Kai-Ingo (2016): The Impact of the Industrial Internet of Things on Established Business Models. In *Proceedings of the 25th International Association for Management of Technology Conference*.

Kindström, Daniel (2010): Towards a service-based business model – Key aspects for future competitive advantage. In *European Management Journal* 28 (6), pp. 479–490.

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

Legner, Christine; Eymann, Torsten; Hess, Thomas; Matt, Christian; Böhmann, Tilo; Drews, Paul et al. (2017): Digitalization. Opportunity and Challenge for the Business and Information Systems Engineering Community. In *Business & Information Systems Engineering* 59 (4), pp. 301–308.

Manyika, James; Chui, Michael; Bughin, Jacques; Dobbs, Richard; Bisson, Peter; Marrs, Alex (2013): Disruptive Technologies: Advances that Will Transform Life, Business, and the Global Economy. In *McKinsey Global Institute*, pp. 1–176.

Martín-Peña, María Luz; Díaz-Garrido, Eloísa; Sánchez-López, José María (2018): The digitalization and servitization of manufacturing: A review on digital business models. In *Strategic Change* 27 (2), pp. 91–99.

Mertens, Peter; Wiener, Martin (2018): Riding the Digitalization Wave. Toward a Sustainable Nomenclature in Wirtschaftsinformatik. In *Business & Information Systems Engineering* 60 (4), pp. 367–372.

Michniewicz, Joachim; Reinhart, Gunther (2016): Cyber-Physical-Robotics – Modelling of modular robot cells for automated planning and execution of assembly tasks. In *Mechatronics* 34, pp. 170–180.

Osterwalder, Alexander; Pigneur, Yves (2010): Business Model Generation. A Handbook for Visionaries, Game Changers, and Challengers. Hoboken, NJ: Wiley.

Penas, Olivia; Plateaux, Régis; Patalano, Stanislao; Hammadi, Moncef (2017): Multi-scale approach from mechatronic to Cyber-Physical Systems for the design of manufacturing systems. In *Computers in Industry* 86, pp. 52–69.

Porter, Michael E.; Heppelmann, James E. (2014): How smart connected products are transforming competition. In *Harvard Business Review* 92 (11), pp. 64–88.

Porter, Michael E.; Heppelmann, James E. (2015): How smart connected products are transforming companies. In *Harvard Business Review* 93 (10), pp. 96–114.

Priem, Richard L.; Butler, John E.; Li, Sali (2013): Toward Reimagining Strategy Research. Retrospection and Prospection on the 2011 AMR Decade Award Article. In *Academy of Management Review* 38 (4), pp. 471–489.

PwC (2016): Turnaround and Transformation in Cybersecurity. Key findings from The Global State of Information Security Survey 2016. PriceWaterhouseCoopers. Available online at https://www.pwc.com/sg/en/publications/assets/pwc-global-state-of-information-security-survey-2016.pdf, checked on 8/2/2018.

Radziwon, Agnieszka; Bilberg, Arne; Bogers, Marcel; Madsen, Erik Skov (2014): The Smart Factory: Exploring Adaptive and Flexible Manufacturing Solutions. In *Procedia Engineering* 69, pp. 1184–1190.

Riedl, René; Benlian, Alexander; Hess, Thomas; Stelzer, Dirk; Sikora, Hermann (2017): On the Relationship Between Information Management and Digitalization. In *Business & Information Systems Engineering* 59 (6), pp. 475–482.

Röglinger, Maximilian; Urbach, Nils (2017): Digitale Geschäftsmodelle im Internet der Dinge. In *Geschäftsmodelle in der digitalen Welt*, pp. 77–94.

Römer, Michael; Röglinger, Maximilian; Linhart, Alexander; Schmidl, Jörg; Utz, Lena; Venus, Michael (2017): Designing IT Setups in the Digital Age. In *AT Kearney and Project Group Business and Information Systems Engineering of Fraunhofer Institute for Applied Information Technology FIT*, pp. 1–12.

Smith, G. E.; Watson, K. J.; Baker, W. H.; Pokorski II, J. A. (2007): A Critical Balance: Collaboration and Aecurity in the IT-Enabled Supply Chain. In *International Journal of Production Research* 45 (11), pp. 2595–2613.

Spiegel Online (2017): Hacker legen weltweit Firmen lahm. Großangelegte Cyberattacke. Edited by Spiegel Online. Spiegel Online. Available online at http://www.spiegel.de/netzwelt/web/maersk-hacker-legen-computer-von-groesster-reederei-der-welt-lahm-a-1154696.html, checked on 8/12/2018.

Tilson, David; Lyytinen, Kalle; Sørensen, Carsten (2010): Research Commentary —Digital Infrastructures. The Missing IS Research Agenda. In *Information Systems Research* 21 (4), pp. 748–759.

Tupa, Jiri; Simota, Jan; Steiner, Frantisek (2017): Aspects of Risk Management Implementation for Industry 4.0. In *Procedia Manufacturing* 11, pp. 1223–1230.

Turber, Stefanie; Smiela, Christoph (2014): A Business Model Type for the Internet of Things. In *Proceedings of the 22nd European Conference on Information Systems*.

Wübbeke, Jost; Meissner, Mirijam; Zenglein, Mxax J.; Ives, Jaqueline; Conrad, Björn (2016): Made in China 2025 – The making of a high-tech superpower and consequences for industrial countries. In *merics Papers on China – Mercator Institute for China Studies 2.*

Yang, Zhixin; Zhang, Pengbo; Chen, Lei (2016): RFID-enabled indoor positioning method for a real-time manufacturing execution system using OS-ELM. In *Neurocomputing* 174, pp. 121–133.

Yoon, Joo-Sung; Shin, Seung-Jun; Suh, Suk-Hwan (2012): A Conceptual Framework for the Ubiquitous Factory. In *International Journal of Production Research* 50 (8), pp. 2174–2189.

Zuehlke, Detlef (2010): SmartFactory—Towards a factory-of-things. In *Annual Reviews in Control* 34 (1), pp. 129–138.

II Return Management in Digitized Value Networks

This chapter deals with the potentials of the comprehensive digital transformation and the application of digital technologies in the industrial sector as companies focus first on return management in terms of their business model and revenue side and evaluate which investments are the most promising. Corresponding investment decisions in line with value-based management principles have to be made under consideration of involved costs, risks, and benefits. Accordingly, an integrated view of risks and returns is necessary. On the one hand, this requires a holistic perspective on the effects of digital technologies due to their complexity, dynamics, and diverse application possibilities. For this, research papers P1 and P2 investigate chances and challenges of digital transformation and digital technologies on the overall business model level and within smart manufacturing environments. On the other hand, the return expectations of business decisions cannot be evaluated isolated from the associated risks. In this respect, research paper P3 presents an approach for the evaluation of investment that considers costs, benefits, and risks originating from uncertainty of demand. Thus, this chapter includes the following three research papers:

The first research paper P1 „*Industrieunternehmen und die Transformation von Geschäftsmodellen im Kontext der Digitalisierung – Eine empirische Studie über die Auswirkungen anhand des Business Model Canvas*“ (Section II.1) investigates the effects and challenges of digital hybrid value creation on business models of industrial companies. Further, a real-world case study and practical recommendations for a targeted digital transformation of business models are presented.

The second research paper P2 “*Structuring the Anticipated Benefits of the Fourth Industrial Revolution*” (Section II.2) focuses on the anticipated benefits of digital technologies within smart manufacturing environments and presents a structured overview of benefits in a four-dimensional framework. Further, managerial implications for both research and practice are discussed.

The third research paper P3 “*Evaluating Investments in Flexible On-Demand Production Capacity – A Real Options Approach*” (Section II.3) introduces an investment evaluation approach on the basis of real option analysis that captures flexibility of external on-demand production capacity and uncertainty of volatile customer demand.

II.1 Research Paper 1: "Industrieunternehmen und die Transformation von Geschäftsmodellen im Kontext der Digitalisierung – Eine empirische Studie über die Auswirkungen anhand des Business Model Canvas"[1]

Authors:	Jochen Übelhör[a,b] [a] Research Center Finance & Information Management, Department of Information Systems Engineering & Financial Management (Prof. Dr. Hans Ulrich Buhl), University of Augsburg jochen.uebelhoer@fim-rc.de [b] Project Group Business & Information Systems Engineering of the Fraunhofer FIT, Augsburg, Germany

In:	HMD - Praxis der Wirtschaftsinformatik, 2019, 56 (2), pp. 453-467

Abstract:

The paper examines the impact of digitalization on industrial companies' business models in the context of the development of integrated, data-based product-service bundles. Examples of this are manufacturers of automation robots that offer their customers digital services for intelligent control, optimization or maintenance in addition to their core physical product. By analyzing the data generated during ongoing operations, it is possible to create new customized solutions and thus generate additional customer benefits. Industrial companies can thus generate decisive competitive advantages and open up new markets by developing digital business models. The paper first examines the effects of digitalization on industrial companies' business models and uses the Business Model Canvas as an established method for business model development to present and evaluate them in a structured way. On the basis of five interviews with experts from leading companies in various key industries, key impacts, the resulting challenges, and practical recommendations for action are discussed and derived. The developments associated with digitalization are illustrated by a case study based on the example of Mitsubishi Electric. The paper introduces practitioners to the effects

[1] This is a post-peer-review version of an article published in HMD - Praxis der Wirtschaftsinformatik, 2019, 56(2), pp. 453-467. The final authenticated version is available online at: https://doi.org/10.1365/s40702-018-0429-3

of the digital transformation of business and provides starting points for the transition to digital hybrid value creation.

II.1.1 Digitalisierung als Wegbereiter der digitalen, hybriden Wertschöpfung

Die Digitalisierung bietet Industrieunternehmen erhebliches ökonomisches Potential durch die Entwicklung integrierter, datenbasierter Produkt-Dienstleistungsbündel. So ergab eine Umfrage unter 235 Industrieunternehmen, dass diese durch digitalisierte Produkte und Dienstleistungen allein bis 2020 Umsatzsteigerungen von durchschnittlich 12,5% erwarten. Hochgerechnet auf die deutsche Industrie entspricht dies einem Umsatzplus von über 30 Mrd. Euro p.a. (Koch et al. 2014). Wesentliche Grundlage hierfür sind Entwicklungen rund um das Internet der Dinge und die sog. Industrie 4.0, zu denen neben innovativen digitalen Technologien wie cyber-physischen Systemen, Cloud Computing, Big Data Analytics, Blockchain, Virtual und Augmented Reality oder künstlicher Intelligenz insb. die umfassende, internetbasierte Vernetzung von intelligenten Objekten wie Maschinen, Anlagen und Produkten zählt (Lasi et al. 2014; Porter und Heppelmann 2014). Durch die eingebauten Sensoren erzeugen intelligente Objekte im Betrieb beim Kunden umfangreiche Datenmengen, welche die Basis für die Entwicklung datenbasierter, digitaler Services darstellen (Iansiti und Lakhani 2014).

Ein Beispiel hierfür ist Mitsubishi Electric mit Lösungen wie Smart Condition Monitoring. Dabei werden die von Industriegütern wie bspw. CNC-Bearbeitungsmaschinen erzeugten Daten cloudbasiert gesammelt und analysiert. Indem der Verschleiß von Bauteilen frühzeitig erkannt und vorbeugende, bedarfsgetriebene Wartungen geplant werden können, ergibt sich eine höhere Verfügbarkeit teurer, oftmals hochausgelasteter Industriegüter. Im Kontext der Digitalisierung wandeln sich Industrieunternehmen dabei von reinen Produktanbietern zu digitalisierten Lösungsanbietern (Iansiti und Lakhani 2014). Die Ausgestaltungsformen können von der Ergänzung des physischen Kernprodukts um digitale Dienstleistungen bis hin zum kompletten Wandel zum Lösungsanbieter, bei dem das physische Produkt nur noch Teil der Lösung ist, reichen (Fleisch et al. 2015). Entsprechend erzeugen Industrieunternehmen im Rahmen einer hybriden Wertschöpfung durch die Kombination spezifischer Ressourcen und Fähigkeiten (Mehr-)Wert mittels integrierter, kundenindividueller Leistungsbündel aus Sachgütern und Dienstleistungen (sog. hybriden Produkten), die für Kunden durch die Integration den Wert der Teilleistungen übersteigen (Böhmann und Krcmar 2006). Sich

ergänzende Produkt-Dienstleistungsbündel werden dabei schon seit langem von Unternehmen angeboten (etwa Wartungsservices für eigene Maschinen). Die Digitalisierung ermöglicht nun jedoch durch intelligente, digitale Technologien und die internetbasierte Vernetzung von Unternehmen und Kunden die Entwicklung bezahlbarer, kundenindividueller und datenbasierter Lösungsangebote und die Erschließung neuer Branchen und Märkte. Vor diesem Hintergrund wird die Schaffung von Werten durch die Erstellung integrierter, datenbasierter Produkt-Dienstleistungsbündel zur Abgrenzung von herkömmlichen Produkt-Dienstleistungsbündeln im Folgenden als digitale, hybride Wertschöpfung bezeichnet.

Für Industrieunternehmen besteht hierbei ein hoher Handlungsdruck. Zum einen leidet das Geschäft mit Industriegütern zunehmend unter sinkenden Margen durch Konkurrenten aus Billiglohnländern, die inzwischen auch bei hochtechnologischen Industriegütern wie Automatisierungsrobotern kostengünstige Produkte anbieten (Kindström 2010). Zum anderen steigt die Nachfrage von Kunden nach individuellen Lösungen für spezifische Problemstellungen (Porter and Heppelmann 2014). Gleichzeitig steigt der Innovationsdruck durch (z.T. branchenfremde) Wettbewerber, da auch diese innovative, digitale Serviceangebote entwickeln (Röglinger und Urbach 2016). Setzen sich Unternehmen daher nicht mit der der Entwicklung digitaler Services und der damit verbundenen digitalen Transformation ihrer Geschäftsmodelle auseinander, besteht die Gefahr, Marktanteile zu verlieren und zu Commodity-Lieferanten physischer Produkte zu werden. Entsprechend ist es für Industrieunternehmen im Rahmen ihrer Digitalisierungsstrategie von zentraler Bedeutung, sich durch proaktives Handeln und die Entwicklung digitaler Geschäftsmodelle mit entsprechenden kundenindividuellen, datenbasierten Serviceangeboten Wettbewerbsvorteile zu erarbeiten und neue Märkte zu erschließen (Gimpel und Röglinger 2015).

Die Digitalisierung und die Entwicklung digitaler Services haben jedoch erhebliche Auswirkungen auf die bestehenden Geschäftsmodelle der Unternehmen (McDonald und Roswell-Jones 2012). So steigt durch multiple Wertversprechen und kundenindividuelle Lösungsangebote die Komplexität des Geschäftsmodells. Außerdem entstehen auf Basis der beim Kunden erzeugten Daten Abhängigkeiten zwischen physischen Produkten und digitalen Services. Darüber hinaus erfordern digitale Services neue Fähigkeiten, Ressourcen, Partner oder Erlösmodelle, zusätzlich zu den bereits vorhandenen Schlüsselaktivitäten und -ressourcen wie etwa Produktentwicklung oder Produktionsanlagen. Industrieunternehmen stehen daher vor der Herausforderung, ihre Geschäftsmodelle, ihr komplettes

Wertschöpfungssystem und die darauf ausgerichteten Prozesse, Systeme und Infrastruktur gezielt weiterzuentwickeln und dabei die resultierenden Komplexitäten und Abhängigkeiten zu berücksichtigen.

Vor diesem Hintergrund besteht das Ziel dieses Artikels darin, die Auswirkungen der Digitalisierung auf die Geschäftsmodelle von Industrieunternehmen und die daraus resultierenden Herausforderungen anhand des Business Model Canvas (BMC) als etablierte, strukturgebende Methode zur Geschäftsmodellentwicklung aufzuzeigen und zu beurteilen. Hierzu wurden neben einer Literaturanalyse im Rahmen einer empirischen Studie Interviews mit fünf Experten aus der Industrie geführt. Veranschaulicht werden die beschriebenen Entwicklungen durch eine Fallstudie über Mitsubishi Electric, einem international führenden Technologiekonzern. Zuletzt werden im Beitrag praxisrelevante Handlungsempfehlungen gegeben, die Praktikern bei der Entwicklung digitaler Geschäftsmodelle im Zusammenhang mit digitaler, hybrider Wertschöpfung Orientierung geben sollen.

II.1.2 Digitale Geschäftsmodelle und der Business Model Canvas

Bis heute gibt es in der wissenschaftlichen Literatur keine allgemein gültige Definition des Begriffs Geschäftsmodell. Je nach Untersuchungsschwerpunkt existieren unterschiedliche Definitionen, die im Rahmen verschiedener Literaturüberblicke aufgearbeitet und strukturiert werden (z.B. Zott et al. 2011; Schallmo 2013). Amit und Zott (2001) etwa definieren in einem theoretisch fundierten Ansatz ein Geschäftsmodell als „*den Inhalt, die Struktur und die Steuerung von Transaktionen, die so gestaltet sind, dass sie durch die Nutzung von Geschäftschancen Wert schaffen*“. Mit Fokus auf Unternehmensaktivitäten entwickeln Zott und Amit (2010) diese Definition weiter und beschreiben ein Geschäftsmodell als „*System interdependenter Aktivitäten, das über die betrachtete Firma hinausgeht und ihre Grenzen überschreitet“*. Schallmo (2013) hingegen definiert ein Geschäftsmodell als „*die Grundlogik eines Unternehmens, die beschreibt, welcher Nutzen auf welche Weise für Kunden und Partner gestiftet wird* […]“ und „ […] *wie der gestiftete Nutzen in Form von Umsätzen an das Unternehmen zurückfließt* […].“ Der stärker der Praxis entspringenden Definition von Osterwalder und Pigneur (2011) folgend, kann ein Geschäftsmodell auch als das „*Grundprinzip, nach dem eine Organisation Werte schafft, vermittelt und erfasst*“, beschrieben werden. Es beschreibt damit, wie ein Unternehmen Produkte und Dienstleistungen erstellt und dadurch Kundennutzen schafft, um Wettbewerbsdifferenzierung

und Kundenbindung zu erreichen, und Werte generiert und abschöpft. Diese Definition eines Geschäftsmodells liegt auch dem vorliegenden Beitrag zugrunde.

Von digitalen Geschäftsmodellen wurde bislang oftmals im Zusammenhang mit digitalen Branchen wie bspw. eCommerce gesprochen. Durch die Digitalisierung und die Entwicklungen rund um das Internet-of-Things vermengen sich nun auch in der physischen Industrie die bisher nicht-digitalen Geschäftsmodelle mit entsprechenden digitalen Geschäftsmodellmustern zu einem hybriden Konstrukt, bei dem sich der Wert als Kundennutzen aus einem physischen Produkt und einem oder mehreren damit verbundenen digitalen Services ergibt (Fleisch et al. 2017). Entsprechend kann von einem digitalen Geschäftsmodell gesprochen werden, „*wenn Veränderungen in den digitalen Technologien grundlegende Veränderungen in der Art und Weise, wie Geschäfte getätigt und Umsätze generiert werden, auslösen*“ (Veit et al. 2014). Im Kontext der Unternehmensarchitektur bilden Geschäftsmodelle die konzeptuelle und architektonische Schnittstelle zwischen der aus der Vision des Unternehmens abgeleiteten Unternehmensstrategie und den Geschäftsprozessen zur Umsetzung des Geschäftsmodells (Al-Debei und Avison 2010).

Um Geschäftsmodelle strukturiert zu entwickeln und zu beschreiben, gibt es verschiedene Methoden, zu denen auch der BMC zählt. Hierbei werden, wie in Abbildung II.1-1 zu sehen, neun grundlegende Bausteine (Kundensegmente, Wertversprechen, Kundenbeziehungen, Kanäle, Schlüsselressourcen, Schlüsselaktivitäten, Schlüsselpartner, Einnahmequellen und Kostenstruktur) in die vier Bereiche Kunden, Angebot, Infrastruktur und finanzielle Überlebensfähigkeit eingeordnet (Osterwalder und Pigneur 2011). Anhand der neun Bausteine wird das Geschäftsmodell eines Unternehmens beschrieben und somit strukturiert dargestellt.

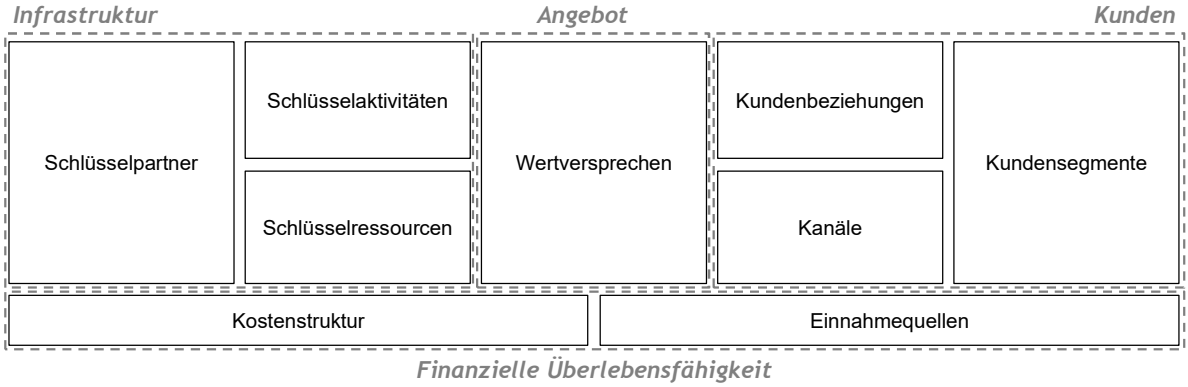


Abbildung II.1-1: Schematische Darstellung des BMC – Eigene Darstellung in Anlehnung an Osterwalder und Pigneur (2011)

Zur Veranschaulichung sind in Tabelle II.1-1 beispielhafte Elemente und Ausgestaltungsmöglichkeiten der neun Bausteine eines Geschäftsmodells nach Osterwalder und Pigneur (2011) präsentiert.

BMC-Kategorie	***Beispiel***
Kundensegmente	*Massenmarkt, Nischenmärkte, multi-sided Markets*
Wertversprechen	*Produkt, Dienstleistung zur (kundenindividuellen) Problemlösung*
Kundenbeziehungen	*Individuelle Kundenbetreuung, Selbstbedienung, automatisierte Dienstleistung*
Kanäle	*Vertriebsteam, Händler, Online-Plattform, Mobile Apps*
Schlüsselressourcen	*Produktionsanlagen, IT-Infrastruktur, Softwareentwicklung, Patente, Produktdaten*
Schlüsselaktivitäten	*Produktion von Gütern, Entwicklung digitaler Services, Online-Systemplattform*
Schlüsselpartner	*Rohstoff-Lieferanten, Cloud-Anbieter, Entwicklungspartner, IT-Dienstleister*
Einnahmequellen	*Verkauf von Produkten, Leasing, pay per use, Subscription*
Kostenstruktur	*Kosten für Produktionsanlagen, Kosten für IT-Infrastruktur, Entwicklungskosten*

Tabelle II.1-1: Beispielhafte Elemente eines Geschäftsmodells – Eigene Darstellung

Durch die visuelle und strukturierte Darstellung ist der BMC ein geeignetes Instrument zur Geschäftsmodellentwicklung und kann aufgrund der geringen Komplexität bei interaktiven Methoden wie Workshops von interdisziplinären Teams oder bspw. zur unternehmensinternen Kommunikation des Geschäftsmodells angewendet werden. Dies stellt insb. vor dem Hintergrund der steigenden Komplexität digitaler Geschäftsmodelle einen wesentlichen Vorteil dar. Allerdings weist der BMC auch Nachteile auf. So lassen sich Rahmenbedingungen, die es bei der Entwicklung von Geschäftsmodellen gerade in zunehmend dynamischen Märkten zu berücksichtigen gilt, im BMC nur indirekt, etwa über die Kunden-Dimension, abbilden. Hierzu schlagen Osterwalder und Pigneur (2011) jedoch mit makroökonomischen Effekten, Markttreibern, (technologischen) Trends und Industriefaktoren die Berücksichtigung weiterer vier Dimensionen und damit eine Erweiterung des BMC vor. Außerdem ermöglicht der BMC keinen Vergleich mit Geschäftsmodellen von Wettbewerbern. Daher stellt der BMC nur ein Instrument des notwendigen Methodenbaukastens für die digitale Transformation von Geschäftsmodellen dar. Es bedarf darüber hinaus weiterer Instrumente wie etwa Heat Maps zur Schwachstellenanalyse, Wettbewerbsanalysen oder Transformations- und Investitionsplänen zur operativen Umsetzung.

II.1.3 Auswirkungen datenbasierter Produkt-Dienstleistungsbündel

Die Wertschöpfung datenbasierter Produkt-Dienstleistungsbündel hat vielfältige Auswirkungen auf die Geschäftsmodelle von Industrieunternehmen und stellt diese vor verschiedene Herausforderungen. In diesem Kapitel werden zunächst grundlegende Auswirkungen beschrieben, bevor anschließend auf daraus resultierende Herausforderungen eingegangen wird. Die Auswirkungen und Herausforderungen wurden im Rahmen von fünf Experteninterviews mit weltweit agierenden Unternehmen aus der Technologie- und Industriegüterbranche mit jeweils mehr als 25.000 Mitarbeiter bzw. ein Vielfachem davon diskutiert und abgeleitet. Alle interviewten Experten bestätigten, dass die Digitalisierung maßgeblichen Einfluss auf ihr jeweiliges Geschäftsmodell hat und dass die gezielte Weiterentwicklung zu digitalen Geschäftsmodellen mit datenbasierten Produkt-Dienstleistungsbündeln von hoher Bedeutung für ihr Unternehmen ist. Abbildung II.1-2 zeigt die Auswirkungen, gegliedert nach den neun Bausteinen des BMC, und die resultierenden Herausforderungen.

BMC-Kategorie	***Auswirkungen***
Kundensegmente	Neue Zielgruppen und Märkte
	Multi-sided Markets
Wertversprechen	Individuelle Lösungsangebote durch digitale Services im Fokus (Besitz des physischen Produkts im Hintergrund)
	Physisches Produkt mit multiplen digitalen Services
Kundenbeziehung	Relationale, durchgängige Kundenbeziehung
	Digital-basierte Kundeninteraktion
Kanäle	Product als Point-of-Sale
	Vertrieb von Dienstleistungen digitaler Natur
	Automatisierte Dienstleistungen
	Partner-Vertriebskanäle
Schlüsselaktivitäten	Produkt- und Softwareentwicklung
	Vernetzung mit Kunden
	Data Analytics
	Datenschutz/-sicherheit
Schlüsselressourcen	Physisches Produkt beim Kunden
	Daten des Produkts, erzeugt beim Kunden
	Hochspezialisierte Fachkräfte
	Intelligente, digitale Technologie und IKT-Infrastruktur
Schlüsselpartner	Digitales Ökosystem: Einbindung externer Partner
	Kunden
Einnahmequellen	Neue Payment-Formen für individuelle, digitale Services
	Besitz des physischen Produkts nicht mehr im Fokus
Kosten	Kosten für IKT-Infrastruktur und Softwareentwicklung

Abbildung II.1-2: Auswirkungen der Digitalisierung auf Geschäftsmodelle und resultierende Herausforderungen – Eigene Darstellung

- Kundensegmente*:* Industrieunternehmen können durch die Entwicklung digitaler Services **neue Zielgruppen und Märkte** erschließen, da auf Basis der erzeugten Kundendaten auch digitale Services für neue Zielgruppen entwickelt werden können. Darüber hinaus

entstehen **multi-sided Markets**, bei welchen neben der primären Kundenzielgruppe auch weitere Zielgruppen bedient werden. Bspw. können die gewonnen Daten zum Energieverbrauch von Produktionsanlagen anonymisiert und als Verbrauchsmuster gebündelt Energieversorgern und Netzbetreibern zur Optimierung ihrer Netzinfrastruktur angeboten werden.

- Wertversprechen: Der Produktverkauf mit After-Sales-Betreuung wandelt sich künftig zu **kundenindividuellen Lösungsangeboten** für spezifische Kundenprobleme. „One-fits-all"-Angebote verlieren in diesem Zusammenhang an Bedeutung. Grundlage dafür sind kundenindividuelle, digitale Services, die aufgrund geringer Grenzkosten künftig bezahlbar angeboten werden können. Dadurch tritt zum einen der Besitz **physischer Produkte in den Hintergrund**. Zum anderen werden **verschiedene digitale Services** angeboten, die je nach kundenspezifischer Problemstellung mit dem physischen Produkt kombiniert werden.

- Kundenbeziehung: Die primär transaktionalen Kundenbeziehung wandelt sich künftig zu einer dauerhaften **relationalen Beziehung**, da Kunden durchgängig begleitet werden müssen, um ein Verständnis für die individuellen Problemstellungen des Kunden entlang dessen Ökosystems und Wertschöpfungsprozesse zu gewinnen. Zudem nimmt die **digital-basierte Interaktion** mit Kunden aufgrund der digitalen Natur der Serviceangebote und der internetbasierten Vernetzung mit diesen zu.

- Kanäle: Künftig wird das **Produkt als Point-of-Sale** für die digitalen Services zur zentralen Schnittstelle zum Kunden. Dabei wird der Anteil an **automatisierten Vorgängen** ohne direkte Beteiligung von Mitarbeitern zunehmen, da intelligente, vernetzte Objekte Bestellvorgänge selbst vornehmen oder Wartungen selbständig initiieren. Darüber hinaus wandelt sich der Vertrieb vom einmaligen Produktverkauf zum **dauerhaften Vertrieb von Lösungen mit digitaler Natur**. Zusätzlich ergeben sich im Rahmen von Cocreation-Ansätzen weitere Vertriebskanäle durch **externe Partner**.

- Schlüsselaktivitäten: Standen vormals v.a. die Entwicklung und Produktion von Industriegütern im Fokus, werden diese künftig durch Aktivitäten wie **Softwareentwicklung**, **Data Analytics** sowie **Datenschutz und -sicherheit**, die für digitale Services entscheidend sind, ergänzt. Zudem ist künftig die verlässliche, internetbasierte **Vernetzung mit Kunden** eine zentrale Schlüsselaktivität.

- Schlüsselressourcen: Künftig bilden die beim Kunden **von den Produkten erzeugten Massendaten** die Grundlage für die digitalen Serviceangebote. Dementsprechend zählt auch das **Produkt beim Kunden** zu den Schlüsselressourcen. Des Weiteren benötigen Unternehmen **hochspezialisierte Fachkräfte** in Bereichen wie Data Science oder Cyber Security. Zuletzt zählen **innovative, digitale Technologien** wie Künstliche Intelligenz und die entsprechende **IKT-Infrastruktur**, die das Unternehmen mit seinen Kunden vernetzt und die beim Kunden erzeugten Daten cloudbasiert sammelt und analysiert, zu den Schlüsselressourcen.
- Schlüsselpartner: Aufgrund der steigenden Anzahl an benötigten Schlüsselfähigkeiten sind Industrieunternehmen nur begrenzt dazu in der Lage, sämtliche Fähigkeiten selbst zu entwickeln und bereitzuhalten. Dies trifft in besonderem Maße auf kleine und mittelständische Unternehmen zu, deren Kernkompetenz bei der Entwicklung und Produktion physischer Industriegüter liegt. Daher müssen Unternehmen in zunehmendem Maße **externe Partner** in ihre digitalen Wertschöpfungsprozesse integrieren und digitale Ökosysteme schaffen. Hierzu zählen etwa IoT-Plattformen, Cloud-Infrastrukturen oder digitale Services. Außerdem wird auch der **Kunde selbst** durch dessen Integration in den Wertschöpfungsprozess zu einem Schlüsselpartner.
- Einnahmequellen: Durch den Wandel vom reinen Produktverkauf zu lösungsorientierten, digitalen Serviceangeboten wird die Entwicklung **neuer Einnahmequellen und Erlösarten** notwendig. Der gleichzeitige **Bedeutungsverlust des Besitzes physischer Produkte** trägt zu dieser Entwicklung bei. Zu vielversprechenden Ansätzen zählen v.a. pay per use-Bezahlmodelle für Industriegüter in Kombination mit Subscription-Modellen für digitale Serviceangebote.
- Kosten: Waren bisher die Entwicklung, Produktion und Vertrieb von Industriegütern die Hauptkostentreiber von Industrieunternehmen, zählen hierzu künftig v.a. auch **Kosten für Softwareentwicklung und IKT-Infrastruktur**.

II.1.4 Resultierende Herausforderungen

Die beschriebenen Auswirkungen stellen Unternehmen vor Herausforderungen, die mit den interviewten Experten erarbeitet und validiert wurden und im Folgenden beschrieben werden:

- **Multiple Wertversprechen**: Konzentrierte sich das Wertversprechen bislang auf das physische Kernprodukt, bieten Unternehmen künftig durch verschiedene, digitale Services weitere Wertversprechen für kundenindividuelle Problemstellungen an. Eine Kernfrage ist dabei, welche digitalen Services mit dem physischen Produkt kombiniert werden sollen. Je nach Ausprägung des Wandels zum reinen Lösungsanbieter, ändert sich das Wertversprechen dabei zum Teil radikal. Unternehmen müssen Kunden zum einen den Nutzen der angebotenen Lösungen vermitteln. Zum anderen müssen sie mit der resultierenden Komplexität multipler Wertversprechen umgehen und diese sowohl mit Blick auf die prozessuale Unterstützung als auch den ökonomischen Wertbeitrag steuern.
- **Bestimmungsgerechte Verwendung von Daten**: Im Zusammenhang mit den beim Kunden erzeugten Daten gilt es zu klären, wem die erzeugten Daten gehören und für welche Zwecke diese verwendet werden dürfen. Dies ist entscheidend, da von einem bestimmungsgerechten Umgang die langfristige Beziehung zu den Kunden maßgeblich abhängt.
- **Zunehmende Komplexität des Geschäftsmodells**: Durch die Zunahme der Wertversprechen, neue Kundenzielgruppen und Kanäle, zusätzliche Schlüsselaktivitäten, -ressourcen und -partner sowie neue Einnahmequellen und Erlösarten steigt generell die Komplexität von Geschäftsmodellen.
- **Abhängigkeit zwischen Produkt und digitalen Services**: Aufgrund der erforderlichen Massendaten als Grundlage für digitale Services besteht eine erhebliche Abhängigkeit zwischen der physischen und digitalen Komponente der digitalen, hybriden Wertschöpfung. Dies muss bei der Entwicklung beachtet werden. Außerdem ist die digitale Wertschöpfung dadurch von der zuverlässigen Funktionsweise der Produkte und der zuverlässigen Vernetzung abhängig.
- **Integrierte Entwicklung**: Durch die unterschiedlichen Entwicklungs- und Produktlebenszyklen physischer Produkte und digitaler Services stehen Unternehmen vor der Herausforderung, diese aufgrund der beschriebenen Abhängigkeitsbeziehung in Einklang miteinander zu entwickeln.
- **Technologische Eignung physischer Produkte:** Die Erschließung neuer Märkte kann die technologische Anpassung der physischen Produkte an neue Einsatzanforderungen erfordern.

- **Cyber Security und Safety**: Aufgrund der internetbasierten Vernetzung mit Kunden und Partnern sowie vernetzter Produkte und Produktionskomponenten steigt die Anfälligkeit der IKT-Systeme für Cyber Security Risiken. Daher müssen sensible Kundendaten vor dem Zugriff Unbefugter geschützt werden. Da durch die enge Verknüpfung mit den operativen Maschinensteuerungen zudem auch die Maschinensicherheit (Safety) und Verfügbarkeit betroffen sein können, stellt Cyber Security künftig eine zentrale Herausforderung dar.
- **Gewinnung spezifischer Fachkräfte**: Da für Schlüsselaktivitäten wie Data Analytics oder Datenschutz hochspezialisierte Fachkräfte notwendig sind, stehen Unternehmen vor der Herausforderung, diese bereits heute sehr stark nachgefragten Spezialisten zu gewinnen.
- **Einbindung externer Partner und Kunden**: Durch die zunehmende Einbindung externer Partner und Kunden in den Wertschöpfungsprozess müssen entsprechende Schnittstellen in den dazu notwendigen Systemen eingerichtet und entsprechende interorganisationale Informationssysteme eingesetzt werden. Zudem müssen Wertschöpfungsprozesse und die zugrunde liegenden Informationsflüsse verstärkt unternehmensübergreifend geplant, koordiniert und gesteuert werden.
- **Gestaltung von Erlösmodellen**: Aufgrund der Vielzahl möglicher Ausgestaltungsformen muss künftig eine Balance zwischen der gewünschten Individualität und der dennoch notwendigen Standardisierung gefunden werden. Während es wichtig ist, der Individualität der angebotenen Kundenlösungen Rechnung zu tragen, führt eine Vielzahl individueller Erlösmodelle insb. bei einer hohen Kundenzahl zu erheblicher Komplexität und Intransparenz.

Unternehmen, die diese Herausforderungen in den Griff bekommen, haben gute Chancen, sich gegenüber Wettbewerbern durchzusetzen, Marktanteile zu gewinnen und neue Märkte zu erschließen.

II.1.5 Fallstudie Mitsubishi Electric

Im Folgenden wird anhand des Geschäftsbereichs Fabrikautomation von Mitsubishi Electric der Wandel eines klassischen Geschäftsmodells zu einem digitalen Geschäftsmodell beispielhaft dargestellt. Mitsubishi Electric ist als weltweit agierender Technologiekonzern mit knapp 140.000 Mitarbeitern und einem Umsatz von 39 Mrd. USD p.a. in den Bereichen Fabrikautomation, Energie, Kommunikation, Gebäudetechnologie und Transportation tätig.

Im Geschäftsbereich Fabrikautomation zählt das Unternehmen zu den weltweit führenden Anbietern von Automatisierungs- und Verarbeitungstechnologien für industrielle Kunden. Die Kernprodukte reichen von Steuerungen, Antriebstechnik, Visualisierungstechnologie, SCADA-Softwarelösungen, Netzwerktechnologie, Niederspannungsschaltgeräten über Industrieroboter bis hin zu CNC-Steuerungen und -Antrieben für Werkzeugmaschinen, Erodiermaschinen sowie Laserbearbeitungsmaschinen. Diese wurden bisher überwiegend durch klassischen Produktverkauf, Leasing- oder Lizenz-Modelle an Kunden vertrieben. Aufbauend auf einem weltweiten Service-Netzwerk wurden Kunden im After-Sales-Bereich mit Wartungsdienstleistungen und Technologieberatungen betreut. Abbildung II.1-3 zeigt den BMC für das klassische Geschäftsmodell sowie den BMC des zukünftigen digitalen Geschäftsmodells, bei dem die bisherigen, klassischen Komponenten wie etwa Produktion und Produktionsanlagen um die notwendigen Fähigkeiten, Ressourcen, Partner, etc. für beispielhafte digitale Services erweitert wurden, und die mit der digitalen Transformation verbundenen Auswirkungen.

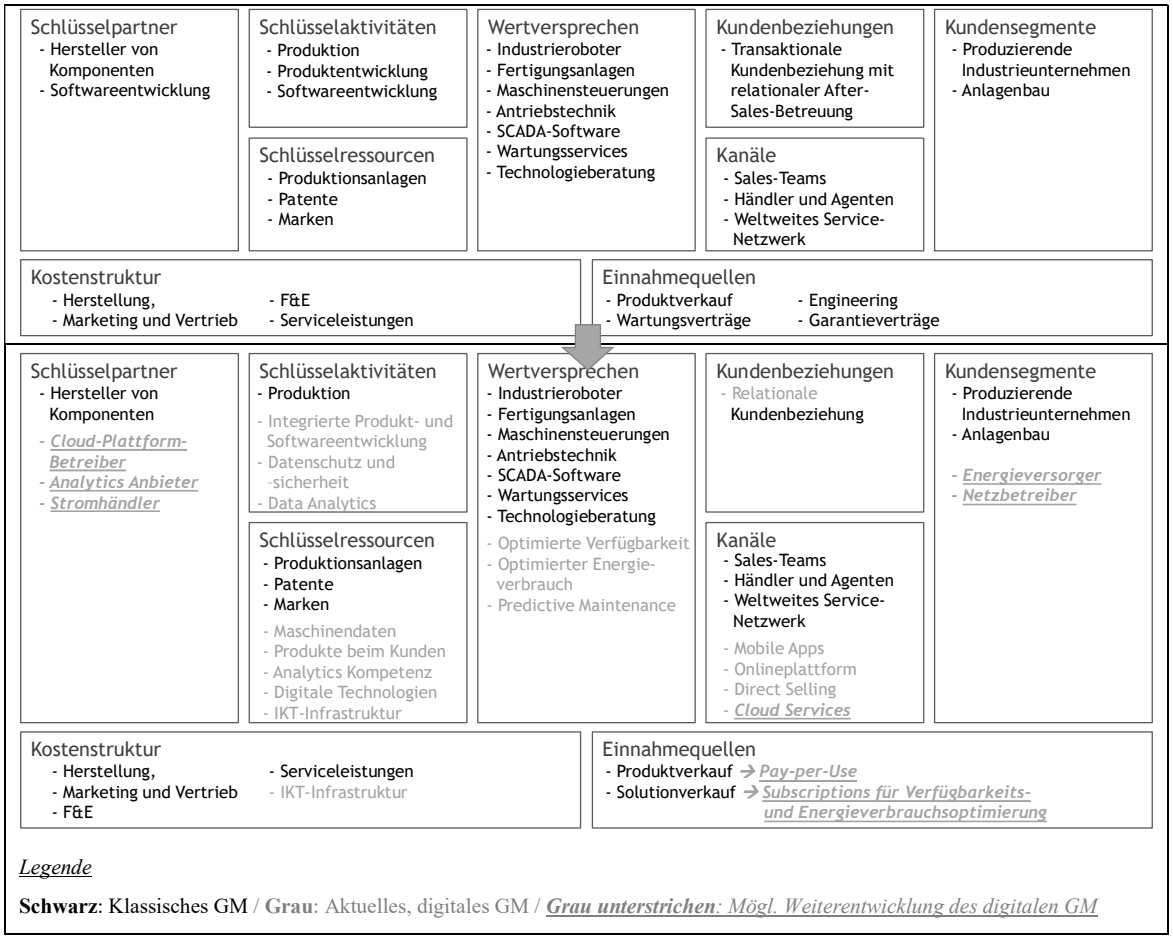


Abbildung II.1-3: Traditionelles (oben) und digitales Geschäftsmodell (unten) des Geschäftsbereichs Fabrikautomation von Mitsubishi Electric im Vergleich – Eigene Darstellung

Im Rahmen verschiedener Digitalisierungsprojekte wurden digitale Serviceangebote entwickelt, die auf die bei Kunden erzeugten Daten der Industrieanlagen zurückgreifen. So wird mit *Smart Condition Monitoring* Kunden ein optimiertes Wartungsmanagement angeboten, bei dem Maschinendaten ausgewertet und durch bekannte Fehlermuster Wartungsbedarf von Maschinen frühzeitig erkannt wird. Dadurch werden reduzierte Stillstandszeiten und eine gesteigerte Verfügbarkeit hochausgelasteter Industrieanlagen erreicht. Ein anderer digitaler Service ist das optimierte Energiemanagement der gesamten Industrieanlage auf Basis der Energieverbrauchsdaten. Dabei wird auf Basis einer Initialanalyse zunächst der Energieverbrauch optimiert. Aufbauend darauf wird ein laufendes Peak-Management angeboten, wodurch Produktionsabläufe so gesteuert werden, dass teure Lastspitzen vermieden werden ohne den Produktionsablauf zu beeinträchtigen.

Auf Basis des heutigen, digitalen Geschäftsmodells sind vielfältige Weiterentwicklungsmöglichkeiten denkbar. So könnte bspw. durch die Anbindung von Energie-Handelsplattformen eine Berücksichtigung von Echtzeit-Strompreisen bei der Produktionsablaufplanung und der Maschinensteuerung erfolgen oder durch die Integration in eine Demand-Side-Management-Plattform die Energienachfrageflexibilität für Kunden monetarisiert werden. Darüber hinaus lassen sich auch weitere Kundenzielgruppen erschließen, indem etwa die Echtzeit-Energieverbrauchsdaten in anonymisierter Form und als Verbrauchsmuster gebündelt an Energieversorger und Netzbetreiber vertrieben werden. Derartige Entwicklungen erfordern von Mitsubishi Electric eine laufende Anpassung der Prozesse, Strukturen und Systeme, so dass bspw. die Kooperation mit Partnern wie SAP mit der HANA-Cloud oder IBM-Watson für Analytics-Applikationen künftig stark an Bedeutung gewinnt, um sich auf die für das Kerngeschäft erforderliche Kernkompetenzen konzentrieren zu können.

II.1.6 Praxisrelevante Handlungsempfehlungen

Basierend auf den gewonnenen Erkenntnissen werden abschließend grundlegende Handlungsempfehlungen aufgezeigt. Aufgrund der stets unternehmensindividuellen Erfordernisse und Ausgangssituationen können diese Praktikern als Orientierung und Anhaltspunkte für die Entwicklung digitaler Geschäftsmodelle dienen:

- Zentraler Ausgangspunkt bei der Entwicklung digitaler Lösungsangebote sollte stets der Kunde und das zu lösende Kundenproblem sowie der Aufbau einer langfristigen

Kundenbeziehung sein. Nur bei Schaffung eines echten Mehrwerts sind Kunden bereit, Daten zur Verfügung zu stellen, die dann im Rahmen eines win-win-Setting zur digitalen Wertschöpfung eingesetzt werden können. Zudem machen sich Unternehmen mit laufenden Einnahmen aus Subscriptions unabhängiger von der konjunkturabhängigen Auftragslage bei Industriegütern.

- Bei kleinen und mittelständischen Kunden sollte der Fokus zunächst darauf liegen, vorhandene Potentiale zu heben („low hanging fruits“), da diese aufgrund ihrer begrenzten finanziellen Investitionsvolumina nur eingeschränkt zu Investitionen in neue Anlagen in der Lage sind. Dies kann bspw. mit individuellen Lösungen durch zielgerichtete technologische Nachrüstung bestehender Produktionsanlagen und der Nutzung bereits vorhandener Daten erreicht werden.
- Aufgrund der vielfältigen Schlüsselaktivitäten und -ressourcen stellt der Ansatz der Cocreation mit Partnern für Industrieunternehmen, insb. kleine und mittelständische Unternehmen, einen vielversprechenden Weg dar, da nicht alle erforderlichen Fähigkeiten selbst aufgebaut und vorgehalten werden können. Durch die Zusammenarbeit mit Partnern, etwa für Cloud-Infrastruktur und Analytics-Applikationen, können sich Industrieunternehmen auf ihre Kernkompetenzen wie die Entwicklung physischer Produkte und die enge Begleitung des Kunden fokussieren. Dabei ist allerdings darauf zu achten, nicht zum reinen Commodity-Lieferanten des physischen Produkts zu werden.
- Da auch ohne Ansätze wie Cocreation die Einbindung externer Partner und Kunden in digitale Wertschöpfungsprozesse zunimmt, sind offene Produkt- und Systemschnittstellen sowie offene Standards wie OPC UA oder MTConnect für den Datenaustausch und die Integration von modularen Applikationen von großer Bedeutung.
- Im Rahmen der Produkt- und Softwareentwicklung sollten Unternehmen einen Portfolioentwicklungsansatz verfolgen, bei dem eine enge Abstimmung zwischen der Entwicklung physischer Produkte und digitaler Services stattfindet und bestenfalls integriert erfolgt.
- Hinsichtlich Cyber Security müssen die angebotenen Services hohe Sicherheitsstandards erfüllen, damit Kundendaten geschützt sind. Dies ist für das Vertrauen der Kunden und deren Bereitschaft zur Datenbereitstellung von elementarer Bedeutung.

- Um benötigte Fachkräfte zu gewinnen, müssen Unternehmen Möglichkeiten schaffen, diese projektbezogen in virtuellen Teams einzusetzen. Dabei sind der Zugriff auf externe Dienstleister und Freelancer sowie entsprechende Hochschulkooperationen potentielle Wege abseits der Festanstellung, bei denen jedoch ebenfalls hoher Wettbewerb herrscht.
- Aufgrund der Komplexität digitaler Geschäftsmodelle gewinnt der Einsatz interdisziplinärer, crossfunktionaler Teams mit agilen Arbeitsmethoden bei der Geschäftsmodellentwicklung und -umsetzung an Bedeutung, da hierzu Kompetenzen aus verschiedenen Unternehmensbereichen und kreative Arbeitsweisen wie Design Thinking notwendig sind.
- Bei der Entwicklung neuer Einnahmequellen und Erlösarten sind den möglichen Ausgestaltungsformen keine Grenzen gesetzt. Wichtig dabei ist, dass die Komplexität im Sinne der Transparenz überschaubar bleibt und in Verbindung mit dem Lösungsangebot stets ein beidseitiger Nutzen gegeben ist. Nur dann sind Kunden auch bereit, für digitale Services zu bezahlen.

Die dargestellten Auswirkungen, Herausforderungen und Handlungsempfehlungen stellen einen generischen Rahmen für die zielgerichtete Entwicklung digitaler Geschäftsmodelle im Kontext der digitalen, hybriden Wertschöpfung dar, welcher auf der Analyse verschiedener Realweltbeispiele und der geführten Experteninterviews beruht. Aufgrund der Vielfältigkeit möglicher Geschäftsmodelle und der gerade erst beginnenden Verbreitung digitaler Geschäftsmodelle im Industriesektor stellt diese Arbeit daher keine abschließende Sicht auf das Thema dar. Zudem erfordert die Entwicklung konkreter digitaler Geschäftsmodelle zwingend die Berücksichtigung unternehmensspezifischer Faktoren und Rahmenbedingungen, die im Rahmen von interdisziplinären Workshops zur Geschäftsmodellentwicklung ermittelt werden müssen. Darüber hinaus ist die Entwicklung und Umsetzung digitaler Geschäftsmodelle ein laufender, iterativer Transformationsprozess. Ab wann ein Geschäftsmodell dabei als „digital“ bezeichnet werden kann, lässt sich allein auf Basis der im Rahmen diesen Beitrages erfolgten Forschung nicht eindeutig ableiten, da der Übergang von traditionellen Geschäftsmodellen zu digitalen fließend erscheint und unternehmensspezifisch ist. Dies stellt jedoch einen Ansatzpunkt für weitere Forschung und die Entwicklung entsprechender Ansätze wie etwa Reifegradmodelle zur Bewertung des Digitalisierungsgrades von Geschäftsmodellen dar, um Unternehmen weitere Hilfestellung beim Transformationsprozess bereitzustellen.

Denn nur durch das kontinuierliche Hinterfragen und Weiterentwickeln des Geschäftsmodells können Unternehmen im von der Dynamik des technologischen Fortschritts geprägten Wettbewerb bestehen und langfristig ihre Wettbewerbsfähigkeit sicherstellen. Gelingt dies, bietet die Entwicklung digitaler Geschäftsmodelle und die digitale, hybride Wertschöpfung für proaktiv handelnde Unternehmen erhebliche Potentiale.

II.1.7 Literatur

Al-Debei, MM, Avison, D (2010) Developing a Unified Framework of the Business Model Concept. European Journal of Information Systems 19:359–376

Amit R, Zott C (2001) Value Creation in e-Business. Strategic Management Journal 22:493–520

Böhmann T, Krcmar H (2006) Komplexitätsmanagement als Herausforderung hybrider Wertschöpfung im Netzwerk. In Innovative Kooperationsnetzwerke 81-105, https://doi.org/10.1007/978-3-8350-9307-2_3

Fleisch E, Weinberger M, Wortmann F (2015) Geschäftsmodelle im Internet der Dinge. Schmalenbachs Zeitschrift für betriebswirtschaftliche Forschung 67:444–465

Fleisch E, Weinberger M, Wortmann F (2017) Geschäftsmodelle im Internet der Dinge. In: Reinheimer S. (eds.) Industrie 4.0. Edition HMD. Springer Vieweg, Wiesbaden, https://doi.org/10.1007/978-3-658-18165-9_1

Gimpel H, Röglinger M (2015) Digital Transformation; Changes and Chances – Insights based on an Empirical Study. Projektgruppe Wirtschaftsinformatik des Fraunhofer-Instituts für Angewandte Informationstechnik FIT, Augsburg/Bayreuth

Iansiti M, Lakhani KR (2014) Digital Ubiquity – How Connections, Sensors, and Data Are Revolutionizing Business. Harvard Business Review 92:91–99

Kindström D (2010) Towards a Service-based Business Model – Key Aspects for Future Competitive Advantage. European Management Journal 28:479–490

Koch V, Kuge S, Geissbauer R, Schrauf S (2014) Industrie 4.0 – Chancen und Herausforderungen der vierten industriellen Revolution. Strategy& und PWC, Düsseldorf

Lasi H, Fettke P, Kemper H-G, Feld T, Hoffmann M (2014) Industrie 4.0. Wirtschaftsinformatik 56:261–264

McDonald MP, Roswell-Jones A (2012) The Digital Edge; Exploiting Information & Technology for Business Advantage. Gartner, Inc., Stanford

Osterwalder A, Pigneur Y (2011) Business Model Generation; Ein Handbuch für Visionäre, Spielveränderer und Herausforderer. Campus Verlag, Frankfurt, New York

Porter ME, Heppelmann JE (2014) How Smart, Connected Products are Transforming Competition. Harvard Business Review 92:64–88

Röglinger M, Urbach N (2016) Digitale Geschäftsmodelle im Internet der Dinge. Geschäftsmodelle in der digitalen Welt:77–94

Schallmo D (2013) Geschäftsmodell-Innovation – Grundlagen, bestehende Ansätze, methodisches Vorgehen und B2B-Geschäftsmodelle. Springer Gabler, Wiesbaden

Veit D, Clemons E, Benlian A, Buxmann P, Hess T, Kundisch D, Leimeister JM, Loos P, Spann M, (2014) Business Models – An Information Systems Research Agenda. Business & Information Systems Engineering, 6:45–53

Zott C, Amit R, Massa L (2011) The Business Model: Recent Developments and Future Research. Journal of Management 37:1019–1042

Zott C, Amit R (2010) Business Model Design: An Activity System Perspective. Long Range Planning, 43:216–226

II.2 Research Paper 2: "Structuring the Anticipated Benefits of the Fourth Industrial Revolution"

Authors:	Annabelle Geißler[a], Björn Häckel[b,c], Jochen Übelhör[a,c] Christian Voit[a,c] [a] Research Center Finance & Information Management, Department of Information Systems Engineering & Financial Management (Prof. Dr. Hans Ulrich Buhl), University of Augsburg annabelle.geissler@fim-rc.de jochen.uebelhoer@fim-rc.de [b] University of Applied Sciences, Augsburg, Germany bjoern.haeckel@hs-augsburg.de [c] Project Group Business & Information Systems Engineering of the Fraunhofer FIT, Augsburg, Germany
In:	Proceedings of the 25th Americas Conference on Information Systems, 2019

Abstract: *The digitalization of production facilities and the accompanying changes are anticipated to transform entire industries posing a fierce pressure on companies to deal with these developments regarding their information technology management. To lay the foundation for the development of corresponding business strategies, we structure benefits of Industry 4.0 through a structured literature review and categorize them using an established framework for IS benefits. Benefits for companies arise within four dimensions and concern various issues ranging from production related benefits to superordinate benefits affecting the business model. To conclude, managerial implications resulting from dependencies and the variety of benefits are presented.*

II.2.1 Introduction

In the recent past, there has been a tremendous hype built up around *Industry 4.0*. The term comprises technological developments such as Internet-of-Things (IoT), Internet-of-Services, or cyber physical systems (CPS) (Lasi et al. 2014). In this paper, we focus on CPS as a representative of Industry 4.0, the implementation of smart factory concepts and their anticipated benefits. As *Industry 4.0* is a terminology particular common in Germany and in absence of a common global terminology, we explicitly include related concepts such as *Industrial Internet*, *Smart Manufacturing*, or *Advanced Manufacturing* that are common in English-speaking countries. In our understanding, Industry 4.0 comprises in its inner kernel the advanced digitalization of production facilities through the digital connection of smart machines and products with networked embedded systems and the extensive integration of information systems, digital services, and Internet-based technologies (Barrett et al. 2015; Schuh et al. 2014b; Zuehlke 2010). These promise great potentials and benefits for industrial applications as smart products are envisioned to self-control their manufacturing process and smart factories are anticipated to self-optimize production processes in real-time and respond context-specific to turbulences in production and to fast changing customer demands (Schuh et al. 2014b). Besides others, these capabilities increase efficiency and competitiveness as they enable the flexible production of highly customized products at costs comparable to mass production (Radziwon et al. 2014). Further, innovative digital business models like predictive maintenance or pay-per-use concepts utilize the tremendous amount of generated production and product data and enable innovative products enhanced with digital services (Lasi et al. 2014).

These developments are anticipated to deeply impact existing business strategies and success models and transform whole economies in a disruptive manner (Iansiti and Lakhani 2014). Therefore, companies in all industries face a fierce pressure to deal with the fundamental changes and rethink their strategies regarding investments in Industry 4.0 technologies to retain competitiveness (Geisberger and Broy 2015). Otherwise, increasing efficiency of competitors, market entries of non-traditional competitors, and new digital business models intensify competition and, ultimately, jeopardize companies that fail to undergo the necessary transformation process. Accordingly, companies must not only evaluate whether to invest into Industry 4.0, but especially into which specific technologies and in which order. To come to these crucial strategic decisions in correspondence with value-based management principles,

investments have to be evaluated ex-ante under consideration of involved costs, risks, and benefits (Faisst and Buhl 2005). While costs and risks have already been researched quite extensively, benefits of Industry 4.0 have not yet been investigated in a structured manner. Till date, authors only point out benefits for motivational reasons or evaluate highly specific and application-dependent benefits. To the best of our knowledge, there is no comprehensive picture of Industry 4.0 technologies and their contribution to value creation. Consequently, the evaluation of benefits remains a major obstacle as the variety and complexity of technologies and the absence of best-practices or industry standards complicate their identification and quantification. However, this would be necessary to ensure a holistic view on Industry 4.0 business strategies. To close this gap, our research focuses on benefits of Industry 4.0 and addresses the following research question:

RQ: *Which benefits of Industry 4.0 are anticipated in scientific literature?*

By identifying benefits based on a structured review of scientific literature and by categorizing them into a structured benefits framework, we provide a comprehensive overview of the benefits of Industry 4.0. This helps to better describe the characteristics of Industry 4.0 technologies that are associated with value creation. Further, our research represents an essential first step towards the comprehensive evaluation of smart manufacturing technologies and lays the ground for a subsequent identification and quantification of benefits. The remainder of our paper is organized as follows: We outline our methodology in Section 2. Section 3 provides a review on the investigated literature. Section 4 presents the identified benefits and a categorization of these benefits into an IS benefits framework. Section 5 contains a discussion of managerial implications, before Section 6 presents a conclusion and gives an outlook on further research.

II.2.2 Research Methodology

As Industry 4.0 is a quite young field of research and the body of corresponding literature on benefits of Industry 4.0 is rather limited, the aim of our research is not the synthesis of research on benefits, but a methodically sound identification of respective benefits mentioned in scientific literature. For the approach conducted in this research, the methods presented by Bandara et al. (2011), Fettke (2006), vom Brocke et al. (2009), and Webster and Watson (2002) concerning structured literature reviews in the IS field serve as a basis. Although the approaches coincide in their basic structure (e.g., all authors incorporate a literature search

comprising keyword search in databases), they differ regarding their exact research procedure and purpose. Therefore, we combine the approaches and derive four steps: Subsequent to a literature search (1), relevant articles are identified (2) and analyzed (3). Afterwards, the results are structured (4).

Step 1 - Search process: Since the investigated topic is an emerging field and concerns various disciplines, a concept-centric literature search is executed (Webster and Watson 2002). To query a wide selection of journals and to include conference proceedings, we query databases listed in Table II.2-1 with search terms for Industry 4.0 and related concepts (i.e. *Industry 4.0*, *Internet-of-Things*, or *smart manufacturing*) in combination with terms that ensure results with a strong association industrial applications (i.e. *production*, *manufacturing*, or *factory*). The keyword search is conducted in the search fields abstract, title, and keywords as this search strategy is supposed to render papers focusing on the target topic (Bandara et al. 2011). The search strategy renders a total of 177 results.

Databases	ScienceDirect, EbscoHost, ProQuest, AIS eLibrary
Search Fields	Title, Abstract, Keyword
Source Types	Journals, Conferences
Search Terms	(Industry 4.0 OR Industrie 4.0 OR Internet of Things OR Industrial Internet OR Cyber Physical System OR Cyber Physical Production System OR Smart Factory OR Smart manufacturing) AND (production OR manufacturing OR factory OR Produktion OR Fabrik OR Industrie)

Table II.2-1: Parameters of Keyword Search

Step 2 - Selection of relevant literature: As vom Brocke et al. (2009) argue, the limitation of the amount of literature by keyword search should be content-based and include analyzing titles, abstracts and full texts. Accordingly, titles of all articles are examined to exclude articles not dealing with Industry 4.0 or dealing with non-industrial applications. Further, all articles in other languages than English or German are excluded. Then, abstracts of the remaining articles are analyzed to select those discussing Industry 4.0. In a last step, full texts of the remaining articles are screened by examining relevance for Industry 4.0 and if benefits of Industry 4.0 are mentioned in the article. This results in 57 articles (55 in English and 2 in German) relevant for further analysis. 27 articles are published in conference proceedings from different fields like production engineering, or computer sciences. The other 30 articles were published in journals from different fields ranging from engineering and computer sciences to management sciences.

Step 3 - Analysis of relevant literature: 57 publications are analyzed for mentioned benefits of Industry 4.0. Thereby, we define *benefit* as an umbrella term for positive effects like opportunities, potentials, value, or improvements for companies achieved through the implementation of Industry 4.0 technologies. Thus, macro-economic effects for economies are not considered. Thus, we subsume different levels of benefits, i.e. different degrees of concretization, under one term. This approach seems reasonable as Industry 4.0 is a young and emerging field of research and, so far, the vast majority of benefits remain rather vague potentials with no empirical evidence in literature. Each benefit mentioned and the respective publication are recorded in a database resulting in an initial list of multiple benefits. After consolidating the initial list and removing doubles and highly similar benefits, we obtain a list of 365 benefits.

Step 4 - Synthesis of analysis results: There are different frameworks for structuring benefits. For instance, DeLone and McLean (1992) provide a framework with six dimensions regarding aspects of IS and Abelein et al. (2009) develop a framework consisting of technical, organizational, and strategic business dimensions. An established framework for IS benefits proposed by Anthony (1965) structures benefits into the three dimensions *operational*, *managerial*, and *strategic* as this allows the distinction of benefits regarding the hierarchical levels of decision-making in organizations, i.e. *operational control*, *managerial control*, and *strategic planning*. Since we aim to provide the basis for the analysis of individual use cases and concrete decisions, we regard Anthony's (1965) framework as most suitable. This classification supports the differentiation of the impact of benefits and, thus, facilitates their subsequent in-detail evaluation and quantification. Numerous authors applied an extended version of Anthony's three dimensional framework by adding the dimensions *organizational* and *information technology (IT) infrastructure* (e.g. Shang and Seddon 2000, Shang and Seddon 2002; Wang et al. 2016) as it was discovered that certain IT benefits could not (unambiguously) be clustered without them, in example organizational benefits in terms of improved focus, cohesion, learning and execution were identified (Shang and Seddon 2002). However, as we view advancements of IT as core enabler of Industry 4.0, we refrain from gathering benefits describing enhancements of IT and do not include *IT infrastructure* in our framework. Additionally, IT is developing at an increasingly pace, so the inclusion of corresponding benefits would impair the framework's long-term relevance.

Each benefit is assigned to one of the four dimensions. Nevertheless, there are interdependencies between the dimensions that are addressed later in this paper. To ensure objectivity, the benefit assignment is done by two researchers separately and merged while assignment differences are discussed. In a second step, benefits within each dimension are clustered, again by two researchers separately, and matched to consolidated benefits. Finally, we obtain our benefits framework as the central artefact of our research: a structured representation of Industry 4.0 benefits. The framework is evaluated by a discussion with ten other researchers and the results of the evaluation are considered in the further development of the framework presented in Section 4.

II.2.3 Overview of the Investigated Literature

In the following, we give an overview on the examined scientific literature concerning Industry 4.0 from different fields of research like engineering, operations research or sustainability. Due to the innovative nature, many authors approach Industry 4.0 in a general manner, propose definitions, and discuss the state of technologies and future research and development challenges. For example, Mikusz and Csiszar (2015) develop a framework to examine characteristics and abilities of a CPS application in industrial robotics. Wang et al. (2015) outline characteristics and definitions of CPS and present advancements in CPPS to point towards research directions. Other authors focus on risks and opportunities of smart manufacturing (Banham 2015), review the term *smart* in relation to technology, and propose a definition for smart factories (Radziwon et al. 2014). However, due to a macro-perspective view on Industry 4.0, these approaches make only general statements on benefits of industry 4.0 in the context of new business models.

Despite these general approaches, there are publications addressing specific topics accompanying Industry 4.0 and related concepts. For example, some investigate architectures or models for the integration of CPS/CPPS in manufacturing and the realization of smart factories (Bagheri et al. 2015; Majstorovic et al. 2015). Other authors like Wright (2014) outline the effects of CPPS regarding products or focus on effects for humans in smart manufacturing environments (Dombrowski and Wagner 2014). An issue examined by several authors concerns production and process management (Denkena et al. 2014; Reischauer and Schober 2015; Seitz and Nyhuis 2015). For example, Seitz and Nyhuis (2015) present advantages of CPS for production planning, controlling, and monitoring. A different stream

of literature deals with the implication for supply chains (Frazzon et al. 2015; Papazoglou et al. 2015; Veza et al. 2015). A reference architecture for smart manufacturing networks is developed by Papazoglou et al. (2015), while Veza et al. (2015) propose a management approach for smart factory networks. Laboratory research facilities are another topic discussed (Faller and Feldmüller 2015; Hummel et al. 2015; Schuh et al. 2015a; Weyer et al. 2015; Zuehlke 2010). For instance, Hummel et al. (2015) point towards the importance of learning factories for the qualification and training of professionals. Moreover, several different topics are discussed such as the collection and processing of data, data analytics, and simulations (Barthelmey et al. 2014; Lee et al. 2014; Neuböck and Schrefl 2015; Rosen et al. 2015), the development of new business models (Rudtsch et al. 2014), collaboration mechanisms (Schuh et al. 2014b; Schuh et al. 2015b), service innovations (Hertrich et al. 2015) or lean production principles (Kohlberg and Zuehlke 2015). These approaches give explicit examples for benefits, however, due to the specific research context, they are only partially applicable for the comprehensive evaluation of the strategic use of Industry 4.0.

Based on this diverse body of scientific literature, we can conclude that scientific literature mentioning benefits of Industry 4.0 and related concepts differs in focus and scope and deals with various aspects of these concepts. Despite the variety of different approaches, to the best of our knowledge, there is no structured framework that provides practitioners with a comprehensive overview of potential benefits. Therefore, we aim to contribute to this research gap by proposing a structured benefits framework to enable decision makers to identify relevant fields of actions for their digitalization strategy and to evaluate potential benefit dimensions from the realization of Industry 4.0 investments and their contribution to value creation in organizations.

II.2.4 Categorizing the Benefits of Industry 4.0

In the following, we present our benefits framework for Industry 4.0 that is based on an IS benefits framework as it provides predefined dimensions for the consolidation and categorization of the extensive list of identified benefits. Further, the framework is designed for managers to support the assessment of benefits and, therefore, is appropriate for the categorization of benefits considering practitioners' needs regarding organizational decision-making and strategy development. As mentioned in Section 2, the applied framework comprises *operational*, *managerial*, *strategic*, and *organizational* benefits. Operational

benefits contain benefits concerning periodically repeated actions and improvements of practical tasks (Shang and Seddon 2002), while managerial benefits refer to benefits resulting from a better supply of information facilitating advances in the resource allocation and control, operation monitoring and support of strategic business decisions (Shang and Seddon 2002). Benefits affecting long-term planning and high-level decisions are referred to as strategic benefits (Shang and Seddon 2002). Further, organizational benefits involve overarching goals such as focus, learning, and execution within organizations (Shang and Seddon 2002). The benefits are allocated to one of the four dimensions. Since many benefits address same or related issues, similar benefits are consolidated and clustered within the respective dimensions. Figure II.2-1 shows our benefits framework for Industry 4.0 comprising benefits anticipated in scientific literature. As each benefit is a condensate of several benefits from scientific literature, we provide detailed insights into related concepts of each benefit in Table II.2-2 to Table II.2-5 and indicate the number of articles within our final paper sample in which a benefit was mentioned. However, the number of articles is only informative and does not allow an assessment of the significance of a benefit.

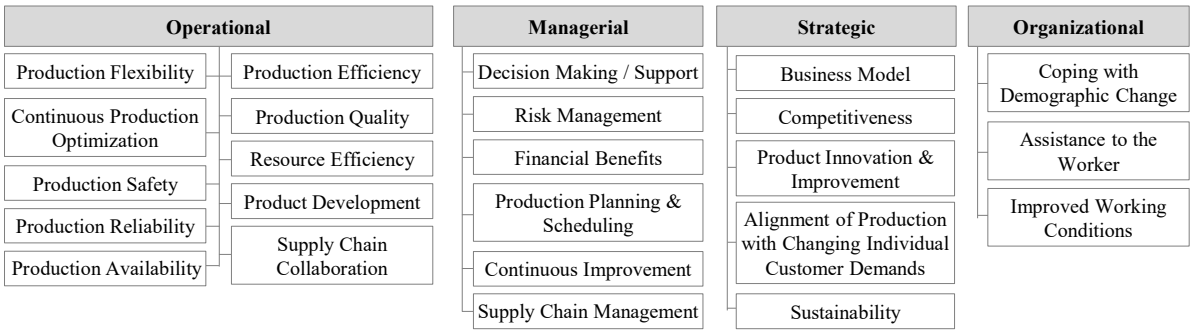


Figure II.2-1. Benefits framework for Industry 4.0 – Own Illustration

Benefits assigned to the *operational dimension* of our framework are primarily production related. For instance, *continuous production optimization* refers to the capability of smart factories to (self-) optimize the production system or production processes. Thereby, Industry 4.0 technologies allow the optimization regarding various goals and business metrics as stated by Weyer at al. (2015) and Kolberg and Zuehlke (2015). Another concept widely discussed is *production flexibility*. While in some cases, flexibility is not further expanded on, in some publications it is associated to modularity and reconfigurability of production systems and processes through plug-and-play principles. Veza et al. (2015) present a different perspective, pointing towards the flexibility in terms of short-term responsiveness in case of disruptions. Further related concepts are adaptability, agility, and variability. Another aspect of production

expected to benefit from Industry 4.0 is production quality. The anticipated benefits are mainly a reduction of reworking or scrap. Wright (2014) for instance states that wireless sensors can guarantee that final products are completely manufactured. Further, *production reliability* is supposed to benefit from Industry 4.0 including robustness, resilience, and the handling of unprecedented events enabling production systems to reduce potential human error (Banham 2015) and to autonomously improve or maintain a status by self-diagnosis technologies (Mönks et al. 2016). A special case of reliability is production availability discussed extensively in literature and referring to a reduction of downtime and a higher usability of intelligent factories.

Benefit	Related Concept
production flexibility [24]	i.a. flexibility, adaptability, and reconfigurability of production systems; modularity of production modules; easing of engineering and set up; flexibility during technical modification; less time consumption during commissioning; no engineering efforts for reconfiguration; high process variability; adaptability to new product variants or production systems
continuous production optimization [26]	i.a. optimization of production; of production systems and processes; enhanced equipment efficiency; compensation of limited manufacturing capabilities; self-optimization of production systems; enhanced production capabilities
production safety [8]	i.a. higher safety; safer asset utilization; reduction of safety incidents
production reliability [23]	i.a. high reliability; robustness; resilience; handling of unprecedented events; flexibility to respond to disruptions and failures in real-time; autonomous problem handing and reaction to maintain the system's status
production availability [4]	i.a. increased/high availability; reduction of machine downtime; usability of intelligent factories
production efficiency [33]	i.a. improved production efficiency; more efficient asset utilization; just-in-time proceeding of goods; efficient transportation; increased service efficiency; increase of throughput; faster production ramp-up; improved technical support and maintenance; improved quality control
production quality [10]	i.a. fewer product defects; reduction of reworking; lowering of scrap and failures; quality improvement
resource efficiency [15]	i.a. energy savings; less energy consumption; resource efficient production; optimal resource consumption; reduction of material and supply usage; reduction of waste; gains in material efficiency
product development [7]	i.a. innovative product development; accelerated development processes; flexible product development; better quality of development; reduction of number of iterations between product designers and process planners
supply chain collaboration [4]	i.a. increase of collaboration productivity; higher supply chain productivity; higher agility and integration of complete supply chain; improved overall performance of supply chains in terms of service-level and flexibility; increase of logistic performance

Table II.2-2: Operational Benefits of Industry 4.0

Further, an increase of *production safety* is expected including higher safety of machines and the reduction of safety incidents. Another operational benefit is *production efficiency*. While some authors mention general efficiency gains in relation to production or asset utilization, others, anticipating more specifically, for instance, a promotion of just-in-time manufacturing. One concept in regard to production efficiency is a better technical support of machinery and plant equipment. Rudtsch et al. (2014) describe the concept of remote maintenance that will support maintenance processes through web-based technologies and IoT. Further operational benefits not directly affecting the shop floor are *resource efficiency* and *product development*. Resource efficiency is addressed in some cases in general, but also more specific in regard to energy efficiency in terms of a lower energy consumption or energy savings. Similarly, general benefits regarding resources are expected to materialize through a more accurate resource deployment, which is also reflected in waste reduction and a lower overall consumption of resources. In addition to the production of products, benefits are also anticipated for product development. As Rosen et al. (2015) argue, ubiquitous connectivity will close the digitalization loop and enable optimized product design cycles. Further, Schuh et al. (2014a) state that simulation and virtualization will enable accelerated development processes. Thereby, virtualized development processes contribute to *resource efficiency* through reduced material usage. Contemplating a network of firms, another operational benefit is improved *supply chain collaboration* as higher collaboration productivity through improved information sharing and increased IS integration across company-boundaries within the eco system is one core characteristic of Industry 4.0.

Managerial benefits comprise - similar to the operational level - benefits directly related to production as well as benefits not related to production. There, the benefit *production planning & scheduling* subsumes the optimization of production management and planning, of maintenance scheduling, and of inventory management as well as efficient and advanced planning processes. Schuh et al. (2015b) outline that an improved cooperation within a network of firms enables improved forecasting and advanced and efficient planning processes and, thus, facilitate to counteract over-production as a result of bullwhip-effects. Further, *continuous improvement* enabled by increasing transparency through improved data acquisition and analysis affects production as it concerns effective and efficient process and performance improvement. For instance, Kolberg and Zuehlke (2015) elaborate on Industry 4.0 technologies and their application in regard to lean production principles and conclude

that innovative automation technology is a promising topic. While benefits regarding *decision making / support* might concern production, they are not limited to it. Yang et al. (2016) state that real-time information about positioning and working status might assist decisions concerning production and inventory management. Schuh et al. (2015b) further argue that enabling a higher transparency within the supply chain contribute to comprehensibility and, thus, sustainability of decisions and their effects. Benefits not directly linked to production concern *risk management*. While Majstorovic et al. (2015) and Davis et al. (2012) address risk management without presenting more details on how Industry 4.0 is supposed to assist, Banham (2015) discusses the reduction of risk at length, arguing that overall strategic, operational and financial risks are reduced. For instance, the increased flexibility of production systems reduces both strategic risks in regard to fast changing customer demands and operational risks in regard to lengthy technical modifications, while improved product development reduces product failure risks and, thus, financial risks. Benefits concerning positive financial aspects are summarized as *financial benefits* resulting from various aspects like effects on the shop floor. For example, Bagheri et al. (2015) refer to significant economic potential of Industry 4.0 enhanced factories. Similar to the operational dimension, benefits regarding *supply chain management* also exist in the managerial dimension, for instance, in regard to shared information management, risk management or general optimization. Indeed, managerial benefits are more divers including a better handling of complexity, security for single parts of a supply chain, and a better level of information sharing.

Strategic benefits comprise abilities by generating new *business models*, enabling *product improvement and innovation*, and the *alignment of production with changing, individual customer demands* as well as an enhancement of *competitiveness* and *sustainability*. Further, new *business models* become feasible. While some authors make rather general statements on new opportunities for value-creation, Veza et al. (2015) and Mikusz and Csiszar (2015) give explicit examples arguing that new business models emerge in form of complementary or additional services. According to Mikusz and Csiszar (2015), new business models facilitated by networked CPS within production facilities and the availability of real-time information are *Add-On*, *Product as a Point of Sales*, *Object Self-Service*, and *Lock-in* business models. Veza et al. (2015) state that new business models appear in the form of *Manufacturing-as-a-Service*, *Industrial Product-Service Systems*, or comparable.

Benefit	Related Concept
decision making / support [11]	i.a. effective and efficient decision making; improved decision support; improved performance monitoring in distributed manufacturing; real-time reaction on problems in production
risk management [4]	i.a. improved risk prediction, planning, and management; reduction of strategic, operational, and financial risk
financial benefits [4]	i.a. economic potential; improvement of working capital; radical performance improvement
production planning & scheduling [15]	i.a. efficient and advanced planning process; optimization of manufacturing management, maintenance, and service scheduling; optimal production planning and inventory management; adaptive production scheduling; reduced planning costs
continuous improvement [4]	i.a. effective and efficient process improvement; continuous improvement processes; enhancing existing lean production solutions and extending their applicability; improvement of overall performance and maintenance management; continuous improvement of manufacturing processes; higher quality of processes; improvement of quality of production
supply chain management [4]	i.a. dynamic management of complex environments with short-lived supply chains; security for all supply chain's elements, access to data, knowledge about demand/stock/sales/prediction of anomalies; optimization of value chain by implementation of autonomously controlled and dynamic production; solving problem of complexity in supply chains

Table II.2-3: Managerial Benefits of Industry 4.0

Regarding *product innovation and improvement*, benefits include the enhancement of product performance, its design, quality, and sustainability as well as additional digital services, and shorter innovation cycles. For example, Davis et al. (2012) argue that new innovative products are facilitated by increased workforce and manufacturing innovation. Another benefit is the *alignment of production with changing, individual customer demands*. It refers to the efficient production of individualized products in variable volumes, i.e., mass customization (Dombrowski and Wagner 2014). Further, higher customer satisfaction and an increased flexibility for changing customer demand are expected. *Competitiveness* includes, besides an increased competitiveness in general, benefits regarding cost and profit (contributing to financial benefits), market responsiveness, and a shorter time-to-market. For instance, Schuh et al. (2014b) and Davis et al. (2012) state that costs per unit decrease and higher profits can be achieved through shorter time-to-market. *Sustainability*, considered indispensable for a company's long-term success (Perrot 2015), is another benefit that also contributes to resource efficiency on the operational level. While benefits addressing sustainability in general are mentioned in some publications, others address ecologic sustainability specifically. For

instance, Schuh et al. (2015b) elaborate on how Industry 4.0 ultimately enhances ecological sustainability.

Benefit	Related Concept
business model [6]	i.a. innovative business models; improved or novel business processes within value creation along product life cycle; new market opportunities; new value-creation opportunities
Competitiveness [13]	i.a. increased competitiveness; maintain competitiveness through mass customization; production of individual products at reasonable cost; lower cost per piece; reduction of cost pressure; reduction of pressure regarding demands for individualized products; improvement of time-to-market; improved ability to respond to varying market demands
product innovation & improvement [18]	i.a. individualization of products; innovative, complementary products and services; enhancement of product design and in-product services; additional customer-value on use; extension of products with digital services; improvement of next product generations; distribution of product information to customer; reduction of product failure risk
alignment of production to changing, individual customer demands [17]	i.a. product individualization; mass customization; lot size one; optimized product customization; increased customer satisfaction; rapid response to changing customer needs and individual customer requirements; alignment of manufacturing with customer demand through flexible production
Sustainability [5]	i.a. maximizing environmental sustainability; benefits for sustainability; improved processes sustainability; sustainable practices

Table II.2-4: Strategic Benefits of Industry 4.0

In the *organizational dimension*, *assistance of the worker* is expected to benefit from Industry 4.0 by new ways of support, for example, through advanced gathering, processing, and visualization of process date (Schuh et al. 2015a) and virtual instructions at the point of action through smart devices (Weyer et al. 2015). Further, working conditions are expected to ameliorate through novel tasks, human-centric production systems, and health related issues. Rudtsch et al. (2014) mention that human-centered production processes enable production processes to follow human speed and instruction. Moreover, decoupling the place of work from the location of the worker by wireless technology will increase the mobility of humans in production. Further, coping with demographic change constitutes the third organizational benefit as Industry 4.0 technologies can contribute to less burdening work systems (Hummel et al. 2015).

Benefit	Related Concept
coping with demographic change [1]	i.a. less burdening work systems to cope with intensifying demographic change
assistance to the worker [4]	i.a. context-aware assistance to people and machines in task execution; task simplification; new ways of gathering, processing, and visualization process data; virtual instructions and sensor-based monitoring
improved working conditions [7]	i.a. improved health, better working environment; assistance towards more productive, less burdening work; decoupling of workplace from physical location of worker; human-centered production processes regarding speed and instructions; adjustment to human workforce

Table II.2-5: Organizational Benefits of Industry 4.0

II.2.5 Managerial Implications and Challenges

In the following, we discuss managerial implications and challenges gained in the course of our research that should be considered in the strategic alignment of companies in all manufacturing industries:

1. The structured processing of benefits revealed that not all benefits, although allocated to separate dimensions with varying scope, are independent from each other. Some benefits are rather mutually dependent and complementary. Thereby, it appears that the implementation of Industry 4.0 technologies to achieve benefits on the operational level is often times a precondition for the realization of benefits on managerial or strategic levels. For instance, the realization of strategic benefits like the alignment of production to changing, individual customer demands requires the realization of production flexibility or an accelerated product development process. Accordingly, the manifold interdependencies inherent in potential benefits must be considered by management, especially in terms of cause-effect relations to determine which benefits are intertwined and to identify all benefits resulting from the implementation of certain enabling technologies.
2. The benefits' assignment to the respective framework dimensions revealed that the line between operational and managerial benefits rather vanishes through the developments of Industry 4.0, especially regarding the production system. Examples for this transformation identified in the framework are benefits concerning adaptability, utilization, optimization, predictive maintenance, or autonomous problem handling. These result from the capability of production systems to provide real-time information on an unprecedented fine-granular level and, thus, to self-control the production process in real-time, a key-characteristic of Industry 4.0. This ability influences traditional planning processes and contributes to an

amalgamation of operational and managerial tasks. Thus, management faces the challenge to adapt its managerial processes, accordingly.

3. While some benefits are commonly mentioned to describe the concept of Industry 4.0 (Neugebauer et al. 2016), they are often times not set in context with concrete enabling technologies. Thus, guidance on how to realize specific benefits by means of enabling technologies is missing. This was also found by Strozzi et al. (2017), who state that research focuses primarily on conceptual work and experiments and rarely discusses actual test-beds and lessons learned from practice. Accordingly, management faces the challenge to determine concrete investment measures in enabling technologies and to develop robust transformation roadmaps in the course of their digitalization strategy.
4. Yet, some articles mention first examples for implemented benefits and their enabling technologies. For instance, Herterich et al. (2015) conduct case-studies regarding impacts of CPS on industrial services. Their benefits can be assigned primarily to operational benefits including a reduction of downtime or an increased fix time and rate. This leads to the impression that operational benefits might appear earlier, whereas strategic benefits might materialize on a longer time horizon. A survey conducted by the American Society for Quality mentioned by Banham (2015) gives a similar impression. It reveals that 82% of manufacturers could realize production efficiency gains and 49% could reduce product defects by investing in smart machines. Also, 45% could increase customer satisfaction, which constitutes a strategic benefit. Therefore, management needs to critically review the impacts of employed technologies and establish measures to assess benefits on a longer time-horizon. To evaluate the success of ex-ante pursued benefits, performance indicators should be developed enabling the ex-post evaluation of benefits and their realization. For this, our benefits framework can serve as a starting point.
5. The magnitude and diversity of benefits revealed by our analysis and the accompanying costs and risks of investments clearly indicate the importance for management to systematically evaluate Industry 4.0 technologies and to apply structured approaches to manage benefits actively (Peppard et al. 2015). Accordingly, the comprehensive evaluation of Industry 4.0 technologies requires appropriate qualitative and quantitative methods of economic investment and decision theory. Our structured overview of possible benefits can serve as a starting point, for instance, for a structured benefits management approach by means of a benefits dependency network as presented by Peppard et al. (2015).

II.2.6 Conclusion, Limitations, and Outlook

The developments of Industry 4.0 lead to the advancing digitalization of production facilities and the development of digital enhanced business models promising great potentials in all manufacturing sectors. The accompanying changes are anticipated to transform business strategies and success models posing a fierce pressure on companies to deal with these developments in a proactive manner. Despite the obvious importance, there was no comprehensive picture of the contribution of Industry 4.0 technologies to the value creation of companies as a structured overview over the benefits of Industry 4.0 was missing. However, this is necessary for a comprehensive identification and subsequent quantification of benefits in regard to value-based investment decision strategies. Therefore, our work contributes to research by developing a structured benefits overview. For this, we identified 365 benefits anticipated in literature, consolidated them to 24 conclusive benefits and categorized them into an IS benefits framework. Our overview demonstrates the different dimensions in which Industry 4.0 technologies contribute to value creation. It becomes apparent that their strategic value resides in optimizing internal and cross-company value creation processes and the opportunity to develop new products and business models.

Despite the merits of this paper in terms of systematically structuring the benefits of Industry 4.0, there are some limitations, which can be noted as potential areas for further research. For instance, our analysis only includes benefits that are mentioned in scientific literature. Therefore, potential benefits that are not considered by researchers, or cannot be conceived yet, are missing. Moreover, this neglects potential findings only included in non-scientific publications. Further, in our literature analysis, we did not consider whether benefits are the focus of an article or only listed for motivational or descriptive purposes. Thus, research building up on our framework has to consider that the feasibility of the latter might not be thoroughly researched yet. Additionally, anticipated benefits in literature address different hierarchical levels (e.g. reduction of waste vs. increase of competitiveness) and are in some cases mutually dependent regarding their realization. This represents a starting point for further research on the hierarchy of benefits, on cause-effect-chains, and on causal relations among complementary benefits that could be displayed by benefit dependency networks (Ward and Daniel 2006). Additionally, we categorize the identified benefits in an adapted IS benefits framework. Future research should examine whether there are other ways of benefits categorization that would also be promising and possibly even more appropriate. So far, there

is no empirical evidence in literature and, at the same time, great uncertainty in practice about which of the anticipated benefits might truly become reality. We refrained from theoretically operationalize the respective benefits as the concrete extent and value of a benefit is highly use-case specific and would have exceeded the scope of this paper. Thus, the evaluation and quantification of benefits under consideration of risk and return aspects is another important topic for further research. The same holds true for the development of concrete transformation roadmaps and digitalization strategies that support companies in deriving an appropriate portfolio and sequence of Industry 4.0 projects.

Despite these limitations and open topics for further research, we strongly believe that the developed benefits framework contributes to research on Industry 4.0 and presents a first step in enabling decision makers to identify relevant fields of actions, to develop comprehensive business strategies, and consequently, to derive value from the realization of Industry 4.0 investments.

II.2.7 References

Abelein U, Habryn F, Becker A (2009) Towards a Holistic Framework for Describing and Evaluating Business Benefits of a Service Oriented Architecture. EDOCW, Auckland, New Zealand, pp. 282–289

Anthony RN (1965) Planning and Control Systems: A Framework for Analysis. Boston: Harvard University.

Bagheri B, Yang S, Kao HA, Lee J (2015) Cyber-Physical Systems Architecture for Self-Aware Machines in Industry 4.0 Environment. IFAC-INCOM 48(3):1622–1627

Bandara W, Miskon S, Fielt E (2011) A Systematic, Tool-Supported Method for Con-ducting Literature Reviews in Information Systems. ECIS Proc

Banham R (2015) Industrial Intelligence. Risk Management 62(2): 20–24

Barrett M, Davidson E, Prabhu J, Vargo SL (2015) Service Innovation in the Digital Age: Key Contributions and Future Directions. MISQ 39(1):135–154

Barthelmey A, Störkle D, Kuhlenkötter B, Deuse J (2014) Cyber Physical Systems for Life Cycle Continuous Technical Documentation of Manufacturing Facilities. Procedia CIRP 17:207–211

Davis J, Edgar T, Porter J, Bernaden J, Sarli M (2012) Smart Manufacturing, Manufacturing Intelligence and Demand-dynamic Performance. Computers & Chemical Engineering 47:145–156

DeLone W, McLean ER (1992) Information Systems Success: The Quest for the Dependent Variable. ISR 3(1):60–95

Denkena B, Schmidt J, Krüger M (2014) Data Mining Approach for Knowledge-based Process Planning. Procedia 15

Dombrowski U, Wagner T (2014) Mental Strain as Field of Action in the 4th Industrial Revolution. Procedia CIRP 17

Faisst U, Buhl HU (2005) Integrated Enterprise Balancing mit integrierten Ertrags- und Risikodatenbanken. BISE 47(6):403–412

Faller C, Feldmüller D (2015) Industry 4.0 Learning Factory for Regional SMEs. Procedia CIRP 32:88–91

Fettke P (2006) State-of-the-Art des State-of-the-Art. BISE 48(4):257–266

Frazzon EM, Silva LS, Hurtado PA (2015) Synchronizing and Improving Supply Chains through the application of Cyber- Physical Systems. IFAC-INCOM 48(3):2059–2064

Geisberger E, Broy M (2015) Living in a Networked World - Integrated Research Agenda Cyber-physical Systems. Munich, Germany: Acatech

Herterich MM, Uebernickel F, Brenner W (2015) The Impact of Cyber-physical Systems on Industrial Services in Manufacturing. Procedia CIRP 30:323–328

Hummel V, Hyra K, Ranz F, Schuhmacher J (2015) Competence Development for the Holistic Design of Collaborative Work Systems in the Logistics Learning Factory. Procedia CIRP 32:76–81

Iansiti M, Lakhani KR (2014) Digital Ubiquity: How Connections, Sensors, and Data are Revolutionizing Business. Harv Bus Rev 92(11):90–99

Kolberg D, Zuehlke D (2015) Lean Automation enabled by Industry 4.0 Technologies. IFAC 48(3):1870–1875.

Lasi H, Fettke P, Kemper HG, Feld T, Hoffmann M (2014) Industry 4.0. BISE 6(4):239–242

Lee J, Bagheri B, Kao HA (2015) A Cyber-Physical Systems Architecture for Industry 4.0-based Manufacturing Systems. MFGLET 3:18–23

Lee J, Kao HA, Yang S (2014) Service Innovation and Smart Analytics for Industry 4.0 and Big Data Environment. Procedia CIRP 16:3–8

Majstorovic V, Macuzic J, Sibalija T, Zivkovic S (2015) Cyber-Physical Manufacturing Systems – Manufacturing Metrology Aspects. Proc Manufac Sys 10(1):9–14

Mikusz M, Csiszar A (2015) CPS Platform Approach to Industrial Robots: State of the Practice, Potentials, Future Research Directions. PACIS 2015 Proc

Mönks U, Trsek H, Dürkop L, Geneiß V, Lohweg V (2016) Towards Distributed Intelligent Sensor and Information Fusion. Mechatronics 34:63–71

Neuböck T, Schrefl M (2015) Modelling Knowledge about Data Analysis Processes in Manufacturing. IFAC 48(3)

Neugebauer R, Hippmann S, Leis M, Landherr, M (2016) Industrie 4.0 – From the perspective of applied research. Procedia CIRP 57:2–7

Papazoglou M, van den Heuvel WJ, Mascolo J (2015) Reference Architecture and Knowledge-based Structures for Smart Manufacturing Networks. IEEE Software 61–69

Peppard J, Ward J, Daniel E (2007) Managing the Realization of Business Benefits from IT Investments. MIS Q Exec 6(1)

Perrott BE (2015) Building the Sustainable Organization: An integrated approach. J Bus Strategy 36(1):41–51

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

Reischauer G, Schober L (2015) Controlling von Industrie 4.0-Prozessen. CMR 59(5):22–28

Rosen R, Wichert G von, Lo G, Bettenhausen KD (2015) About The Importance of Autonomy and Digital Twins for the Future of Manufacturing. IFAC 48(3):567–572

Rudtsch V, Gausemeier J, Gesing J, Mittag T, Peter S (2014) Pattern-based Business Model Development for Cyber-Physical Production Systems. Procedia CIRP 25:313–319

Schuh G, Gartzen T, Rodenhauser T, Marks, A (2015a) Promoting Work-based Learning through INDUSTRY 4.0. Procedia CIRP 32:82–87

Schuh G, Potente T, Varandani R, Schmitz T (2014a) Global Footprint Design Based on Genetic Algorithms – An “Industry 4.0” Perspective. CIRP Annals 63(1):433–436

Schuh G, Potente T, Wesch-Potente C, Weber AR, Prote JP (2014b) Collaboration Mechanisms to Increase Productivity in the Context of Industrie 4.0. Procedia CIRP 19:51–56

Schuh G, Reuter C, Hauptvogel A (2015b) Increasing Collaboration Productivity for Sustainable Production Systems. Procedia CIRP 29:191–196

Seitz KF, Nyhuis P (2015) Cyber-Physical Production Systems Combined with Logistic Models – A Learning Factory Concept for an Improved Production Planning and Control. Procedia CIRP 32:92–97

Shang S, Seddon PB (2000) A Comprehensive Framework for Classifying the Benefits of ERP Systems. AMCIS Proc

Shang S, Seddon PB (2002) Assessing and Managing the Benefits of Enterprise Systems. Inf Syst J 12(4):271–299

Strozzi F, Colicchia C, Creazza A, Noè C (2017) Literature review on the 'Smart Factory' concept using bibliometric tools. Int J Prod Res 55(22):1–20

Veza I, Mladineo M, Gjeldum N (2015) Managing Innovative Production Network of Smart Factories. IFAC 48(3)

vom Brocke J, Simons A, Niehaves B, Reimer K (2009) Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process. ECIS Proc

Wang L, Törngren M, Onori M. (2015) Current Status and Advancement of Cyber-physical Systems in Manufacturing. J Manuf Sys 37:517–527

Wang Y, Kung L, Byrd TA (2016) Big data analytics: Understanding its capabilities and potential benefits for healthcare organizations. Technological Forecasting and Social Change

Ward JL, Daniel E (2006) Benefits Management: Delivering Value from IS and IT Investments. Wiley & Sons Ltd

Webster J, Watson R (2002) Analyzing the Past to Prepare for the Future: Writing a Literature Review,” MIS Q 26(2)

Weyer S, Schmitt M, Ohmer M, Gorecky D (2015) Towards Industry 4.0 - Standardization as the Crucial Challenge for Highly Modular, Multi-vendor Production Systems. IFAC 48(3):579–584

Wright, P (2014) Cyber-physical Product Manufacturing. MFGLET 2(2):49–53

Yang Z, Zhang P, Chen L (2016) RFID-enabled Indoor Positioning Method for a Real-time Manufacturing Execution System Using OS-ELM. Neurocomputing 174:121–133

Zuehlke D (2010) SmartFactory – Towards a Factory-of-Things. Annu Rev Control 34(1):129–138

II.3 Research Paper 3: "Evaluating Investments in Flexible On-Demand Production Capacity – A Real Options Approach"[2]

Authors:	Bettina Freitag[a], Lukas Häfner[a,b], Verena Pfeuffer[a], Jochen Übelhör[a,b] [a] Research Center Finance & Information Management, Department of Information Systems Engineering & Financial Management (Prof. Dr. Hans Ulrich Buhl), University of Augsburg bettina.Freitag@student.uni-augsburg.de lukas.haefner@fim.rc.de verena.pfeuffer@student.uni-augsburg.de jochen.uebelhoer@fim-rc.de [b] Project Group Business & Information Systems Engineering of the Fraunhofer FIT, Augsburg, Germany

In:	Business Research, 2020, 13 (1), pp. 133-161

Abstract: *Ongoing digitalization of production accelerates trends like mass customization, ever shorter lead times, and shrinking product life cycles. Thereby, industrial companies face increasingly volatile demand that complicates an appropriate production capacity planning. On the other hand, the comprehensive digitalization of production environments favors, amongst others, the dynamic integration of flexible external on-demand production capacity provided by specialized external capacity providers (ECPs). To enable the usage of on-demand production capacity, industrial companies may require significant upfront investments (e.g., for inter-organizational information systems, planning and organizational processes, employee training). The objective of this paper is to develop a model that evaluates such enabling upfront investments from the perspective of a manufacturing company. To consider flexibility of action, we apply real options analysis in a discrete-time binomial tree model and weigh these so-called expansion options to related cash outflows. In addition, we evaluate our model by means of a simulation and sensitivity analyses and derive insights for*

[2] This is a post-peer-review version of an article published in Business Research. The final authenticated version is available online at: https://doi.org/10.1007/s40685-019-00105-w

both researchers and practitioners. The insights gained by our model present a profound economic basis for investment decisions on upfront investments in flexible on-demand production capacity.

II.3.1 Introduction

With the rise of online market places like Amazon and Alibaba, and the on-demand availability of almost any product imaginable, manufacturing companies in all industries face significant challenges in their capacity planning. Customers now expect highly individualized products, instant availability, and ever-shorter time-to-market and delivery times (Garrido 2012). This is also the case in the business-to-business sector, in which individualized, engineered-to-order business models are increasingly important (Mosig et al. 2017). The effects of these developments are intensified by globalization and technological progress, which lead to reduced product life-cycles in, for instance, the electronics, semiconductor, toy, and fashion industries (Alaniazar 2013). In particular, demand for highly individualized products which cannot, economically, be produced for stock (and are thus comparable to services, which cannot be physically stored) encourages companies to switch from traditional *make-to-stock* to flexible *make-to-order* (MTO) manufacturing approaches. Yet, when it comes to MTO capacity management, volatile customer demand complicates investment decisions in new production facilities. Depending on the particular technology, the amortization period of such investment may span several years. What is more, miscalculations during investment planning may result in idle capacity or capacity shortages, both of which are likely to have negative economic consequences. While idle capacity incurs idle costs, capacity shortages result in longer delivery periods and, in the case of dissatisfied customers, loss of customer lifetime value. Hence, MTO approaches which do manage to meet volatile customer demand are usually those that benefit from more flexible capacity management, which allows companies to adjust their production in the short-term. This type of flexibility is known as *volume flexibility* (Wickramasinghe and Perera 2016).

Instead of investing in new production facilities, companies obtain volume flexibility by commissioning external capacity providers (ECPs) who offer *manufacturing-as-a-service* (MaaS) (Rauschecker et al. 2014). More precisely, ECPs offer flexible production on-demand using their own production facilities or those of a network. Thereby, they deliver and install on-demand production capacity to the customer’s factory or, if geographical distance makes

it logistically feasible, may offer remote production. In return, the ECP can charge *pay-per-use* fees, as is common practice among businesses offering on-demand production capacity (Xu 2012). ECP services can be particularly profitable for small and medium size enterprises (SMEs), which usually have lower investment budgets. The overarching digitalization of the industrial sector enables companies to commission ECPs, and utilize on-demand production capacity, thanks to lower machine setup costs resulting from easier (IT-based) integration (so called *plug-and-produce*) and multi-functionality of leasable production facilities. Moreover, digitized production infrastructures significantly simplify MTO approaches thanks to the fact that related Cyber-Physical Production Systems (CPPSs), which "synergize conventional production technology and IT" (Penas et al. 2017: p.55), support the mass customization of products in ever smaller batch sizes down to lot-size one (Gerhard 2017). Compared to production costs in traditional environments, costs in CPPSs are comparatively low (Brettel et al. 2014; Wang et al. 2016), which makes outsourcing to low wage countries less attractive (Katzmarzik et al. 2012). The return of manufacturing from globally-distributed to local (near-customer) factories can also help to fulfil time-sensitive customer demand. However, factories focusing on local markets are subject to more volatile customer demand, i.e., machine utilization is less predictable than in factories which manufacture for customers worldwide. Hence, digitized production favors ECP business models, and MTO approaches and companies which offer local production benefit from volume flexibility as offered by ECPs (Matt et al. 2015).

The emerging trend of ECP services is widely evident. For instance, the US online shop *eMachineShop* of the Micro Logic Corporation offers "easy, convenient and low-cost fabrication of custom parts", which are ordered "via the web" and produced in the company's own facilities (eMachineShop 2017). Relying on a business network, Xometry Inc. offers "custom parts through hundreds of manufacturers across the United States" (Xometry 2017). Both of these ECPs offer remote production using 3D printing, and have in common that customers firstly upload or create a CAD model via the respective website, secondly, receive feedback on prices, lead times, and production processes, and, thirdly, submit the order. Another example is EMAG Group, a German supplier of manufacturing systems which covers "the whole process chain, from soft to hard machining" and builds production facilities for "turning, drilling, milling, gear cutting, grinding, laser welding […]" (EMAG 2017). EMAG offers its production facilities for lease in order to "assist companies in reacting to peaks or

losses in production, or to bridge the waiting period for delivery of a new machine or the time taken to recondition / modify an existing one" (EMAG 2017). Although these companies already provide on-demand production capacity, the business models of ECPs may be further extended in the future. For example, ECPs may offer *cloud manufacturing*, i.e., "a customer-centric manufacturing model that exploits on-demand access to a shared collection of diversified and distributed manufacturing resources to form temporary, reconfigurable production lines which enhance efficiency, reduce product lifecycle costs, and allow for optimal resource loading in response to variable-demand customer generated tasking" (Wu et al. 2013: p.1). Cloud manufacturing strives to provide "centralized operation management of the services, choice of different operation modes and embedded access of manufacturing equipment and resources" (Xu 2012: p.79). Those ECPs which offer cloud manufacturing may publish their services in a cloud platform that matches customer inquiries with a producer based on their qualitative and quantitative parameters, establishes and executes a (virtual) manufacturing system, and enables ECP performance evaluation, fee calculation, and payment processing (Ren et al. 2017).

Independent of the established ECP business model, the rise of MaaS has the potential to provide industrial companies with additional volume flexibility, accessed on-demand and without permanent capacity expansion, in order to successfully enable MTO approaches. However, on-demand production capacity comes at a price. On the one hand, the use of on-demand production capacity fosters companies' dependence on ECPs. It also requires the sharing of highly sensitive information, which could ultimately lead to hold-up problems (Haruvy et al. 2018). On the other hand, access to on-demand production capacity (and, therefore, volume flexibility) is likely to require initial upfront investments, e.g., for additional interface technologies such as inter-organizational information systems, the standardizing of planning and organizational processes, employee training, and fees such as availability guarantees for production facilities. Given the costs associated with these investments, the profitability of on-demand production capacity is highly dependent on the industrial companies' customers, in particular their changing preferences and, thus, the development of customer demand over time. This is to say that highly uncertain and volatile customer demand favors corresponding upfront investments, as companies then possess volume flexibility which allows them to expand their otherwise rigid internal production capacity as needed.

Investments in on-demand production capacity have to be evaluated in terms of the resultant managerial flexibility in response to the uncertain development of demand. Yet this is a complex task, and companies which follow principles of value-based management require appropriate methods for decision-support which do not yet exist (cf. Section 2). Hence, the aim of this paper is to develop a valuation method that addresses this situation. Thereby, real options analysis (ROA) comes into consideration which is "an adjusted version of decision tree analysis, involving a redistribution of probability masses such that risk is reallocated in a way that allows for discounting by the risk-free rate" (Benaroch and Kauffman 2000: p.202). ROA is an established method for evaluating investments which focuses on the flexibility of managerial action in response to uncertainty. Accordingly, in this paper, we address the following research question:

RQ: *How can an industrial company evaluate investments in on-demand production capacity considering managerial flexibility of action due to volume flexibility and uncertainty in demand?*

In order to answer this research question, we model and evaluate volume flexibility as a set of expansion options, and integrate the respective option values in an economic analysis of upfront investments using an expanded net present value approach (ENPV). Our research addresses a relevant real-world problem as an answer could facilitate investment decision making in the course of industrial companies' production capacity planning. The remainder of this paper is structured as follows: In Section 2, we review related work on manufacturing strategies, capacity planning, investment evaluation methods, and – in particular – ROA. In Section 3, we describe our research scenario, introduce basic assumptions, and present our model, which evaluates expansion options for on-demand production capacity. Afterwards, in Section 4, we demonstrate our model using an exemplary base case and then evaluate the validity and robustness of the model using randomly chosen simulations and subsequent sensitivity analyses. In Section 5, we discuss the managerial implications. Finally, in Section 6, we conclude our paper by addressing limitations and presenting an outlook for future research.

II.3.2 Theoretical Background, Related Work, and Research Method

In the following, we present related work to our research. Firstly, we discuss manufacturing strategies and capacity planning in the industrial sector. Secondly, we elaborate on investment evaluation methods in general before focusing our discussion on ROA.

II.3.2.1 Manufacturing Strategies and Capacity Planning

Companies may follow various different manufacturing strategies. Olhager and Östlund (1990) describe a "manufacturing continuum ranging from make-to-stock over assemble-to-order and make-to-order to engineer-to-order […]" (p.136). They discuss the customer order point (COP), i.e., the point in a manufacturing process at which a product is matched with an individual customer order. Depending on the degree of customization, the COP may vary between finished products in a make-to-stock concept and raw materials in an MTO concept (Olhager and Östlund 1990). Customized production and mass customization favor flexible MTO approaches. Chen et al. (2003) highlight the fact that MTO approaches require the close integration of suppliers, manufacturers, assemblers of components, and distributors of finished products in order to ensure short lead times. Thereby, digitalization favors the "integration of several different companies through value networks" (Kagermann et al. 2013: p.6). As a result, new forms of collaboration become feasible. For example, embedded manufacturing systems are vertically connected to business processes and horizontally networked with other business partners (Wang et al. 2016). Brettel et al. (2014) argue that "boundaries of companies deteriorate" (p.37) and that collaborative manufacturing becomes increasingly important. As a result of this trend in networked manufacturing, new business models (such as ECPs) emerge and open new market opportunities for companies (Kagermann et al. 2013; Monostori 2014).

As MTO approaches are especially prone to mistakes in capacity planning (cf. Section 1), such manufacturing strategies benefit from the opportunity to flexibly outsource production. Respective make-or-buy decisions in capacity planning have been well researched in the literature (Chase et al. 2004). Kremic et al. (2006) conduct an extensive literature review and conclude that motivations for outsourcing fall into three main categories: cost, strategy, and politics (the latter mostly in the case public organizations). Transaction-cost theory is often used to investigate the cost-saving potential of specialization and economies of scale, while the resource-based view is widely used to explain outsourcing from a strategic perspective

(Boulaksil and Fransoo 2010). In the latter case, companies apply outsourcing to concentrate on core competencies, or to have more flexibility to manage uncertain demand (Lankford and Parsa 1999). Decision support for capacity planning and the outsourcing of physical production is also well researched. For instance, Tomlin (2006) investigates the effects of volume flexibility on sourcing and contingent routing strategy in a single-product setting in the event that a company has the choice between different types of suppliers with and without volume flexibility. Applying Tomlin's approach, companies can investigate different capacity and sourcing strategies – particularly in the case of disruptions – in order to evaluate the volume flexibility of their suppliers. Dong and Durbin (2005) investigate surplus markets, on which suppliers can flexibly sell excess component inventory to other manufacturers experiencing a shortage. They illustrate that suppliers can profit from the opportunity to sell excess inventory in the event of low transaction costs on the surplus market. Tsai and Lai (2007) develop a mathematical approach to optimal decision making in joint production settings. Using this approach, companies producing joint products can arrive at the most mutually-advantageous decisions regarding capacity expansions and outsourcing.

In addition to the literature on dependent, company-internal, and incremental capacity choices, there is also literature on capacity choices that focuses on companies which choose not to periodically adjust their capacity but instead decide to source external capacity from ECPs. This allows the analysis of decision-specific components such as upper internal capacity limits and minimum contract sizes of ECPs. In terms of ECPs which provide services (rather than physical production), Aksin et al. (2008) research a call center and the problems it faces when making decisions about outsourcing, considering several frame conditions. The authors determine optimal capacity levels and characterize optimal pricing conditions for volume-based and capacity-based contracts offered by a vendor (ECP). Another example is the work of Dorsch and Häckel (2012), in which the authors investigate the on-demand exchange of excess capacity for cloud-services, and the effect that this has on excess capacity markets. They develop a mathematical model of the capacity-related optimization problem experienced by service providers with and without excess capacity, and find that flexibility offers economic benefits thanks to excess capacity markets. Furthermore, the same authors develop an optimization approach to investigate the effects that sourcing decisions have on operating costs for business processes, taking particular account of volatile demand and on-demand capacity from an external market (Dorsch and Häckel 2014). However, authors in the

aforementioned research streams on capacity optimization focus on the optimal allocation of existing resources rather than on the provision of decision support for those deciding for or against flexibility-enabling investments.

II.3.2.2 Investment Evaluation Methods

A well-established method for evaluating investments is to calculate the Net Present Value (NPV), which is calculated by subtracting the present value of cash outflows from the present value of cash inflows. If a project's NPV is greater than zero, the project is worth the investment (Myers 1984). To account for project uncertainty (i.e., risks), cashflows can be additionally discounted using a risk-adjusted discount rate. An alternative approach is to adjust cashflows to risk, and discount the adjusted cashflows by the risk-free interest rate (Schwartz and Trigeorgis 2004). However, literature often claims that the NPV underestimates the value of a project as it does not capture managerial flexibility of actions (Kogut and Kulatilaka 1994; Schwartz and Trigeorgis 2004; Lee and Lee 2015), which is a major success factor for appropriate decision making, particularly in the case of digitization projects (Brettel et al. 2014; Vyatkin et al. 2007; Lasi et al. 2014; Spath et al. 2013). As a result, strategically important projects are probably not undertaken as a result of incomplete valuations (Amram and Kulatilaka 1998).

One appropriate approach for capturing managerial flexibility of actions in response to uncertainty is ROA, which transfers option pricing models for financial assets to real-world investment decisions (Copeland and Antikarov 2003; Trigeorgis 1996). Both financial and real options include the opportunity, but not the obligation, to undertake a predetermined action at a future point in time (Luehrman 1998). Myers (1977) defines real options as "opportunities to purchase real assets on possible favorable terms" (p.163). Depending on the kind of managerial flexibility, several types of real options exist, e.g., options to expand, to contract, to abandon, to defer, and to switch (Trigeorgis 1996).

In this paper, we apply ROA in order to evaluate a manufacturing company's flexibility to commission an ECP, which the company may use to address uncertain levels of customer demand. We model respective volume flexibility as an expansion option, which was traditionally defined as an option to "expand the project's scale by making an additional investment" (Trigeorgis 1993: p.3). Dangl (1999) applies ROA to determine the optimal scale and timing of a manufacturing company's capacity expansion. The author concludes that uncertainty in the development of demand considerably increases the optimal scale of capacity

expansion and deferral of investment. Similarly, Benavides et al. (1999) research the optimal scale and timing of capacity expansions within semiconductor industries. They focus on alternative capacity expansion designs, and conclude that uncertainty in demand development favors designs for sequentially deployable expansions and late investment decisions. Lier et al. (2012) research sequential expansion options for modular chemical plants which can be gradually expanded during a fixed project term. This modular approach increases the project value response to uncertain demand development, as compared to large-scale chemical plants which are, at the outset, built to their final stage of expansion. Fernandes et al. (2012) evaluate an option designed to enable a company to stop outsourcing and expand its own production capacity. They find that demand uncertainty considerably affects decisions about integration, i.e., about the occurrence and timing of internal capacity expansions.

In our case, however, additional production capacity is only available at times when the company is able to expansion option. Hence, our type of expansion option is similar to the option of altering the scale, which requires the kind of managerial flexibility that enables a company to "increase the scale of a project/system (and thus the range of potential benefits) if circumstances are favorable; or […] reduce the scale (and thus potential losses) if circumstances are unfavorable" (Fichman et al. 2005: p.25). Abel et al. (1996) implicitly model an option to change scale by evaluating a company's flexibility to both invest and disinvest in production capacity. They conclude that the option to disinvest incentivized the company to make previous investments. In the context of multistage enterprise resource planning (ERP) investment projects, Wu et al. (2009) evaluate several types of real options, including a company's option to change the scale at each stage of a project.

As opposed to previous studies, in our case, option exercise initializes an external service and not an investment in the expansion of internal production capacity. In this vein, Benaroch et al. (2010) build a model for evaluating flexibility to out- and back-source IT service contracts. Contrary to our approach, they focus on an ECP's perspective, with the objective of identifying optimal contract flexibility in terms of service level agreements. In doing so, they neglect some aspects that we explicitly consider, such as the client company's potential for partial outsourcing (they apply an all-or-nothing approach), the possibility of increased costs if the client company's customers become dissatisfied, and an evaluation of necessary upfront investments. Wu et al. (2001) and Wu et al. (2002) research long-term contracting agreements and spot markets for non-storable goods and services. They differentiate between several

cases involving single and multiple buyers and sellers, applying von Stackelberg game-based theoretical frameworks in order to determine the prices at which market equilibrium is achieved. Thereby, Wu et al. (2001) evaluate long-term capacity options (which buyers obtain from sellers) based on Black and Scholes' (1973) and Merton's (1973) evaluations of options. This approach was further developed by Spinler et al. (2002) to include not only spot price uncertainty but also demand and cost uncertainty, and, subsequently, by Spinler et al. (2003) with a view to evaluating risk-sharing between the trading partners. Like our approach, all of these option pricing models based on Wu et al. (2001) consider a seller's reservation price (in our case: minimum contract size) and, if capacity is called, execution fee per unit of output. However, for our purposes, these models do not suit, as our aim is to model a company's (temporal) outsourcing decision problem, which yields additional dependencies on internal production costs, internal production capacity, and customer satisfaction. Klaus et al. (2014) built a model for IT-service providers to outsource excess demand to an ECP if internal service capacity is insufficient. Like us, they weigh the value of their option against the necessary upfront investments, while option exercise triggers costs for external service activation. Further similarities are their consideration of partial outsourcing and dissatisfied customers. However, these authors limit their approach to a one-time outsourcing decision, which must fully compensate the company for upfront investments. In contrast, we allow for several sequential outsourcing decisions: i.e., for a company's initial decision-making on upfront investments, we evaluate multiple (temporal) expansion options. Furthermore, we extend Klaus et al.'s (2014) approach by allowing the ECP to demand a minimum contract size. Despite their differences, the studies by Benaroch et al. (2010), Wu et al. (2001), and Klaus et al. (2014) have an essential property in common with our objective: Due to the trend toward highly individualized products, we consider a company that applies an MTO approach with no production of stock, which is similar to those authors' application context of IT-services that cannot be physically stored. In the context of manufacturing, we found only one other paper that uses ROA to evaluate temporal capacity expansion of companies with MTO approaches: Kleinert and Stich (2010) address companies in the machinery and equipment industry that source subcomponents from suppliers. As unforeseen problems might occur during the manufacturing process, these authors recommend that such companies consider the purchase of additional expansion options from their suppliers. Like our approach, a client company therefore weighs costs for enabling (purchasing) the expansion option – and for the actual option exercise against adverse effects of time delays (customer dissatisfaction in our

case). However, their approach is rather conceptual and is not transformed into a valuation formula. Unlike our approach, their expansion option only refers to a single customer order, and the possibility that the company might produce subcomponents internally is excluded.

To the best of our knowledge, existing literature is insufficient for our purposes, which has encouraged us to develop an appropriate approach for the evaluation of investments which enable the commissioning of ECPs, i.e., recourse to flexible, on-demand production capacity. Thereby, neither an isolated NPV approach nor an isolated ROA is sufficient: instead, a combination of both approaches seems promising. Panayi and Trigeorgis (1998) introduce the ENPV approach, which enhances the common NPV by integrating ROA[3]. For example, investments in a software platform can be evaluated using the ENPV approach: Such a project is likely to exhibit a negative NPV for the platform itself, but may become profitable when the flexibility to develop additional software applications on this platform is taken into account. In this paper, we also apply an ENPV approach. Since our scenario considers the evaluation of upfront investments without considering further deterministic cashflows, it is kept deliberately simple (i.e., the NPV equals cash outflows due to upfront investments). More precisely, in our scenario, the business case of upfront investments must solely pay off by obtained flexibility of action. Nevertheless, our approach can be easily extended for scenarios with additional cash inflows and outflows of the initial (enabling) project. We introduce our ENPV approach in the following section.

II.3.3 Evaluation of On-Demand Production Capacity

In this section, we present our ENPV approach, including ROA. Therefore, we firstly describe our scenario of an MTO production setting. Secondly, we elaborate on assumptions inherent in the model before presenting our approach for modeling and evaluating volume flexibility using on-demand production capacity as an expansion option.

II.3.3.1 Scenario

As previously mentioned, we consider an industrial company that manufactures highly individualized products using an MTO approach. Customers expect the company to deliver products within a contractually stipulated timeframe. The rate of incoming customer orders is highly volatile and, thus, the company must have an appropriate capacity planning. The central

[3] Expanded Net Present Value (ENPV) = Traditional NPV + Value of real options (similar to Panayi and Trigeorgis 1998)

tradeoff for the company is between idle capacity and capacity shortages. Seeking volume flexibility, the company considers commissioning an ECP that offers flexible production capacity on-demand. We assume that the ECP's business model is based on a contractually specified pay-per-use payment model, i.e., the industrial company pays for each unit produced externally. The contract also specifies a minimum contract size for activating the external service, which the company must meet in order to ensure a minimum return for the ECP. Commissioning on-demand production capacity also requires initial upfront investments in, for example, additional interface technologies such as inter-organizational information systems, the standardization of planning and organizational processes, employee training, and fees such as availability guarantees for the ECP's production facilities. In sum, the company faces the challenge to (ex-ante) evaluate the business value of volume flexibility using on-demand production capacity, taking into account both the necessary upfront investments and the highly volatile nature of customer orders. In the following we present our model, which addresses this real-world problem using ROA. Firstly, however, we introduce the necessary assumptions.

II.3.3.2 Basic Scenario and Model Assumptions

We consider a time horizon with regard to an arbitrary time t_n for the company's capacity planning. t_0 is the current point in time, at which the company must decide whether to sign a framework contract with an ECP for a contract term extending until t_n. This contract specifies the company's right to use on-demand production capacity (i.e., to activate the ECP's service) at $n \in \mathbb{N}$ equally distributed times t_i with $i \in [1, n]$ which divide the planning horizon until t_n into n equal periods. More precisely, this means that, if the company signs the framework contract in t_0, it can decide n times whether seizing on-demand production capacity is (for the duration of one period) preferable given the current volatility of customer demand (Figure II.3-1). In terms of ROA, the company can sign the framework contract to purchase n independent expansion options from the ECP. We enumerate expansion options with $i \in [1, n]$ and refer to the maturity date of each option using $T_i = t_i$.

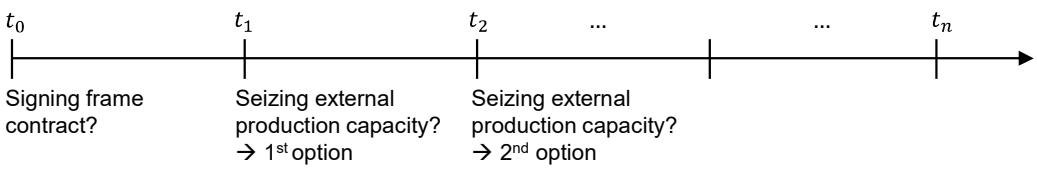


Figure II.3-1: Planning horizon in the Basic Scenario – Own Illustration

The objective of our approach is to investigate whether or not the company should sign the framework contract with the ECP. This involves comparing the value of the expansion options available to the company with the cash outflows required for the necessary upfront investments. As stated above, we apply an ENPV approach to evaluate the company's overall business case (V_0):

$$V_0 = \sum_{i=1}^{n} C_{T_i}(t_0) - I(t_0) \quad (1)$$

Thereby, $C_{T_i}(t_0)$ is the present value of the expansion option with a maturity date in T_i from the perspective of t_0. Accordingly, $I(t_0)$ is the sum of cash outflow for necessary upfront investments in t_0, which is independent of expansion options' exercise. More precisely, as the company decides for or against upfront investments at the current point in time t_0, these upfront investments do not influence the company's future decision making on exercising (temporal) expansion options. If the business case yields $V_0 > 0$, signing the framework contract with the ECP is preferable.

The company sells its MTO products in order to generate revenue. We assume highly volatile customer demand which yields (for a specific MTO product) a total periodical revenue $R(t_i)$. We choose $R(t_i) \geq 0$ to be our only stochastic variable for determining the value of the expansion option since this is a monetary quantity which facilitates the application of ROA (compared to, for instance, the modeling of volatile customer orders).

Assumption 1: $R(t_i)$ follows a multiplicative (stochastic) binomial process over discrete time periods with a constant mean $\mu > 0$ and standard deviation (volatility) $\sigma > 0$. The company observes $R(t_0)$ at the current point in time t_0 and uses this information to predict uncertain future revenues $R(t_i)$.

Moreover, the company possesses a fixed internal production capacity which can process a certain (periodical) maximum revenue $\bar{R} \geq 0$. We assume revenue per unit sold and respective internal production costs $k_{int} \in [0,1]$ (as a proportion of this revenue) to be constant for all customers and all periods until t_n. Thus, for $R(t_i) \leq \bar{R}$, $k_{int} * R(t_i)$ refers to the company's total internal production costs in t_i.

Assumption 2: The company's maximum revenue $\bar{R}$, revenue per unit sold, and internal production costs k_{int} are constant until t_n. Thereby, $\bar{R}$ is a multiple of revenue per unit sold.

Because of the current trend toward MTO approaches, we do not consider stocks of finished products. Due to customer expectations of ever-shorter lead times, we assume that customers will become dissatisfied if the company does not process their orders within a certain time frame.

Assumption 3: Customers expect the company to process their order within a certain time frame which equals one planning period (e.g., one month). If the company cannot deliver a product within this time frame, the respective production costs rise to k_{dis}, with $k_{dis} > k_{int}$ representing the cost of dissatisfied customers.

Thus, if $R(t_i)$ exceeds $\bar{R}$ at time t_i, the production costs associated with dissatisfied customers k_{dis} are incurred and apply to all excess revenue $R(t_i) - \bar{R} \geq 0$. In practice, k_{dis} may result from contractual penalties incurred due to the violation of service level agreements, loss of customer lifetime value, loss of reputation, loss of revenue due to the rejection or cancellation of orders, or a combination of these factors.

However, if an ECP is available, the company can use on-demand production capacity to avoid customer dissatisfaction. At expansion option i's maturity date T_i, the company reviews its current periodical revenue $R(T_i)$ (which is then known) to determine if production costs could be lowered using the ECP's production capacity. In order to reduce complexity, we neglect the fact that the ECP's production capacity is limited and may involve supply-dependent pricing structures.

Assumption 4: The ECP's production capacity is high enough to meet the company's excess revenue, and the ECP charges constant unit prices (i.e., external production costs, from the client company's perspective) of k_{ext} with $k_{dis} > k_{ext} > k_{int}$. Like k_{int} and k_{dis}, k_{ext} is proportional to the company's revenue per unit sold.

As the ECP aims to generate profit, it is reasonable to assume that corresponding external production costs per unit k_{ext} are higher than internal production costs per unit k_{int}. In addition, k_{ext} must be lower than k_{dis}, otherwise the ECP will not be competitive. As

described in Section 3.1, the company's contract with the ECP specifies a minimum contract size MCS every time t_i the company exercises an expansion option, i.e., draws on the on-demand production capacity. As k_{ext} is constant, $\underline{R}$ refers to the minimum revenue the company must draw from its customers in order to yield the required MCS with the ECP, i.e., $\underline{R} = \frac{MCS}{k_{ext}}$.

Assumption 5: MCS and $\underline{R}$ are constant until t_n. If the company does not meet the agreed MCS, it must pay the difference.

Both $\underline{R}$ and MCS significantly influence the activation of external services. Finally, to modify and apply the binomial tree model of Cox et al. (1979) (Section 3.3.2), we require a rather technical assumption.

Assumption 6: The company is a risk-neutral decision maker.

II.3.3.3 Modeling an Expansion Option for On-Demand Production Capacity

In this section, we present our ROA. Firstly, we describe the decision the company must make about seizing on-demand production capacity. Secondly, we develop our option evaluation model based on Cox et al. (1979).

II.3.3.3.1. Decision Problem of Seizing On-Demand Production Capacity

The decision problem focuses on total periodical revenue $R(t_i)$, as $R(t_i)$ is the only stochastic parameter in our model. Starting in $t_i = t_0$, we model $R(t_i)$ as a multiplicative binomial process, i.e., as a binomial tree that forks at each discrete point in time t_i into two different values, both of which reflect uncertainty. One value represents a possible future increase in $R(t_i)$, the other a possible future decrease. We illustrate an exemplary binomial tree with a time horizon of three periods in Figure II.3-2.

We introduce $u > 1$ and $d < 1$ as factors for upward and downward movement of $R(t_i)$, respectively. Thereby, starting at t_0, $R_{u_{t_0}}(t_1) = R(t_0) * u$ represents a possible (future) increase in the total periodical revenue, whereas $R_{d_{t_0}}(t_1) = R(t_0) * d$ represents a possible (future) decrease. At time t_i, the binomial tree possesses $i + 1$ different nodes. $W_{t_{i-1},s} = (w_{t_0}, w_{t_1}, \ldots, w_{t_{i-1}})$ indicates the filtration or "history" of upward and downward movements previous to t_i, with $w_j \in \{u_j, d_j\}$, j$\in\{t_0, t_1, \ldots, t_{i-1}\}$, and $s \in \{1, \ldots, \mathrm{i} + 1\}$ used to number

different nodes at time t_i. This filtration helps to unambiguously identify different nodes at a certain point in time t_i, which is necessary for implementing our algorithm. However, for the sake of readability, we explain the following with a reduced notation that waives all filtrations.

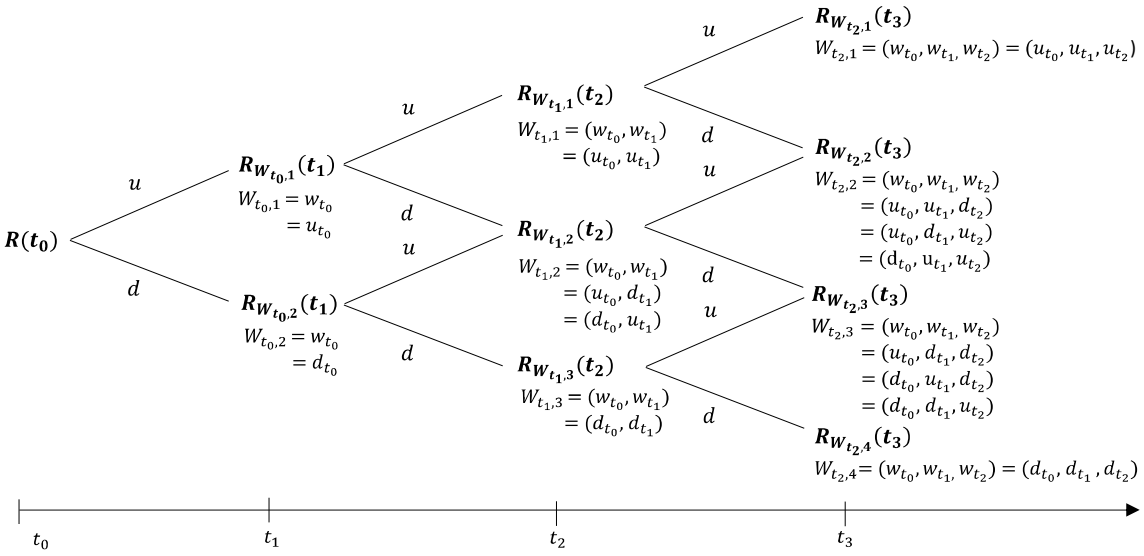


Figure II.3-2: *Binomial tree of the total periodical revenue* $R(t_i)$ – Own Illustration

At time $t_i = T_i$, the company must decide to exercise an expansion option. Therefore, it observes the total revenue of the current period $R(T_i)$ and computes the total production costs with (TPC_{Ex}) and without (TPC_{NoEx}) recourse to on-demand production capacity. The former represents an exercise of the expansion option, the latter represents no exercise. Afterwards, the company subtracts the respective total production costs from the total revenue of the current period (which the company observes) analogous to common option pricing theory. Note that, due to our modelling of cost structure (k_{dis} also includes lost revenue resulting from insufficient production capacity), in both cases (exercise or not) the company accepts every customer order and tries to meet this demand by minimizing related costs. To summarize, the company would only exercise the option if the payoff using on-demand production capacity were greater than the payoff without using on-demand production capacity:

$$R(T_i) - TPC_{Ex} > R(T_i) - TPC_{NoEx} \tag{2}$$

From this equation, we can determine that the company only exercises the corresponding expansion option for $TPC_{NoEx} > TPC_{Ex}$. Hence, at time T_i, the value of the expansion option $C_{T_i}(T_i)$ equals the following:

$$C_{T_i}(T_i) = \max\{TPC_{NoEx} - TPC_{Ex}\,; 0\} \tag{3}$$

For the computation of TPC_{Ex} and TPC_{NoEx}, we must differentiate between two cases: $\bar{R} \geq \underline{R}$ and $\bar{R} \leq \underline{R}$. This is because the relationship between these two parameters critically influences the company's decision problem (cf. Table II.3-1). As $\bar{R}$ is determined by the focal company and $\underline{R}$ by the ECP's business model, both cases can occur. Depending on $R(T_i)$, $\bar{R}$, $\underline{R}$, k_{int}, k_{ext}, and k_{dis}, the company can then determine the proportion of the revenue that should be produced in-house or by the ECP.

Cases for $\bar{R} \geq \underline{R}$		
Case	Computation of TPC_{NoEx} and TPC_{Ex}	$TPC_{NoEx} - TPC_{Ex}$
I.1: $R(T_i) \leq \underline{R} \leq \bar{R} \leq \underline{R} + \bar{R}$	$TPC_{NoEx} = R(T_i) * k_{int}$ $TPC_{Ex} = \underline{R} * k_{ext}$	$= R(T_i) * k_{int} - \underline{R} * k_{ext} < 0$
II.1: $\underline{R} \leq R(T_i) \leq \bar{R} \leq \underline{R} + \bar{R}$	$TPC_{NoEx} = R(T_i) * k_{int}$ $TPC_{Ex} = \underline{R} * k_{ext} + \left(R(T_i) - \underline{R}\right) * k_{int}$	$= \underline{R} * (k_{int} - k_{ext}) < 0$
III.1: $\underline{R} \leq \bar{R} \leq R(T_i) \leq \underline{R} + \bar{R}$	$TPC_{NoEx} = \bar{R} * k_{int} + (R(T_i) - \bar{R}) * k_{dis}$ $TPC_{Ex} = \underline{R} * k_{ext} + \left(R(T_i) - \underline{R}\right) * k_{int}$	$= (R(T_i) - \bar{R}) * (k_{dis} - k_{int}) - \underline{R} * (k_{ext} - k_{int}) \lessgtr 0$
IV.1: $\underline{R} \leq \bar{R} \leq \underline{R} + \bar{R} \leq R(T_i)$	$TPC_{NoEx} = \bar{R} * k_{int} + (R(T_i) - \bar{R}) * k_{dis}$ $TPC_{Ex} = \bar{R} * k_{int} + (R(T_i) - \bar{R}) * k_{ext}$	$= (R(T_i) - \bar{R}) * (k_{dis} - k_{ext}) > 0$
Cases for $\bar{R} \leq \underline{R}$		
I.2: $R(T_i) \leq \bar{R} \leq \underline{R} \leq \underline{R} + \bar{R}$	$TPC_{NoEx} = R(T_i) * k_{int}$ $TPC_{Ex} = \underline{R} * k_{ext}$	$= R(T_i) * k_{int} - \underline{R} * k_{ext} < 0$
II.2: $\bar{R} \leq R(T_i) \leq \underline{R} \leq \underline{R} + \bar{R}$	$TPC_{NoEx} = \bar{R} * k_{int} + (R(T_i) - \bar{R}) * k_{dis}$ $TPC_{Ex} = \underline{R} * k_{ext}$	$= (R(T_i) - \bar{R}) * k_{dis} + \bar{R} * k_{int} - \underline{R} * k_{ext} \gtrless 0$
III.2: $\bar{R} \leq \underline{R} \leq R(T_i) \leq \underline{R} + \bar{R}$	$TPC_{NoEx} = \bar{R} * k_{int} + (R(T_i) - \bar{R}) * k_{dis}$ $TPC_{Ex} = \underline{R} * k_{ext} + \left(R(T_i) - \underline{R}\right) * k_{int}$	$= (R(T_i) - \bar{R}) * (k_{dis} - k_{int}) - \underline{R} * (k_{ext} - k_{int}) \lessgtr 0$
IV.2: $\bar{R} \leq \underline{R} \leq \underline{R} + \bar{R} \leq R(T_i)$	$TPC_{NoEx} = \bar{R} * k_{int} + (R(T_i) - \bar{R}) * k_{dis}$ $TPC_{Ex} = \bar{R} * k_{int} + (R(T_i) - \bar{R}) * k_{ext}$	$= (R(T_i) - \bar{R}) * (k_{dis} - k_{ext}) > 0$

Table II.3-1: Cases for the company's decision problem at time $t_i = T_i$

In cases I.1 and I.2, $R(T_i)$ is lower than or equal to $\underline{R}$ and $\bar{R}$. If the company does exercise the expansion option in these cases, it cannot, or will only just, meet the required MCS with its customer demand, and will simultaneously fail to utilize its internal production capacity (i.e., it outsources customer demand for increased production costs of $k_{ext} > k_{int}$). Conversely, even if the company does not exercise the expansion option, its internal production capacity is sufficient to avoid dissatisfied customers. This is to say that seizing on-demand production capacity would increase total production costs, and can therefore never be profitable ($TPC_{NoEx} - TPC_{Ex} < 0$). The same applies in case II.1: As internal production capacity is still sufficiently large, outsourcing production for $k_{ext} > k_{int}$ can never be profitable. In case II.2, seizing on-demand production capacity can be profitable if the disadvantage of not or only just meeting the required MCS – and therefore (due to outsourcing) not utilizing internal production capacity – is overcompensated for by the advantage of avoiding dissatisfied customers (which would occur without the ECP). In cases III.1 and III.2, the profitability of exercising the expansion option further increases, as the company meets the required MCS with its customer demand. However, for $(T_i) < \underline{R} + \overline{\mathrm{R}}$, the company cannot exercise the expansion option and simultaneously utilize all of its internal production capacity, which is a disadvantage that can still exceed the monetary benefits of avoiding dissatisfied customers. For increasing $R(T_i)$ until $R(T_i) = \underline{R} + \overline{\mathrm{R}}$ (upper interval boundary in cases III.1 and III.2), this disadvantage (and therefore the cost of activating the external service) shrinks to zero. Exercising the expansion option in cases IV.1 and IV.2 ($\underline{R} + \overline{\mathrm{R}} \leq R(T_i)$) is always profitable, since the total internal production capacity is utilized and $k_{dis} > k_{ext}$. Thereby, the company can fully meet the required MCS. As using on-demand production capacity is not obligatory, the company would only exercise the option for $TPC_{NoEx} - TPC_{Ex} \geq 0$.

Figure II.3-3 schematically illustrates the payoff $TPC_{NoEx} - TPC_{Ex}$ and the resulting real option values at time $t_i = T_i$. In Figure 3b, i.e., for $\bar{R} \leq \underline{R}$, we illustrate two cases which can occur depending on parameter values (Cases II.2 and III.2 in Table 1 yield two possible payoff progressions depending on whether exercising the expansion option is profitable, i.e., “at the money”, for $R(T_i) \leq \underline{R}$ or $\underline{R} \leq R(T_i)$).

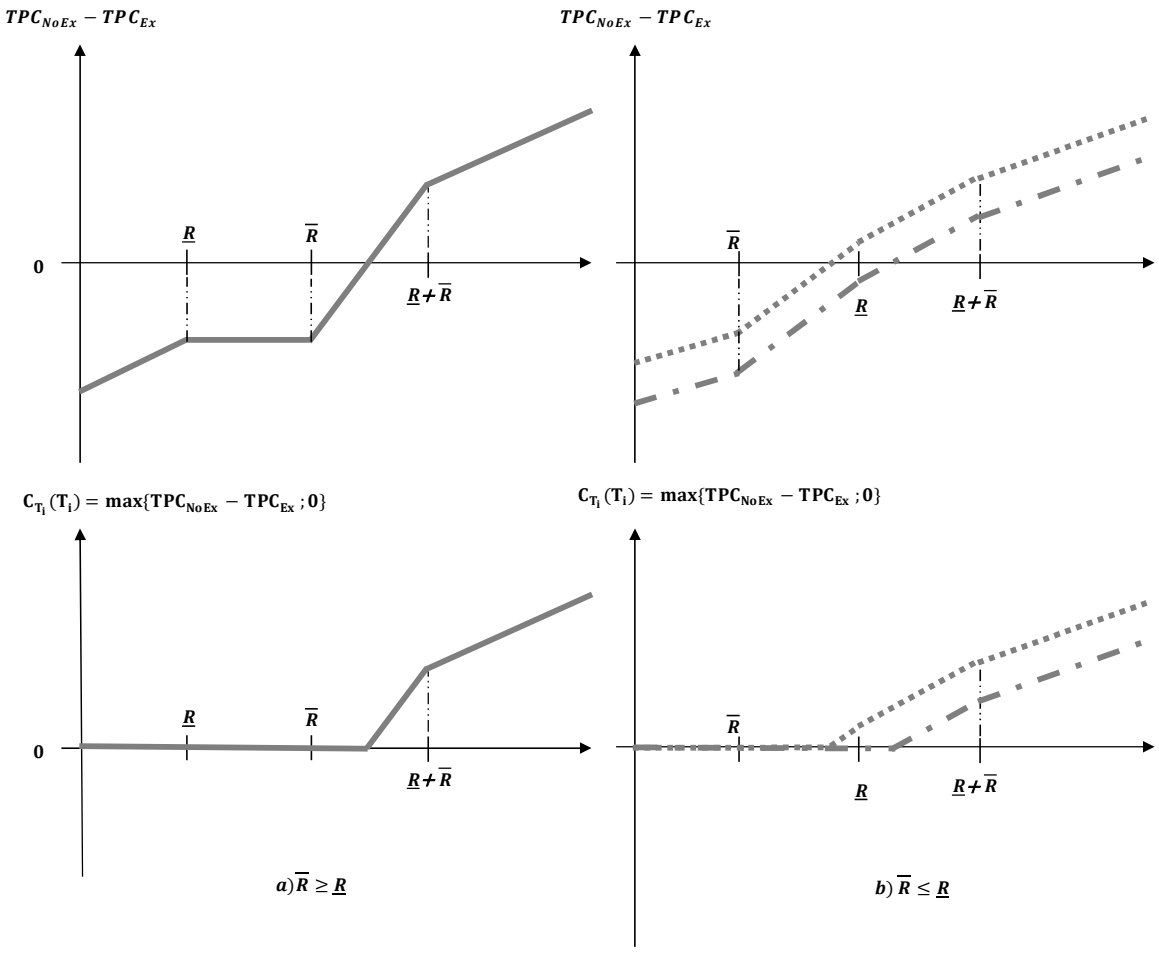


Figure II.3-3: *Cash flows for option exercise at time $t_i = T_i$ for $\bar{R} \geq \underline{R}$ and $\bar{R} \leq \underline{R}$*

II.3.3.3.2. Valuation of the Expansion Option

When entering a framework contract with the ECP, the company has n independent expansion options, whereas the duration of the $i \in n^{th}$ expansion option equals i periods. As the company can exercise each option only once at the respective maturity date, we can apply the established option pricing for European call options. Thereby, $R(t_i)$ is the underlying of our expansion option, since its stochastic development directly affects the expansion option's value. We modify and apply the binomial tree model of Cox et al. (1979), which enables the risk-neutral evaluation of European call options. Binomial tree models are one of the most commonly used methods for option evaluation as they are easy to comprehend and easy to adapt to customized input parameters (Copeland and Tufano 2004). In particular, we choose this discrete-time approach rather than a continuous-time approach, since the latter would

exhibit increased mathematical complexity which may limit applicability for practitioners (Hauschild and Reimsbach 2015).

Since we assume risk-neutral decision-making (Assumption 6), we can apply formulae of Cox et al. (1979) to model the stochastic development of the company's total periodical revenue $R(t_i)$:

$$u = e^{\sigma * \sqrt{\Delta t}}, \qquad d = e^{-\sigma * \sqrt{\Delta t}}, \qquad p = \frac{(1 + r_f)^{\Delta t} - d}{u - d} \tag{4}$$

As mentioned above, $u > 1$ and $d < 1$ are factors influencing the extent of $R(t_i)$'s upward and downward movement within a single time increment. p $[1 - p]$ is the probability of $R(t_i)$ moving upward [downward] within the next period. r_f is the risk-free interest rate. In addition, Cox et al. (1979) introduce a necessary inequality: $d < 1 + r_f < u$ (no-arbitrage assumption). Following Cox et al. (1979), we can now determine the value of the company's expansion options. As we consider n to represent independent expansion options, which are indicated using $i \in [1, n]$, we separately evaluate each expansion option i by computing C_{0,T_i} and then total these values in order to weigh them against cash outflows for upfront investments (Equation 1). Thus, for each expansion option i, we model the binomial tree from $t_i = t_0$ to $t_i = T_i$ as illustrated in Figure 2. Then, in the reverse direction, i.e., from end nodes at the respective maturity date $t_i = T_i$ to root t_0, we conduct option evaluation. More precisely, for expansion option i, we start option evaluation by determining the option value $C_{T_i}(t_i)$ in $t_i = T_i$ according to Equation 3.

As the binomial tree possesses $i + 1$ end nodes in T_i, we must compute $i + 1$ different values for $C_{T_i}(T_i)$ (which we differentiate by applying filtrations as introduced in Section 3.3.1). Since $R(t_i)$ is the only stochastic variable in our model, the subtraction of each end node $TPC_{NoEx} - TPC_{Ex}$ depends only on this variable.

In order to determine the value of the expansion option from the perspective of t_0, i.e., $C_{T_i}(t_0)$, we must compute the probability-weighted average of all $C_{T_i}(T_i)$ and discount them to the present. Reintroducing the filtration notation, Figure II.3-4 illustrates an example with three periods.

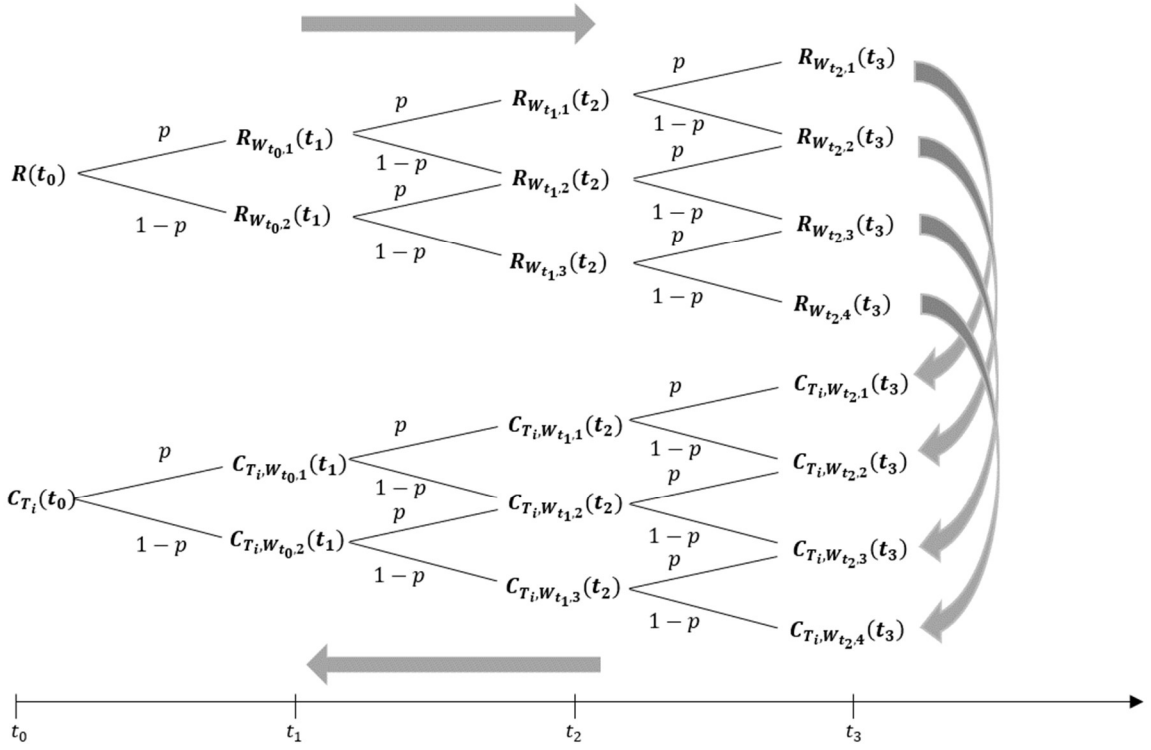


Figure II.3-4: Binomial tree model for option evaluation – Own illustration

For example, the probability of $C_{T_i,\,W_{t_2,\,1}}(t_3)$ equals $p\left(C_{T_i,\,W_{t_2,\,1}}(t_3)\right) = p^3$. Considering all end nodes $s \in \{1, \ldots, \mathrm{i}+1\}$ in the tree, we can compute the value of the expansion option in t_0:

$$C_{T_i}(t_0) = \frac{\sum_s p\left(C_{T_i,\,W_{t_{i-1},s}}(T_i)\right) * C_{T_i,\,W_{t_{i-1},s}}(T_i)}{(1+r_f)^{T_i}} \tag{5}$$

This procedure must be reiterated for every expansion option $i \in [1, n]$. Once this task has been completed, we use Equation 1 to evaluate the company's overall business case V_0.

As we illustrate in Section 2, ROA is widely applied in investment decision analysis. However, as we adapt option pricing from financial option evaluation, we must analyze the original requirements for the valid application of this method. Unfortunately, this analysis has been neglected by many other authors applying ROA (Ullrich 2013). Firstly, following Ullrich (2013), one requirement for the valid application of traditional option pricing models is a strike price that is constant or modeled for its stochastic nature. Within our ROA, we do not explicitly model a strike price which is implicitly part of the subtraction $TPC_{NoEx} - TPC_{Ex}$. However, if we were to aggregate all constant cost factors in each of the cases presented in

Table 1, this would equal a formal representation of the strike price. As a result, we would find that the strike price is only constant within each of the cases but not between different cases. Hence, in order to validly compute the value of the expansion option, our approach must take the stochastic nature of the strike price into consideration. We meet this requirement: As the strike price is case-specific, it only depends on one stochastic variable, which is $R(t_i)$. Therefore, for each end node in $R(t_i)$'s binomial tree, we obtain exactly one value for the strike price of the expansion option. Hence, our approach to ROA is valid in this respect. Secondly, we confirm that each expansion option can be exercised only once at its maturity date. The option's term is already specified when the company makes a decision about signing the framework contract. Thirdly, the value of the underlying must evolve according to a Geometric Brownian Motion (GBM) and exhibit a constant variance. This requirement of a GBM originally refers to continuous-time models. In our discrete-time model, the underlying must therefore evolve according to a multiplicative binomial diffusion process which converges (for decreasing-length time increments) to a GBM (Benaroch and Kauffman 1999). Due to Assumption 1, both requirements apply in the case of the company's total periodical revenue $R(t_i)$. Fourthly, for financial options there must exist a "complete market" that allows continuous trading of both the underlying and the option. As ROA evaluates flexibility of action, this requirement does not usually apply to either the underlying or the option. This is a long-standing problem in ROA literature, and we follow Benaroch and Kauffman (1999) who refer to Mason and Merton (1985) in stating that "irrespective of whether a project is traded, we seek to determine what the project cashflows would be worth if they were traded" (p.77).

II.3.4 Evaluation of the Model

In this section, we demonstrate how our model can be applied in order to evaluate upfront investments in flexible on-demand production capacity. We begin by presenting a set of freely-selected scenario parameters. As manually selected parameters are biased in their validity, we subsequently conduct randomly chosen simulations and sensitivity analyses in order to demonstrate the robustness of our model.

II.3.4.1 Basic Case

As stated in Section 3.1, we use the example of a company that manufactures a single but individualized product using an MTO approach. Seeking to increase volume flexibility, the

company considers commissioning an ECP that offers flexible on-demand production capacity. The company calculates that accessing such on-demand production capacity will require an upfront investment of $I_0 = \$\,300{,}000$ for availability guarantees and the necessary IS infrastructure. Regarding Equation 1, we assume this to be the entirety of cash outflows for upfront investments. The company would enter a 12-month framework contract with the ECP. The contract specifies that the company has the option to decide the on-demand production capacity at the end of every month, meaning that the company will obtain 12 expansion options. Independent of this opportunity, the company's own internal production capacity enables it to process a constant maximum revenue of $\overline{\mathrm{R}} = \$\,1{,}000{,}000$ per month. The ratio of internal production costs to customer revenue equals $k_{int} = 0.7$, and the company's total periodic revenue for the current month $R(t_0) = \$\,1{,}000{,}000$. These figures are used for future revenue predictions. By analyzing historical data, the company estimates that the monthly volatility of $R(t_i)$ will equal 15%, i.e., $\sigma = 0.15$. If customer demand cannot be satisfied, the company estimates costs for dissatisfied customers to a proportion of $k_{dis} = 1.1$ of customer revenue, i.e., due to the loss of customer lifetime value and order cancellations, the company incurs costs exceeding the revenue of a single MTO product. Entering the framework contract with the ECP would enable outsourcing. In the contract, the ECP specifies a minimum contract size of $MCS = \$400{,}000$ for each option exercised, with external production costs to a proportion of $k_{ext} = 0.8$ of customer revenue. Hence, due to $MCS = \underline{R} * k_{ext}$, the company's revenue from its customers that yields the required MCS equals $\underline{R} = \$500{,}000$. Using this information, the company can apply our approach for ROA in order to quantify the value of flexible on-demand production capacity, and then decide whether to make the required initial upfront investment. Assuming an annual risk-free interest rate r_f = 0.7%[4] for risk-neutral evaluation, we obtain the results illustrated in and below Figure II.3-5:

[4] r_f = 0.7% is the mean of the 3-month U.S. Treasury Bill yields observed over the last 10 years (Mukherji 2011; U.S. Department of the Treasury 2017).

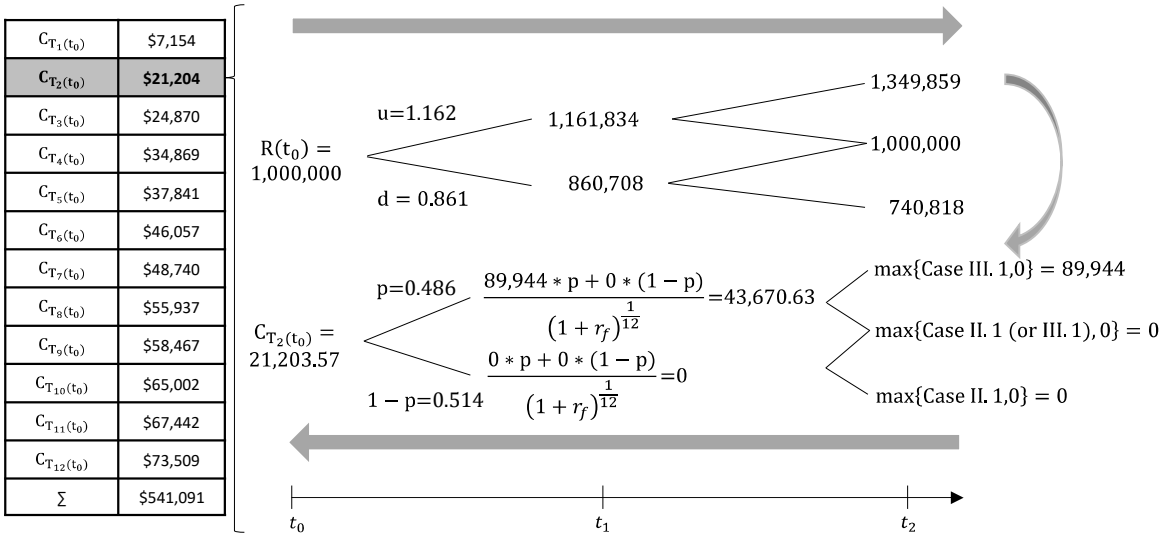


Figure II.3-5: Option Values in t_0 and exemplary computation for $C_{T_2}(t_0)$

- Value of expansion options $\sum_{i=1}^{12} C_{T_i}(t_0) = \$\ 541{,}091$
- Upfront investments $I_0 = \$\ 300{,}000$
- Business case value $V_0 = \$\ 241{,}091$

Since the overall business case has a monetary value greater than zero, the company should make the upfront investment and enter the framework contract with the ECP.

II.3.4.2 Simulation and Sensitivity Analyses

II.3.4.2.1. Simulation

In order to demonstrate the robustness of our model, we conducted randomly chosen simulations and sensitivity analyses. For this purpose, we implemented our model using Microsoft Excel supported by Visual Basic for Application macros, and chose to draw uniformly distributed model parameters from the following intervals (we assume $\overline{R}$ and k_{int} to be constant and to equal our basic case):

- **Annual risk-free interest rate $r_f \epsilon [0; 0.052]$:**

  We chose 5.2% as the upper interval boundary, since the maximum annual return on a 3-month U.S. Treasury Bill within the last 10 years amounted to 5.2% (Mukherji 2011; U.S. Department of the Treasury 2017).

- **Volatility of total periodical revenue $\sigma \epsilon [0.001 + ln(1 + r_f); 1]$:**

We chose this lower interval boundary for σ due to the no-arbitrage condition in Cox et al. (1979)'s binomial tree model: $d < 1+r_f < u$, i.e., $e^{-\sigma*\sqrt{\Delta t}} < 1 + r_f < e^{\sigma*\sqrt{\Delta t}}$. Solving this inequality for σ, we obtained $\sigma > \frac{ln(1+r_f)}{\sqrt{\Delta t}} = ln(1 + r_f)$ (with $\Delta t = 1$). For the interval's upper boundary, we arbitrarily chose $\sigma = 1$, i.e., a periodical volatility of $R(t_0)$ of 100%.

- **Initial month's total periodical revenue $R(t_0)\epsilon[500,000; 1,500,000]$:**
  We arbitrarily chose to draw $R(t_0)$ from a corridor around the base case's $\overline{R}$.
- **External production costs per unit $k_{ext} = 0.7 * (1.001 + q), q\epsilon[0, 0.5]$:**
  Assumption 4 argues that k_{int} must be lower than k_{ext}. Therefore, we scaled k_{ext} with a randomly chosen surcharge of up to 50% of $k_{int} = 0.7$.
- **Production costs per unit for dissatisfied customers $k_{dis} = k_{ext} * (1.001 + p), p\epsilon[0, 0.5]$:**
  Assumption 4 argues that k_{ext} must be lower than k_{dis}. Therefore, we scaled k_{dis} with a randomly chosen surcharge of up to 50% of k_{ext}.
- **Contract term $T_n\epsilon[1; 24]$:**
  We arbitrarily chose contract terms between 1 and 24 months. Each month equals one real option.
- **Minimum contract size $MCS\epsilon[0; 1,000,000]$:**
  We arbitrarily chose to draw MCS from a corridor around the base case's MCS.

Due to the many possible parameter combinations, we repeated our simulation 300,000 times to produce a high quality sensitivity analyses. For each simulation we ran, our algorithm drew input parameters according to the intervals presented, and calculated the value of real options. Accounting for all simulations, we achieved the results depicted in Figure II.3-6.

Within our simulation, the aggregated values of expansion options $\sum_{i=1}^{n} C_{0,T_i}$ vary between zero and \$15,485,424. Although we observe a long tail that we aggregated in Figure 6 for values greater than \$8,000,000, approximately 55% of simulation runs yielded values between \$]0; 1,000,000]. In only 5% of all simulation runs the aggregated value of expansion options is zero, i.e., in 95% of all simulation runs the aggregated value of expansion options is positive and, thus, would help to amortize initial upfront investments. Results of our simulation

indicate that volume flexibility using on-demand production capacity from an ECP is of considerable value to manufacturing companies.

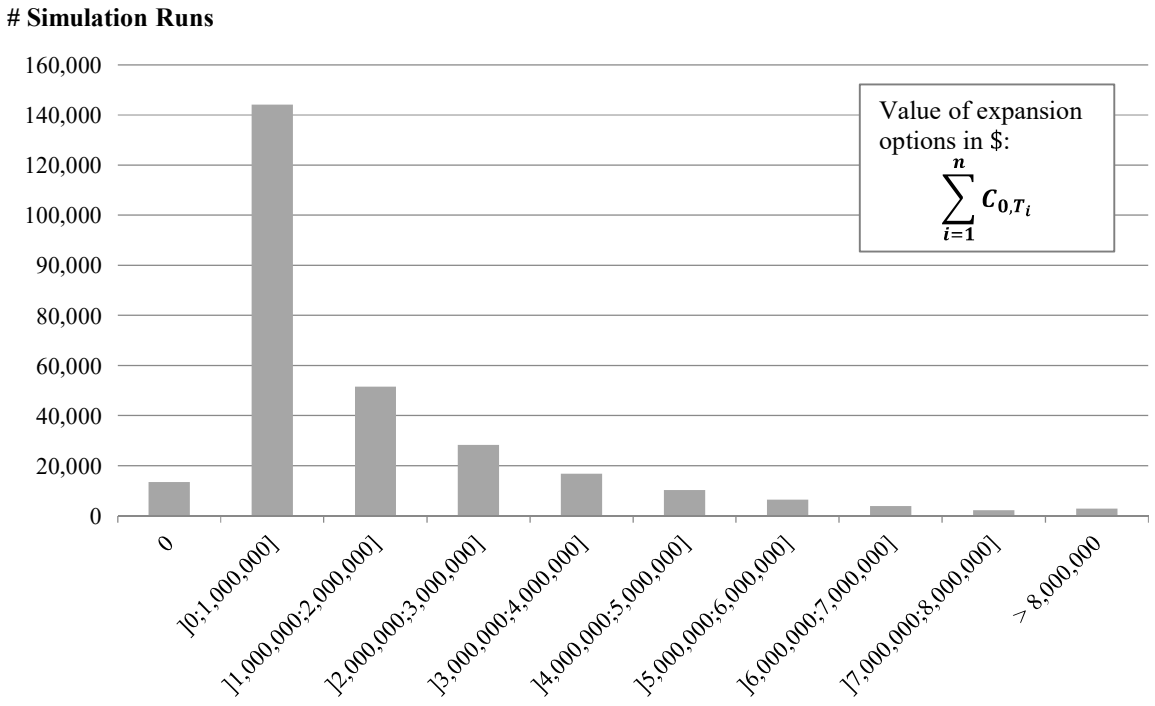


Figure II.3-6: Histogram with absolute simulation results

II.3.4.2.2. Sensitivity Analyses

In order to provide further analysis, we depict sensitivities to our results in Figure II.3-7. To do so, we apply sensitivity analyses according to the famous quantities "Greeks" to verify the validity of our model in terms of common option pricing theory. In particular, we analyze the univariate sensitivities of expansion option values to their contract term T_n ("Theta"), the annual risk-free interest rate r_f ("Rho"), and the volatility of the total periodical revenue σ ("Vega"). In addition to the "Greeks", we analyze univariate sensitivity to MCS, $R(t_0)$, k_{ext}, and k_{dis}, as these were factors that varied in our simulation.

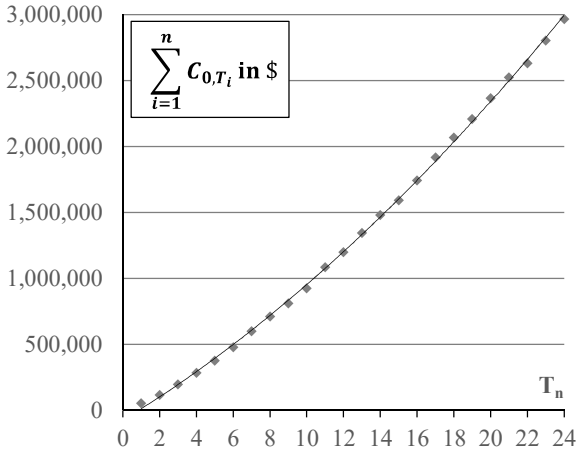


Figure II.3-7a: Contract duration T_n

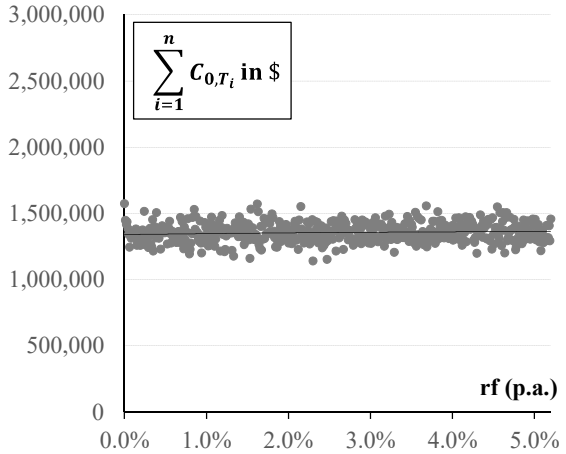


Figure II.3-7b: Risk-free interest rate r_f

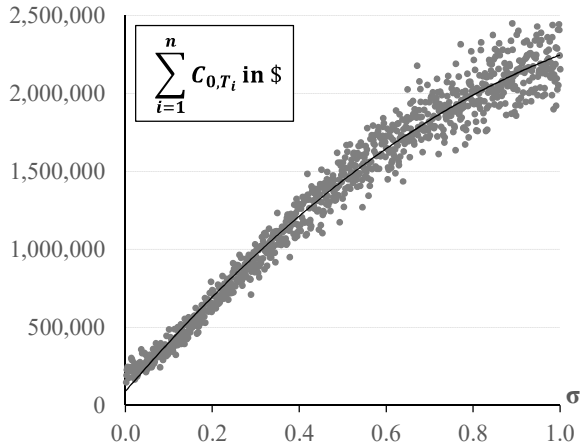


Figure II.3-7c: Volatility σ

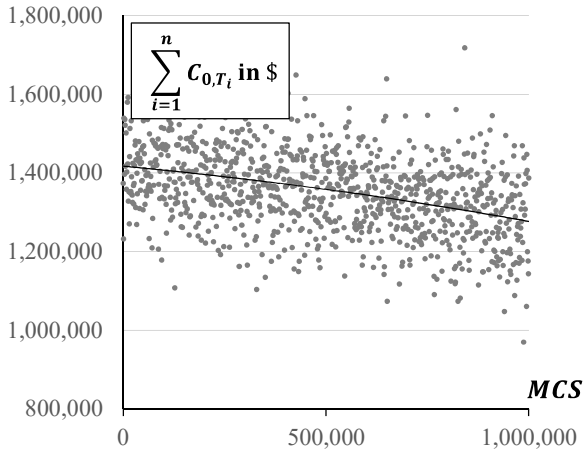


Figure II.3-7d: *Minimum contract size MCS*

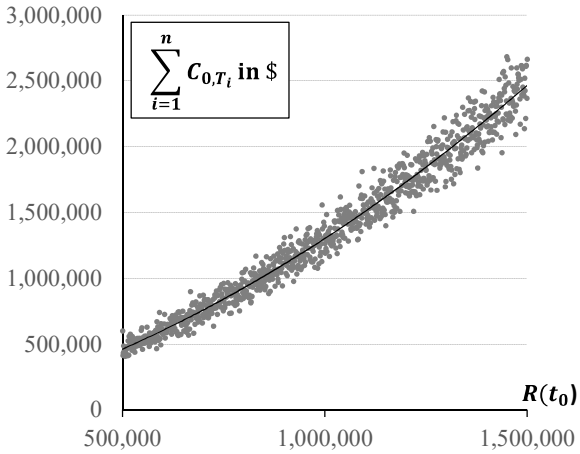


Figure II.3-7e: Initial month's customer revenue $R(t_0)$

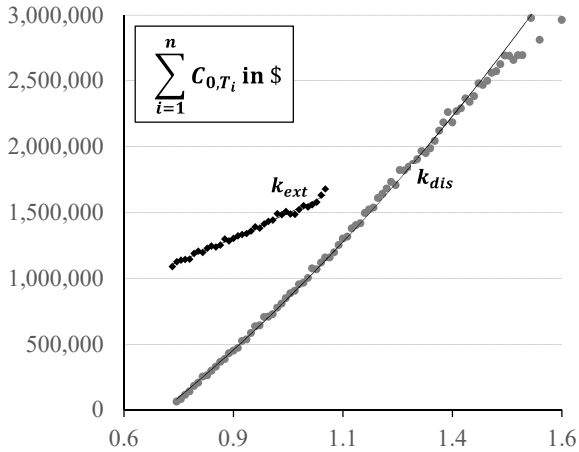


Figure II.3-7f: External production costs k_{ext} and costs for dissatisfied customers k_{dis}

Figure II.3-7: Sensitivity Analyses

The sensitivity analyzes we conducted regarding the "Greeks" reveal the following insights about the robustness of our model:

- First, Theta (Figure II.3-7a) illustrates that the expansion option values increase with

longer contract terms T_n. Longer contract terms are synonymous with larger numbers of expansion options, all of which possess a value greater than or equal to zero.

- Second, Rho (Figure II.3-7b) illustrates that the expansion option values slightly increase with a greater risk-free interest rate r_f. A greater risk-free interest rate increases the company's monetary advantage in that it does not have to pay for additional production capacity until the expiration dates of the expansion options.
- Third, Vega (Figure II.3-7c) illustrates that the expansion option values increase along with the volatility of the company's total periodical revenue σ. Without on-demand production capacity, a greater volatility in the company's total periodical revenue implies that there will be more dissatisfied customers, leading to corresponding costs of k_{dis}, or idle costs in case of unused capacity. A framework contract with the ECP, however, allows the company the flexibility to react to uncertainties in the development of demand.

We conducted statistical two-sample t-tests which confirm this observation (significance levels: 0.1% for Theta and Vega and 5% for Rho). All three observations are in line with common option pricing theory for European call options (Hull and White 1987).

The sensitivity analysis of expansion option values to minimum contract size MCS (Figure II.3-7d)) illustrates that expansion option values decrease for greater MCS. A greater MCS increases fixed costs for the exercise of expansion options and, therefore, decreases their values. We conducted another statistical two-sample t-test which confirms this observation (significance level: 0.1%). The sensitivity analysis of the expansion option values to the initial month's customer revenue $R(t_0)$ illustrates that expansion option values increase with greater $R(t_0)$ (significance level: 0.1%). As a greater $R(t_0)$ also indicates greater values of the total periodical revenue in future, the probability of a decrease in total production costs as a result of the use of on-demand production capacity is also increasing (remember, internal production capacity is assumed to be constant). In addition, a sensitivity analysis of expansion option values to k_{ext} and k_{dis} illustrates that expansion option values increase for greater k_{ext} and k_{dis} (significance levels: 0.1% for both factors). For k_{dis}, this observation is intuitive. Without the ECP, a greater k_{dis} significantly increases costs due to dissatisfied customers, and the company may even incur costs exceeding the revenue of a single MTO product. Inversely, on-demand production capacity is an insurance against such costs and increases the value of expansion options. For k_{ext}, however, this observation may not seem intuitive, as greater costs

for outsourcing should not favor the value of on-demand production capacity. We attribute this observation to our parameter selection, as the draw of k_{dis} depends on k_{ext}. As k_{dis} exceeds k_{ext} based on a multiplicative factor greater than one, the (positive) effect of greater k_{dis} on the value of expansion options exceeds the (negative) effect of greater k_{ext} on expansion option values. This technical limitation of our simulation (that is, the interdependence of both factors) is necessary to guarantee $k_{dis} > k_{ext} > k_{int}$.

II.3.5 Implications

Our results enable us to draw insights relevant to both researchers and practitioners. For researchers, particularly those working in the field of investment decision theory, we provide a methodological contribution: Our approach illustrates how a decision-maker can (i) model an industrial company's use of the on-demand production capacity offered by an ECP, accounting for several expansion options; (ii) evaluate the corresponding volume flexibility; and (iii) evaluate the upfront investments which enable the use of flexible on-demand production capacity, taking into consideration the value of different expansion options. Our approach can be classed as formal, as we identify important requirements for the valid application of ROA (Ullrich 2013) and demonstrate that the sensitivity of our results to model parameters mirror findings from common option pricing theory ("Greeks").

For practitioners, our results demonstrate that the opportunity to seize on-demand production capacity can be of considerable value to industrial companies, especially when working with longer framework contracts. Therefore, companies should investigate whether additional volume flexibility is an appropriate means of reducing the adverse effects of volatile customer demand and production costs. According to our results, on-demand production capacity seems particularly promising for companies in fast-moving industries which exhibit rapidly changing customer preferences and, therefore, highly volatile customer demand (e.g., the consumer electronics industry). In addition, volume flexibility is particularly promising for companies with limited investment budgets, such as SMEs, and during periods of high interest rates, as companies can defer their investments in internal production capacity. Practitioners who are responsible for production capacity planning can use our ROA approach to evaluate volume flexibility and decide on necessary upfront investments within an ENPV approach. Moreover, they can use a respective business case for comparison with other business opportunities such as investments in the expansion of internal production capacity. Practitioners from ECPs can

use our approach for the parametrization of their business models, and for marketing and sales purposes to support potential customers in their business case evaluation.

II.3.6 Conclusion, Limitations, and Further Research

Shorter product life cycles due to technological progress and changing customer preferences, along with customers' desire for the instant availability of highly individualized products, yield increasingly volatile levels of customer demand, which complicate the production capacity planning of industrial companies. Aside from investments in new production facilities or customer order-controlling approaches such as revenue management, companies can make use of volume flexibility using the on-demand production capacity provided by ECPs. However, the dynamic integration of on-demand production capacity may require companies to make substantial upfront investments, which they must evaluate in an appropriate manner, i.e., in line with the principles of value-based management. In this paper, we present an ENPV approach that enables such an appropriate evaluation of necessary upfront investments, taking into account flexibility of action and demand uncertainty. In order to model flexible access to on-demand production capacity and demand uncertainty, we apply ROA using binomial tree evaluation of Cox et al. (1979). We evaluate our model using a simulation and sensitivity analyses, and conclude that, in approximately 95% of all simulation runs, the value of the expansion options, i.e., the value of volume flexibility, is positive.

However, our approach has some limitations which give rise to future research opportunities. For reasons of complexity reduction, we assume that the industrial company can take on an infinite level of on-demand production capacity. Moreover, we set internal and external production costs at a constant level over the planning horizon and do not account for changing costs due to macro-economic or market developments, or for further product life-cycle costs, which are also important to consider (Lukas et al. 2017). In applying formulae of Cox et al. (1979), we use a multiplicative (stochastic) binomial process of the company's total periodical revenue to describe uncertainty, which significantly influences the choice of internal and external production scheduling. However, this may not necessarily hold true in practice as the development of this stochastic variable may not exhibit normally distributed returns with a constant mean and volatility. Therefore, future research could, for example, apply fat tail distributions. Moreover, researching continuous-time approaches for ROA could enable continuous-time evaluation. Since the provision of on-demand production capacity represents

a new business model that lacks widespread in practice, our simulation parameters are not based on real-world data. Therefore, an appropriate next step would be to evaluate our model using a real-world example. By applying an ENPV method, we aim to evaluate investments in new technologies which enable volume flexibility using on-demand production capacity. Nevertheless, these investments could also lead to further benefits, such as improved process efficiency, which are not considered in our model. Consequently, there may be more benefits which could be considered in future research and integrated in a holistic evaluation model of investments in digital transformation. However, our current approach is a first step in this direction, and provides both researchers and practitioners with valuable insights which can be built upon in the future.

II.3.7 References

Abel, Andrew B., Avinash K. Dixit, Janice C. Eberly, and Robert S. Pindyck. 1996. Options, the Value of Capital, and Investment. *The Quarterly Journal of Economics*, 111 (3): 753–777.

Akşin, O. Zeynep, Francis de Véricourt, and Fikri Karaesmen. 2008. Call center outsourcing contract analysis and choice. *Management Science*, 54 (2): 354–368.

Alaniazar, Saman. 2013. Demand modeling and capacity planning for innovative short life-cycle products, Wayne State University Dissertations.

Amram, Martha and Nalin Kulatilaka. 1998. *Real options: Managing strategic investment in an uncertain world*. Boston, Mass.: Harvard Business School Press.

Benaroch, Michel and Robert J. Kauffman. 1999. A Case for Using Real Options Pricing Analysis to Evaluate Information Technology Project Investments. *Information Systems Research*, 10 (1): 70–86.

Benaroch, Michel, Qizhi Dai, and Robert J. Kauffman. 2010. Should we go our own way? Backsourcing flexibility in IT services contracts. *Journal of Management Information Systems*, 26 (4): 317–358.

Benaroch, Michel and Robert J. Kauffman. 2000. Justifying Electronic Banking Network Expansion Using Real Options Analysis. *MIS Quarterly*, 24 (2): 197–225.

Benavides, Dario L., James R. Duley, and Blake E. Johnson. 1999. As good as it gets: Optimal fab design and deployment. *IEEE Transactions on Semiconductor Manufacturing*, 12 (3): 281–287.

Black, Fischer, and Myron Scholes. 1973. The pricing of options and corporate liabilities. *Journal of political economy*, 81 (3): 637–654.

Boulaksil, Youssef and Jan C. Fransoo. 2010. Implications of outsourcing on operations planning: Findings from the pharmaceutical industry. *International Journal of Operations & Production Management*, 30 (10): 1059–1079.

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

Chase, Richard B., Nicholas J. Aquilano, and F. Robert Jacobs. 2004. *Operations management for competitive advantage*, 10th ed. Irwin/McGraw-Hill, Boston, MA.

Chen, Ruey-Shun, Kun-Yung Lu, Shien-Chiang Yu, Hong-Wei Tzeng, and C. C. Chang. 2003. A case study in the design of BTO/CTO shop floor control system. *Information & Management*, 41 (1): 25–37.

Copeland, Thomas E. and Vladimir Antikarov. 2003. *Real options: A practitioner's guide*. New York: Texere.

Copeland, Tom and Peter Tufano. 2004. A Real-World Way to Manage Real Options. *Harvard Business Review*, 82 (3): 90–99.

Cox, John C., Stephen A. Ross, and Mark Rubinstein. 1979. Option pricing: A simplified approach. *Journal of financial economics*, 7 (3): 229–263.

Dangl, Thomas. 1999. Investment and capacity choice under uncertain demand. *European Journal of Operational Research*, 117 (3): 415–428.

Dong, Lingxiu and Erik Durbin. 2005. Markets for surplus components with a strategic supplier. *Naval Research Logistics (NRL)*, 52 (8): 734–753.

Dorsch, Christoph and Björn Häckel. 2012. Matching Economic Efficiency and Environmental Sustainability: The Potential of Exchanging Excess Capacity in Cloud

Service Environments, Proceedings of the Thirty-Third International Conference on Information Systems. *ICIS, Orlando, Florida, USA*.

Dorsch, Christoph and Björn Häckel. 2014. Combining models of capacity supply to handle volatile demand: The economic impact of surplus capacity in cloud service environments. *Decision Support Systems*, 58: 3–14.

eMachineShop. 2017. The World's Longest Established Online Machine Shop. https://www.emachineshop.com/about-emachineshop/. Accessed 23 November 2017.

EMAG. 2017. ServicePlus Vermietung. http://www.emag.com/serviceplus/full-service/renting.html. Accessed 23 November 2017.

Fernandes, Rui, Borges Gouveia, and Carlos Pinho. 2012. Vertical integration moment in dynamic markets. *Strategic Outsourcing: An International Journal*, 5 (2): 121–144.

Fichman, Robert G., Mark Keil, and Amrit Tiwana. 2005. Beyond valuation:"Options thinking" in IT project management. *California Management Review*, 47 (2): 74–96.

Garrido, Fernando. 2012. This time it's personal: from consumer to co-creator. http://www.ey.com/Publication/vwLUAssets/This_time_its_personal/$FILE/AS%20Customer%20Barometer%20This%20Time%20Its%20Personal%20FINAL.pdf. Accessed 25 November 2017.

Gerhard, Detlef. 2017. Product Lifecycle Management Challenges of CPPS, eds. Stefan Biffl, Arndt Lüder, and Detlef Gerhard. In *Multi-Disciplinary Engineering for Cyber-Physical Production Systems: Data Models and Software Solutions for Handling Complex Engineering Projects*, 89–110. Cham: Springer International Publishing.

Haruvy, Ernan, Elena Katok, Zhongwen Ma, and Suresh Sethi. 2018. Relationship-specific investment and hold-up problems in supply chains: Theory and experiments. *Business Research*.

Hauschild, Bastian and Daniel Reimsbach. 2015. Modeling sequential R&D investments: A binomial compound option approach. *Business Research*, 8 (1): 39–59.

Hull, John and Alan White. 1987. The pricing of options on assets with stochastic volatilities. *The journal of finance*, 42 (2): 281–300.

Kagermann, Henning, Johannes Helbig, Ariane Hellinger, and Wolfgang Wahlster. 2013. *Recommendations for implementing the strategic initiative INDUSTRIE 4.0: Securing the*

future of German manufacturing industry; final report of the Industrie 4.0 Working Group: Forschungsunion.

Katzmarzik, Arne, Matthias Henneberger, and Hans Ulrich Buhl. 2012. Interdependencies between automation and sourcing of business processes. *Journal of Decision Systems*, 21 (4): 331–352.

Klaus, Carsten, Felix Krause, and Christian Ullrich. 2014. Determining the business value of volume flexibility for service providers-a real options approach. *Proceedings of the 22nd European Conference on Information Systems, ECIS, Tel Aviv, Israel, June 2014*.

Kleinert, Alexander and Volker Stich. 2010. Valuation of procurement flexibility in the machinery and equipment industry using the real option approach. In *Enterprise Architecture, Integration and Interoperability*, 21–31. Berlin, Heidelberg: Springer.

Kogut, Bruce and Nalin Kulatilaka. 1994. Options Thinking and Platform Investments: Investing in Opportunity. *California Management Review*, 36 (2): 52–71.

Kremic, Tibor, Oya Icmeli Tukel, and Walter O. Rom. 2006. Outsourcing decision support: A survey of benefits, risks, and decision factors. *Supply Chain Management: An International Journal*, 11 (6): 467–482.

Lankford, William M. and Faramarz Parsa. 1999. Outsourcing: A primer. *Management Decision*, 37 (4): 310–316.

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

Lee, In and Kyoochun Lee. 2015. The Internet of Things (IoT): Applications, investments, and challenges for enterprises. *Business Horizons*, 58 (4): 431–440.

Lier, Stefan, Dominik Wörsdörfer, and Marcus Grünewald. 2012. Real Options for Economic Assessments of Innovation Projects in Chemical Production. *Chemie Ingenieur Technik*, 84 (12): 2164–2173.

Luehrman, Timothy A. 1998. Investment opportunities as real options: Getting started on the numbers. *Harvard Business Review*, 76 (4): 51–67.

Lukas, Elmar, Spengler, Thomas Stefan, Kupfer, Stefan, and Kieckhäfer, Karsten. 2017. When and how much to invest? Investment and capacity choice under product life cycle uncertainty. *European Journal of Operational Research*, 260 (3): 1105–1114.

Mason, Scott P. and Robert C. Merton. 1985. The role of contingent claims analysis in corporate finance, eds. Edward I. Altman and Marti G. Subrahmanyam. In *Recent Advances in Corporate Finance*. Homewood, IL: Richard D. Irwin.

Matt, Dominik T., Erwin Rauch, and Patrick Dallasega. 2015. Trends towards Distributed Manufacturing Systems and Modern Forms for their Design. *Procedia CIRP*, 33: 185–190.

Merton, Robert C. 1973. Theory of rational option pricing. *Theory of Valuation*, 229-288.

Monostori, László. 2014. Cyber-physical Production Systems: Roots, Expectations and R&D Challenges. *Procedia CIRP*, 17: 9–13.

Mosig, Tim, Leontin Grafmüller, and Claudia Lehmann. 2017. Business Model Patterns of B2B Mass Customizers: The Case of German Textile SMEs. *International Journal of Industrial Engineering and Management*, 8 (3): 99–110.

Mukherji, Sandip. 2011. The capital asset pricing model's risk-free rate. *The International Journal of Business and Finance Research*, 5 (2): 75-83.

Myers, Stewart C. 1977. Determinants of corporate borrowing. *Journal of financial economics*, 5 (2): 147–175.

Myers, Stewart C. 1984. Finance Theory and Financial Strategy. *Interfaces*, 14 (1): 126–137.

Olhager, Jan and Björn Östlund. 1990. An integrated push-pull manufacturing strategy. *European Journal of Operational Research*, 45 (2-3): 135–142.

Panayi, Sylvia and Lenos Trigeorgis. 1998. Multi-stage real options: The cases of information technology infrastructure and international bank expansion. *The Quarterly Review of Economics and Finance*, 38 (3): 675–692.

Penas, Olivia, Régis Plateaux, Stanislao Patalano, and Moncef Hammadi. 2017. Multi-scale approach from mechatronic to Cyber-Physical Systems for the design of manufacturing systems. *Computers in Industry*, 86: 52–69.

Rauschecker, Ursula, Daniel Stock, Matthias Stöhr, and Alexander Verl. 2014. Connecting factories and related IT environments to manufacturing clouds. *International Journal of Manufacturing Research*, 9 (4): 389–407.

Ren, Lei, Lin Zhang, Lihui Wang, Fei Tao, and Xudong Chai. 2017. Cloud manufacturing: Key characteristics and applications. *International Journal of Computer Integrated Manufacturing*, 30 (6): 501–515.

Schwartz, Eduardo S. and Lenos Trigeorgis. 2004. Real options and investment under uncertainty: An Overview, eds. Eduardo S. Schwartz and Lenos Trigeorgis. In *Real options and investment under uncertainty: Classical readings and recent contributions*, 1–18: MIT Press.

Spath, Dieter, Oliver Ganschar, Stefan Gerlach, Moritz Hämmerle, Tobias Krause, and Sebastian Schlund. 2013. *Produktionsarbeit der Zukunft-Industrie 4.0*: Fraunhofer Verlag Stuttgart.

Spinler, Stefan, Arnd Huchzermeier, and Paul R. Kleindorfer. 2002. An options approach to enhance economic efficiency in a dyadic supply chain. *Cost management in supply chains*, 349-360. Physica, Heidelberg.

Spinler, Stefan, Arnd Huchzermeier, and Paul R. Kleindorfer. 2003. Risk hedging via options contracts for physical delivery. *Or Spectrum*, 25 (3): 379–395.

Tomlin, Brian. 2006. On the value of mitigation and contingency strategies for managing supply chain disruption risks. *Management Science*, 52 (5): 639–657.

Trigeorgis, Lenos. 1993. The nature of option interactions and the valuation of investments with multiple real options. *Journal of Financial and quantitative Analysis*, 28 (1): 1–20.

Trigeorgis, Lenos. 1996. *Real options: Managerial flexibility and strategy in resource allocation*. Cambridge, Mass.: MIT Press.

Tsai, Wen-Hsien and Chien-Wen Lai. 2007. Outsourcing or capacity expansions: Application of activity-based costing model on joint products decisions. *Computers & Operations Research*, 34 (12): 3666–3681.

U.S. Department of the Treasury. 2017. Daily Treasury Yiel Curve Rates. https://www.treasury.gov/resource-center/data-chart-center/interest-rates/Pages/TextView.aspx?data=yield. Accessed 22 November 2017.

Ullrich, Christian. 2013. Valuation of IT Investments Using Real Options Theory. *Business & Information Systems Engineering*, 5 (5): 331–341.

Vyatkin, Valeriy, Zoran Salcic, Partha Roop, and John Fitzgerald. 2007. Now That's Smart! *IEEE Industrial Electronics Magazine*, 1 (4): 17–29.

Wang, Shiyong, Jiafu Wan, Di Li, and Chunhua Zhang. 2016. Implementing Smart Factory of Industrie 4.0: An Outlook. *International Journal of Distributed Sensor Networks*, 12 (1): 3159805.

Wickramasinghe, G. L.D. and Asanka Perera. 2016. Effect of total productive maintenance practices on manufacturing performance: Investigation of textile and apparel manufacturing firms. *Journal of Manufacturing Technology Management*, 27 (5): 713–729.

Wu, Dong. J., Paul R. Kleindorfer, and Jin E. Zhang. 2001. Integrating contracting and spot procurement with capacity options. *INTACH 1996 CISDEM--Community Information Services on Development and Environment Matters*.

Wu, Dong J., Paul R. Kleindorfer, and Jin E. Zhang. 2002. Optimal bidding and contracting strategies for capital-intensive goods. *European Journal of Operational Research*, 137 (3): 657–676.

Wu, Dazhong, Matthew J. Greer, David W. Rosen, and Dirk Schaefer. 2013. Cloud manufacturing: Drivers, current status, and future trends, Proceedings of the ASME 2013 international manufacturing science and engineering conference. *MSEC 13, Madison, Wisconsin, USA*.

Wu, Feng, H. Z. Li, Lap K. Chu, Domenic Sculli, and Kun Gao. 2009. An approach to the valuation and decision of ERP investment projects based on real options. *Annals of Operations Research*, 168 (1): 181–203.

Xometry. 2017. One-Stop Shop for Manufacturing on Demand. https://www.xometry.com/. Accessed 23 November 2017.

Xu, Xun. 2012. From cloud computing to cloud manufacturing. *Robotics and Computer-Integrated Manufacturing*, 28 (1): 75–86.

III Risk Management in Digitized Value Networks

This chapter focuses on risk management in digitized value networks. Due to the increasing importance of information systems for the reliability of physical production infrastructures, information-based risks present a major challenge for risk management. Thereby, especially the increasing interconnection of value chain partners, digitized production infrastructures, products, and production components lead to highly complex information-based dependency structures. On the one hand, these increase the vulnerability of digitized value networks as formerly isolated systems exhibit various entry points and single point failures can spread within the entire network without physical connections. On the other hand, the complex dependency structures complicate risk management in digitized value networks. Regarding these challenges for risk management in digitized value networks, research paper P1 and P2 present approaches for the modeling and simulation of digitized value networks and the analysis of inherent IT availability risks, and research paper P3 proposes a generic architecture for a strategic decision support system for systemic risk management. Thus, this chapter includes the following three research papers:

The first research paper P4 *"Modeling IT Availability Risks in Smart Factories – A Stochastic Petri Nets Approach*" (Section III.1) introduces a modeling approach for complex smart factory information networks based on petri nets enabling the simulation and analysis of IT availability risks. Thereby, different threat scenarios, complex informational dependency structures, and cascading failures are considered.

The second research paper P5 "*Assessing IT Availability Risks in Smart Factory Networks*" (Section III.2) introduces a risk assessment model for IT availability risks in smart factory networks that models interdependencies between the information network and the production network. Further, it provides an approach for the quantification of IT availability risks providing an economic basis for investment decisions in targeted IT security measures.

The third research paper P6 "*Toward Strategic Decision Support Systems for Systemic Risk Management*" (Section III.3) proposes a functional design and a generic architecture for a strategic decision support system for systemic risk management. Further, to support the implementation of such a system, areas for future research and selected research questions are presented.

III.1 Research Paper 4: "Modeling IT Availability Risks in Smart Factories – A Stochastic Petri Nets Approach"[5]

Authors:	Daniel Miehle[a,b], Björn Häckel[c,f], Stefan Pfosser[d], Jochen Übelhör[e,f] a BMW Group, Munich, Germany [b] Technical University of Munich, Germany daniel.miehle@tum.de [c] University of Applied Sciences Augsburg, Germany bjoern.haeckel@hs-augsburg.de [d] BMK electronics, Augsburg, Germany stefan.pfosser@bmk-group.de [e] Research Center Finance & Information Management, Department of Information Systems Engineering & Financial Management (Prof. Dr. Hans Ulrich Buhl), University of Augsburg jochen.uebelhoer@fim-rc.de [f] Project Group Business & Information Systems Engineering of the Fraunhofer FIT, Augsburg, Germany
In:	Business & Information Systems Engineering, 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*

[5] This is a post-peer-review, pre-copyedit version of an article published in Business & Information Systems Engineering. The final authenticated version is available online at: http://dx.doi.org/10.1007/s12599-019-00610-6

on generalized stochastic Petri nets, this 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.

III.1.1 Introduction

A recent worldwide survey by PricewaterhouseCoopers (PwC) among 2,000 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 hours in the US in 2008

(Washington Post 2008) and a technical defect of a single hard disk resulted in a server shutdown for 19 hours 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 percent 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 section 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 section 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 section 6, we discuss the results and limitations of our research and provide an outlook on future research.

III.1.2 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.

III.1.2.1 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.) 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).

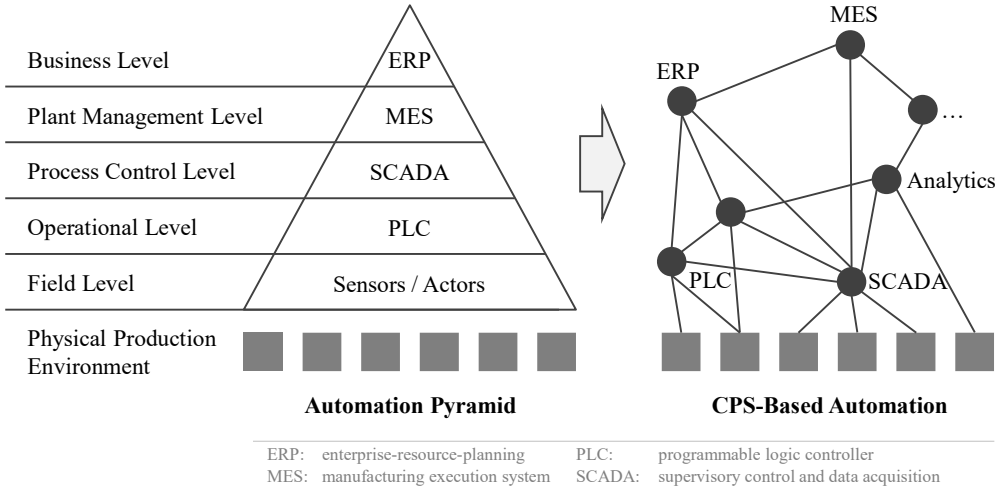


Figure III.1-1: Vertical Integration – Decomposition of automation hierarchy – Own Illustration based on VDI 2013

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. Figure III.1-1). 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 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 Figure III.1-2.

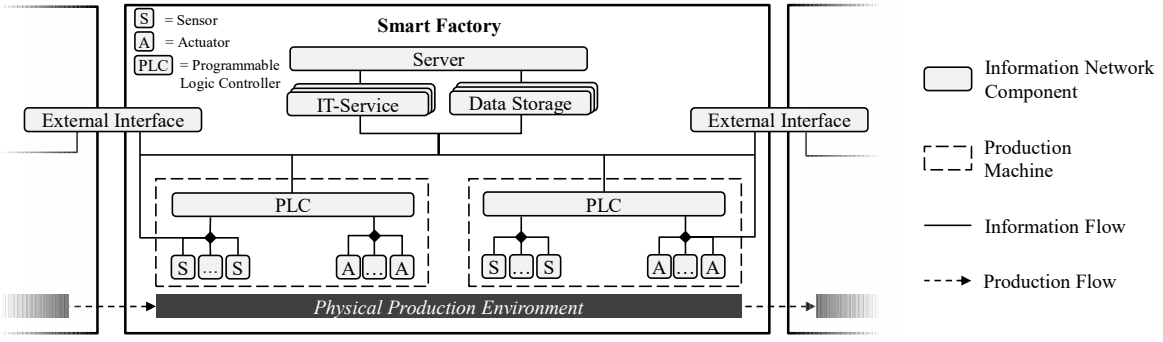


Figure III.1-2: Basic structure of a smart factory – Own Illustration based on Lucke et al. (2008) and Yoon et al. (2012)

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 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.*

III.1.2.2 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 Figure III.1-3, *threats* in smart factories include both intentional *attacks* and unintentional *errors* (Amin et al. 2013).

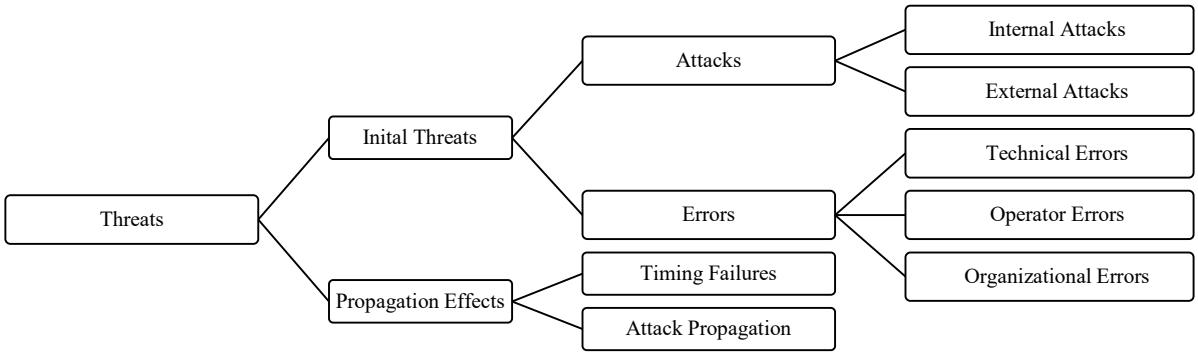


Figure III.1-3: Classification of threats in smart factories – Own Illustration

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 Figure III.1-4.

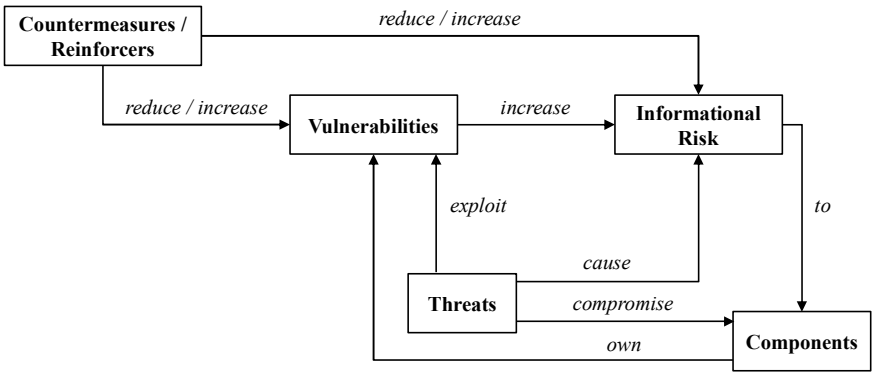


Figure III.1-4: Availability Risk Relations in Smart Factories – Own Illustration based on Common Criteria (2006) and Keller and König (2014)

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 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 one minute 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 III.1-1, 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.

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

Table III.1-1: Component States

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.*

III.1.2.3 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 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 III.1-1).*

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.

III.1.2.4 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.; 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.

III.1.3 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 section 1 by highlighting the relevance of formalized modeling approaches for the depiction and simulation of information networks in smart factories. In section 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. section 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.

III.1.3.1 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 (1988).

To describe the information network by means of our modeling approach in a formalized way, there is a finite set of places $P = \bigcup_{i=1}^{m}\{p_i\} = \{p_1, \dots, p_m\}$[6]. Further, there is a finite set of transitions $T = \bigcup_{j=1}^{n}\{t_j\} = \{t_1, \dots, t_n\}$, 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 1:

[6] Table 4 in the appendix provides an overview of the nomenclature of our PN specification.

$$\boldsymbol{A = O - I} \quad \textbf{(1)}$$

The marking vector $M^h = [M^h(p_1); \dots; M^h(p_m)]$, contains for each point in time h with $h \in \{0, \dots, H\}$ 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 $CR = [cr_1; \dots; cr_m]$ 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 $CP = [cp_1; \dots; cp_n]$ assigns each transition t_j a specific priority or probability, respectively. Further, the guard function vector $G^h = [g^h(t_1); \dots; g^h(t_n)]$ 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 $E^h = [e^h(t_1); \dots; e^h(t_n)]$ 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 $TT = [tt_1; \dots; tt_n]$ determines whether a transition is an immediate ($tt_j = 0$) or timed ($tt_j = 1$) transtion. Further, the fire rate vector $FR = [fr_1; \dots; fr_n]$ 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 $F^h = [f^h(t_1); \dots; f^h(t_n)]$ 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 equation 2:

$$\boldsymbol{M^{h+1} = M^h + A \cdot F^h} \quad \textbf{(2)}$$

As the information network is composed of several components, we define a set of components $C = \bigcup_{k=1}^{o}\{c_k\} = \{c_1, \dots, c_o\}$. For example, and in reference to Figure 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 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 $L_{k,\hat{k}} \in \mathbb{N}$.

III.1.4 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 Figure III.1-5.

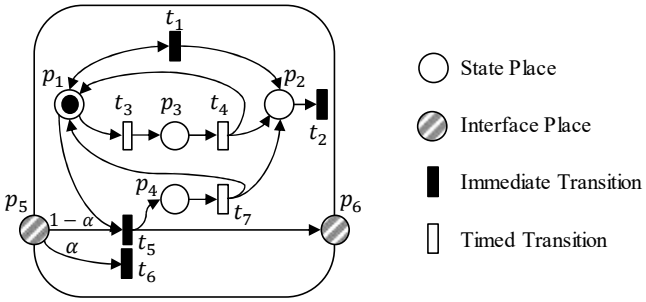


Figure III.1-5: Modeling of an information network component

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 III.1-6 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.

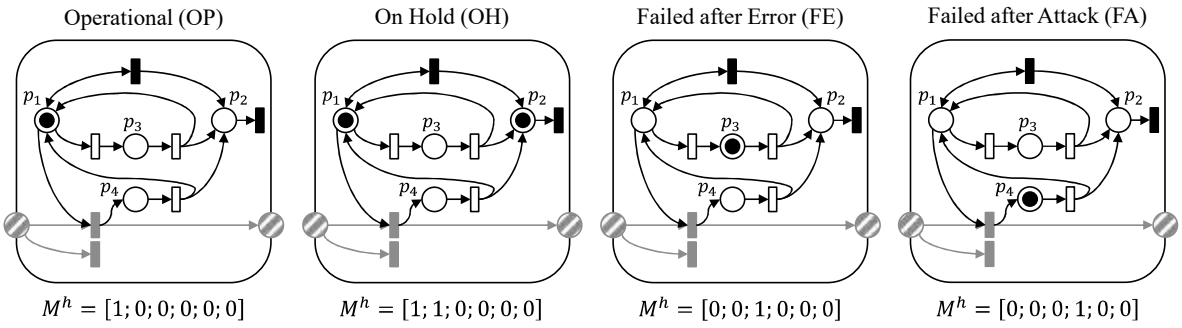


Figure III.1-6: Component states depicted in the model

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 time. Figure III.1-5, 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. Figure III.1-7).

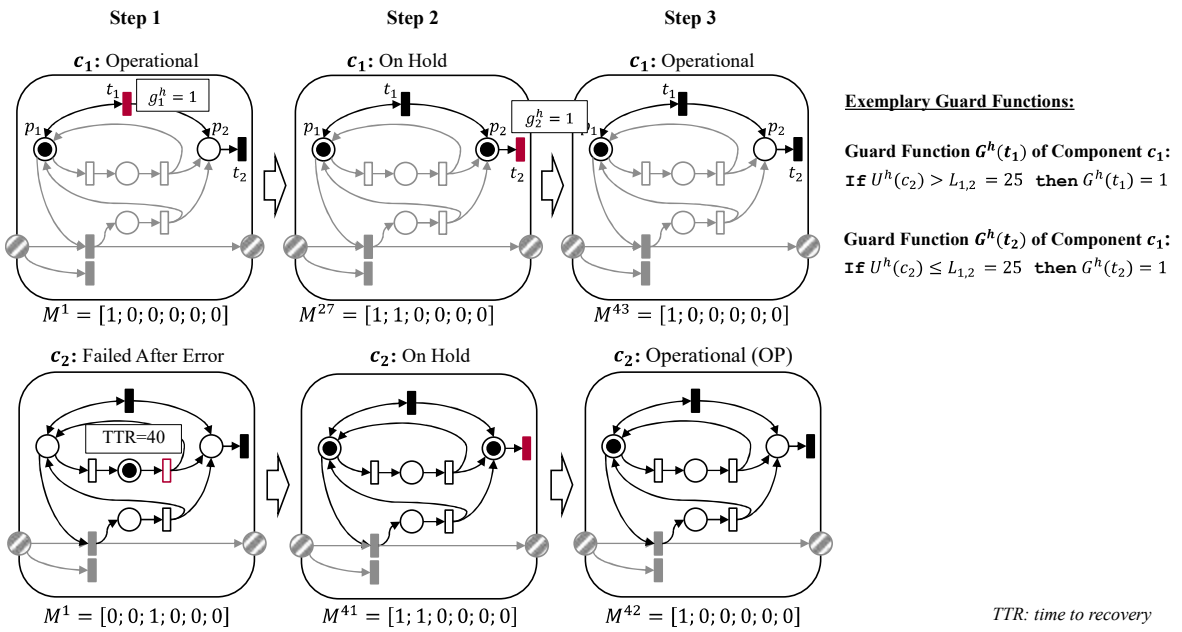


Figure III.1-7: Timing failure sequence

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 *operational, failed after error*, and *on hold* as shown in Figure III.1-8.

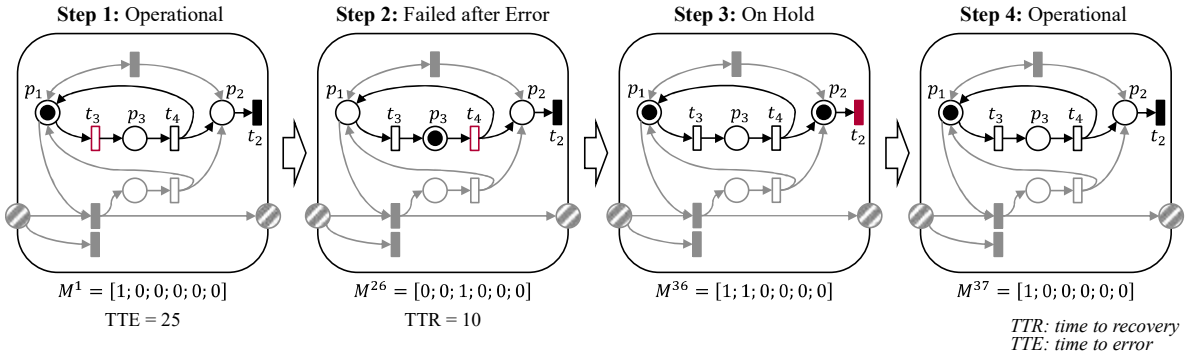


Figure III.1-8: Error sequence

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 Figure III.1-9.

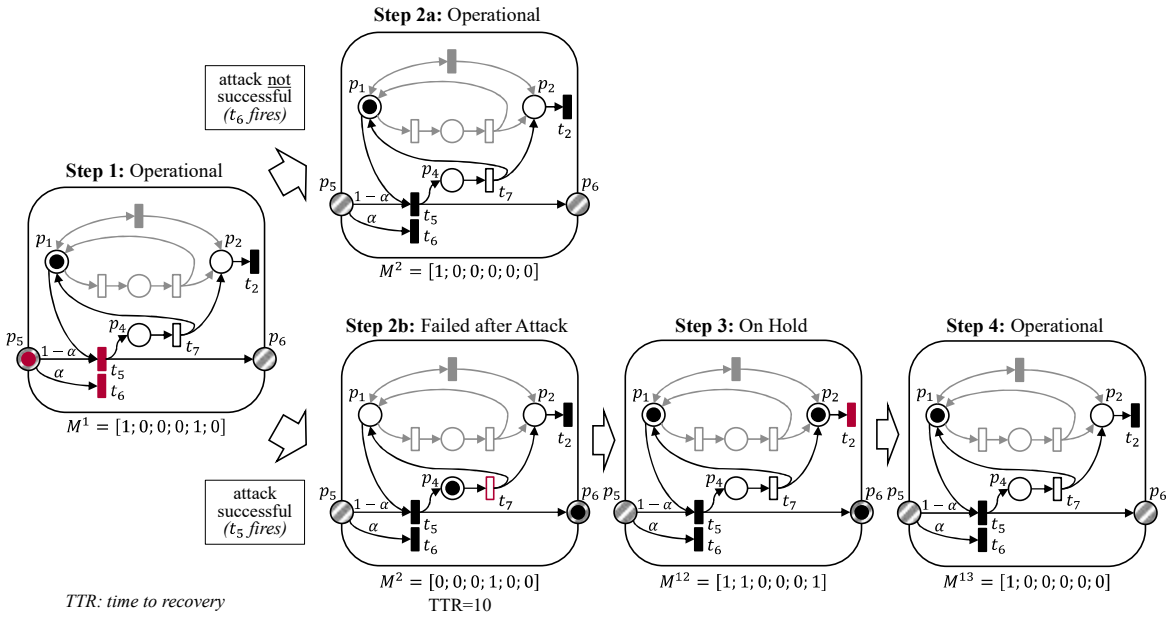
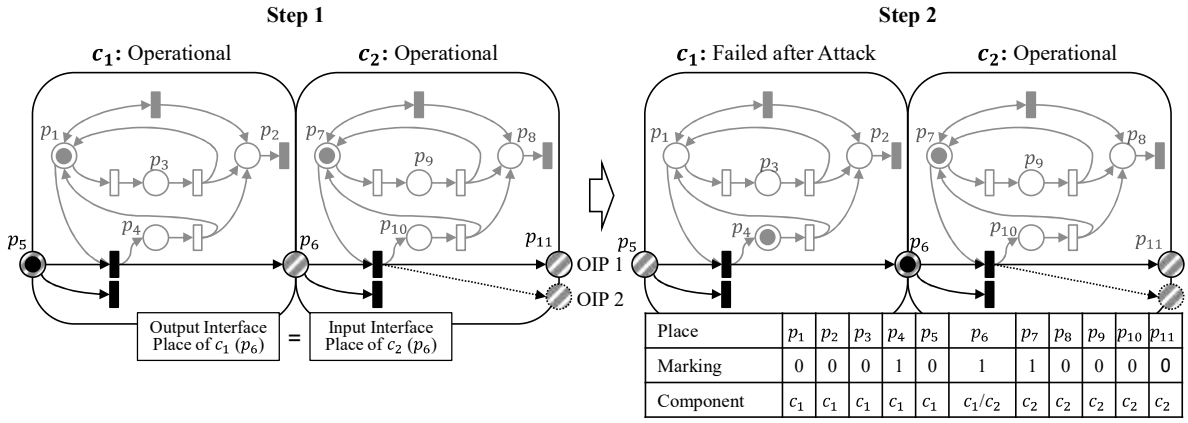


Figure III.1-9: Attack sequence

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).



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

Figure III.1-10: Attack propagation sequence

As shown in Figure III.1-10 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. Figure 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 Figure 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 depict simultaneous attacks (Amin et al. 2013) the number of OIPs within the shock module can be expanded analogously to the modeling module (cf. Figure III.1-11).

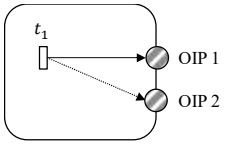


Figure III.1-11: Structure of a shock module

III.1.5 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 sections 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 section 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 section 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 section 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. section 5.4).

III.1.5.1 Feature Comparison

In section 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).

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. section 4).

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

III.1.5.2 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. Figure III.1-12) 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.

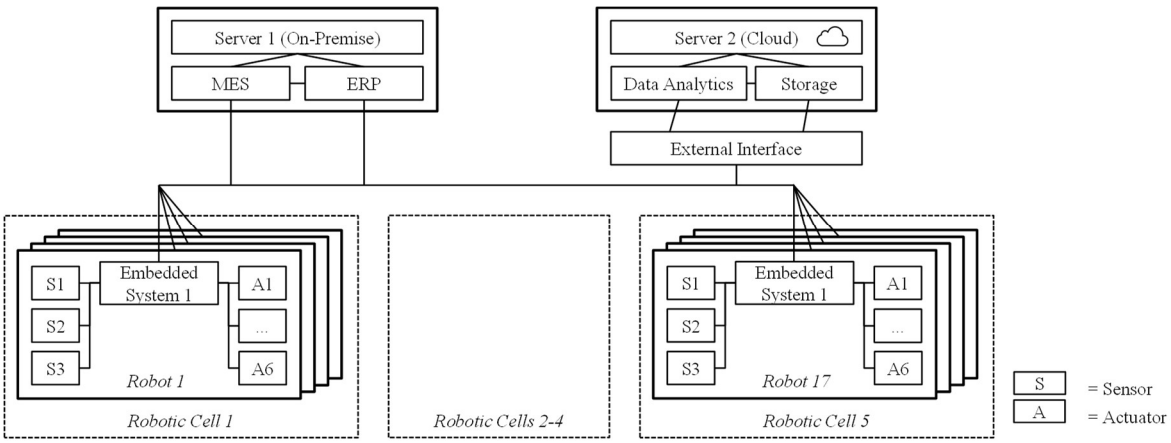


Figure III.1-12: Exemplary smart factory information network

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 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 III.1-2).

	Scenario 1 – Attack		**Scenario 2 – Error**	
	Case 1A	Case 1B	Case 2A	Case 2B
Number of Simulation Runs	1,000			
Number of Points in Time	100			
Number of Components	211			
Error Rate (L_E)	0.0001	0.0001	0.0001	0.0001
Error Recovery Rate (L_ER)	0.01	0.01	0.01	0.1
Security Level α	0.90	0.99	0.90	0.90

Table III.1-2: Scenario specifications

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 1,000 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 cell 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 Figure III.1-13). 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. 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 Figure III.1-13). 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.

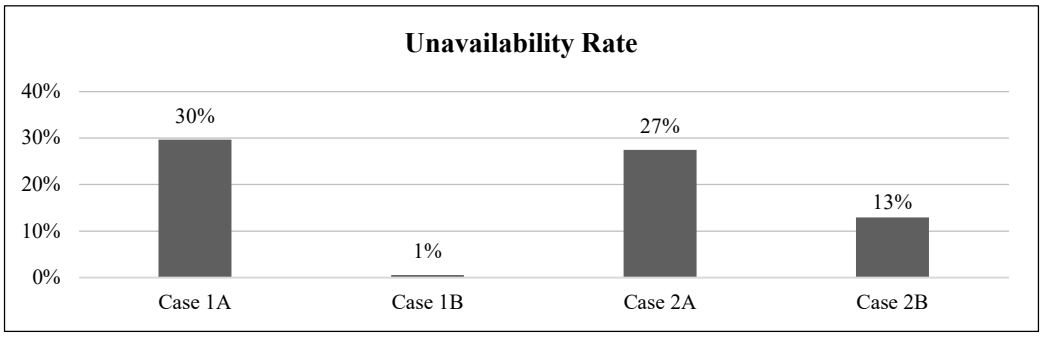


Figure III.1-13: Simulation results: Unavailability rates for Scenario 1 – Attack and Scenario 2 – Error

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. section 5.3).

III.1.5.3 Application of Key Figures

Besides the simulation results described in section 5.2, the data regarding the components' states and their operational capability (ref. Table III.1-1) 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 III.1-3 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 $v^b_{c_k,h}$	$v^b_{c_k,h} = [1; 0; 0; 0]$	$v^b_{c_k,h} = [0; 1; 0; 0]$	$v^b_{c_k,h} = [0; 0; 1; 0]$	$v^b_{c_k,h} = [0; 0; 0; 1]$

Table III.1-3: Component states and corresponding state vectors

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* $AV_h(\widehat{M}, \hat{h})$ *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*[7] *at* $\hat{h}$ *due to an attack or error (see eq. 3).*

Dynamic key figure "Operational availability": *The operational availability of the information network* $opAV_h(\widehat{M}, \hat{h})$ *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* $\hat{h}$ *due to an attack or error (see eq. 4).*

$$AV_h(\widehat{M}, \hat{h}) = \frac{\sum_{c=1}^{C} b^{OP}_{c_k,h} + \sum_{c=1}^{C} b^{OH}_{c_k,h}}{C} \quad (3) \qquad opAV_h(\widehat{M}, \hat{h}) = \frac{\sum_{c=1}^{C} b^{OP}_{c_k,h}}{C} \quad (4)$$

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 $s \in$

[7] $\widehat{M}$ 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.

$\{OP, OH\}$, 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 analyzed 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 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, Figure III.1-14 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.

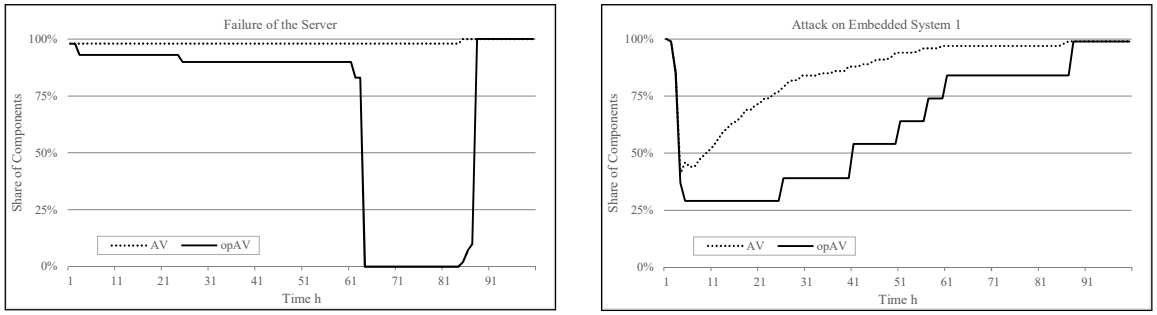


Figure III.1-14: Illustration of AV and opAV after failure (a) and attack (b) for an exemplary simulation run

As shown in Figure III.1-14a, 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 Figure III.1-14a), embedded systems, and all dependent sensors and actuators (drop 3 and 4 in Figure III.1-14a) 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 Figure III.1-14b, 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.

III.1.5.4 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 section 5.2 and the application of key figures in section 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 section 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 section 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 focusses 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.

III.1.6 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 section 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.

III.1.7 Appendix

Parameter	Description
P	Set of places $P = \bigcup_{i=1}^{m}\{p_i\} = \{p_1, \dots, p_m\}$
T	Set of transitions $T = \bigcup_{j=1}^{n}\{t_j\} = \{t_1, \dots, t_n\}$
C	Set of components $C = \bigcup_{k=1}^{o}\{c_k\} = \{c_1, \dots, c_o\}$
I	Input matrix I with $I_{i,j} \in \{0,1\}$
O	Output matrix O with $O_{i,j} \in \{0,1\}$
A	Incidence matrix A with $A_{i,j} \in \{-1,0,1\}$
CR	Conflict resolution vector $CR_i = [cr_1; \dots; cr_m]$
CP	Conflict parameter vector $CP_j = [cp_1; \dots; cp_n]$
TT	Transition type vector $TT_j = [tt_1; \dots; tt_n]$
FR	Fire rate vector $FR_j = [fr_1; \dots; fr_n]$
L	Maximum acceptable interruption time matrix L with $L_{k,\hat{k}} \in \mathbb{N}$
h	Discrete point in time h with $h \in \{0, 1, \dots, H\}$
M^h	Marking vector $M^h = [M^h(p_1); \dots; M^h(p_m)]$ with $M^h(p_i) \in \{0,1\}$
E^h	Enabling vector $E^h = [e^h(t_1); \dots; e^h(t_n)]$ with $e^h(t_j) \in \{0,1\}$
F^h	Firing vector $F^h = [f^h(t_1); \dots; f^h(t_n)]$ with $f^h(t_j) \in \{0,1\}$
G^h	Guard function $G^h = [g^h(t_1); \dots; g^h(t_n)]$ with $g^h(t_j) \in \{true, false\}$
U^h	Unavailability vector $U^h = [u^h(c_1); \dots; u^h(c_o)]$ with $u^h(c_k) \in \mathbb{N}_0$

Table III.1-4: Nomenclature of PN specification

III.1.8 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 April 2017.

Albert, Réka; Jeong, Hawoong; Barabasi, Albert-László (2000): Error and Attack Tolerance of Complex Networks. In: *Nature* 406 (6794), pp. 378–382. DOI: 10.1038/35019019.

Amin, Saurabh; Schwartz, Galina A.; Hussain, Alefiya (2013): In Quest of Benchmarking Security Risks to Cyber-Physical Systems. In: *IEEE Network* 27 (1), pp. 19–24. DOI: 10.1109/MNET.2013.6423187.

Amiri, Amin K.; Cavusoglu, Hasan; Benbasat, Izak (2014): When is IT Unavailability a Strategic Risk?: A Study in the Context of Cloud Computing. In: *Proceedings of the 35th International Conference on Information Systems, Auckland, New Zealand*, pp. 1–11.

Arns, Markus; Fischer, Markus; Kemper, Peter; Tepper, Carsten (2002): Supply Chain Modelling and its Analytical Evaluation. In: *Journal of the Operational Research Society* 53 (8), pp. 885–894. DOI: 10.1057/palgrave.jors.2601381.

Arshad, Naveed; Heimbigner, Dennis; Wolf, Alexander L. (2006): Dealing with failures during failure recovery of distributed systems. In: *Computer Science Technical Reports* (943), pp. 1–12. DOI: 10.1145/1082983.1083067.

Ash, Jeff; Newth, David (2007): Optimizing Complex Networks for Resilience Against Cascading Failure. In: *Physica A: Statistical Mechanics and its Applications* (380), S. 673–683. DOI: 10.1016/j.physa.2006.12.058.

Brettel, Malte; Friederichsen, Niklas; Keller, Michael; Rosenberg, Marius (2014): How Virtualization, Decentralization and Network Building Change the Manufacturing Landscape: An Industry 4.0 Perspective. In: *World Academy of Science: Engineering and Technology International Journal of Mechanical, Aerospace, Industrial, Mechatronic and Manufacturing Engineering* 8 (1), pp. 37–44.

Broy, Manfred; Cengarle, María Victoria; Geisberger, Eva (2012): Cyber-Physical Systems: Imminent Challenges. In: *David Hutchison, Takeo Kanade, Josef Kittler, Jon M. Kleinberg, Friedemann Mattern, John C. Mitchell et al. (eds.): Large-Scale Complex IT Systems. Development, Operation and Management, Bd. 7539*. Springer Berlin Heidelberg (Lecture Notes in Computer Science), 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 on 17 April 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 on 17 April 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=3https://www.bsi.bund.de/SharedDocs/Downloads/ACS/cyber-sicherheits-umfrage_2017.pdf?__blob=publicationFile&v=3, Accessed on 2 June 2018

Buhl, Hans Ulrich; Penzel, Hans-Gert (2010): The Chance and Risk of Global Interdependent Networks. In: *Business & Information Systems Engineering* 2 (6), pp. 333–336. DOI: 10.1007/s12599-010-0131-7.

Buldyrev, Sergey V.; Parshani, Roni; Paul, Gerald; Stanley, H. Eugene; Havlin, Shlomo (2010): Catastrophic Cascade of Failures in Interdependent Networks. In: *Nature* 464 (7291), pp. 1025–1028. DOI: 10.1038/nature08932.

Cardenas, Alvaro; Amin, Saurabh; Sinopoli, Bruno; Giani, Annarita; Perrig, Adrian; Sastry, Shankar (2009): Challenges for Securing Cyber Physical Systems. In: *Workshop on Future Directions in Cyber-Physical Systems Security*, pp. 1–4.

Colombo, Armando Walter; Karnouskos, Stamatis (2009): Towards the Factory of the Future: A Service-oriented Cross-layer Infrastructure. In: *ICT shaping the world: a scientific view* (65), pp. 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 on 17 April 2017.

Danziger, Michael M.; Shekhtman, Louis M.; Bashan, Amir; Berezin, Yehiel; Havlin, Shlomo (2016): Vulnerability of Interdependent Networks and Networks of Networks. In: *Antonios Garas (ed.): Interconnected Networks*. Cham: Springer International Publishing (Understanding Complex Systems), pp. 79–99.

Eden, Peter; Blyth, Andrew; Jones, Kevin; Soulsby, Hugh; Burnap, Pete; Cherdantseva, Yulia; Stoddart, Kristan (2017): SCADA System Forensic Analysis Within IIoT, In: *L. Thomas and D. Schaefer (eds.): Cybersecurity for Industry 4.0 - Analysis for Design and Manufacturing*. Springer, Cham, pp. 73-101.

Fridgen, Gilbert; Stepanek, Christian; Wolf, Thomas (2014): Investigation of Exogenous Shocks in Complex Supply Networks – A Modular Petri Net Approach. In: *International Journal of Production Research* 53 (5), pp. 1387–1408. DOI: 10.1080/00207543.2014.942009.

Gao, Jianxi; Buldyrev, Sergey V.; Stanley, H. Eugene; Havlin, Shlomo (2012): Networks Formed from Interdependent Networks. In: *Nature Physics* 8 (1), pp. 40–48. DOI: 10.1038/NPHYS2180.

Gregor, Shirley; Hevner, Alan R. (2013): Positioning and Presenting Design Science Research for Maximum Impact. In: *Management Information Systems Quarterly* 37 (2), pp. 337–355.

Hallikas, Jukka; Karvonen, Iris; Pulkkinen, Urho; Virolainen, Veli-Matti; Tuominen, Markku (2004): Risk Management Process in Supplier Networks. In: *International Journal of Production Economics* 90, pp. 47–58.

Hao, Kecheng; Xie, Fei (2009): Componentizing Hardware/Software Interface Design. In: *Conference on Design, Automation and Test in Europe, Dresden, Germany*, pp. 232–237.

Hermann, Mario; Pentek, Tobias; Otto, Boris. 2015. "Design Principles for Industrie 4.0 Scenarios - A Literature Review." *Technische Universität Dortmund - Working Paper 01/2015*.

Hevner, Alan R.; March, Salvatore T.; Park, Jinsoo; Ram, Sudha (2004): Design Science in Information Systems Research. In: *Management Information Systems Quarterly* 28 (1), pp. 75–106.

Jensen, Kurt (1991): Coloured Petri Nets: A High Level Language for System Design and Analysis. *In: G. Goos, J. Hartmanis, D. Barstow, W. Brauer, P. Brinch Hansen, D. Gries et al. (eds.): Advances in Petri Nets 1990*. Springer Berlin Heidelberg (Lecture Notes in Computer Science), pp. 342–416.

Kaplan, Stanley; Garrick, B. John (1981): On The Quantitative Definition of Risk. In: *Risk Analysis* 1 (1), pp. 11–27. DOI: 10.1111/j.1539-6924.1981.tb01350.x.

Keller, Robert; König, Christian (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, Heiner; Fettke, Peter; Kemper, Hans-Georg; Feld, Thomas; Hoffmann, Michael (2014): Industry 4.0. In: *Business & Information Systems Engineering* 6 (4), pp. 261–264. DOI: 10.1007/s12599-014-0334-4.

Lee, Jay; Bagheri, Behrad; Kao, Hung-An (2015): A Cyber-Physical Systems Architecture for Industry 4.0-based Manufacturing Systems. In: *Manufacturing Letters* 3, pp. 18–23. DOI: 10.1016/j.mfglet.2014.12.001.

Lucke, Dominik; Constantinescu, Carmen; Westkämper, Engelbert (2008): Smart Factory - A Step towards the Next Generation of Manufacturing. In: *The 41st CIRP Conference on Manufacturing Systems*.

Marsan, Marsan; Balbo, Gianni; Conte, Gianfranco (1984): A Class of Generalized Stochastic Petri Nets for the Performance Evaluation of Multiprocessor Systems. In: *ACM Transactions on Computer* 2 (2), pp. 93–122.

Merlin, Philip (1974): A Study of the Recoverability of Computer System. In: *PhD thesis, University of California, Irvine*.

Mertens, Peter; Barbian, Dina (2015): Grand Challenges – Wesen und Abgrenzungen. In: *Informatik Spektrum* 38 (4), pp. 264–268. DOI: 10.1007/s00287-015-0897-6.

Molloy, Michael Karl (1981): On the Integration of Delay and Throughput Measures in Distributed Processing Models. In: *PhD thesis, University of California, Los Angeles*.

Monostori, László (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. DOI: 10.1016/j.procir.2014.03.115.

Murata, Tadao (1989): Petri Nets - Properties, Analysis and Applications. In: *Proceedings of the IEEE* 77 (4).

Faisal, Mohd Nishat; Banwet, D. K.; Shankar, Ravi (2007): Information Risks Management in Supply Chains. An Assessment and Mitigation Framework. In: *Journal of Enterprise Information Management* 20 (6), pp. 677–699. DOI: 10.1108/17410390710830727.

Offermann, Philipp; Blom, Sören; Schönherr, Marten; Bub, Udo (2010): Artifact Types in Information Systems Design Science – A Literature Review. In: *David Hutchison, Takeo Kanade, Josef Kittler, Jon M. Kleinberg, Friedemann Mattern, John C. Mitchell et al. (eds.): Global Perspectives on Design Science Research*, Springer Berlin Heidelberg (Lecture Notes in Computer Science), pp. 77–92.

Peffers, Ken; Tuunanen, Tuure; Rothenberger, Marcus A.; Chatterjee, Samir (2007): A Design Science Research Methodology for Information Systems Research. In: *Journal of Management Information Systems* 24 (3), pp. 45–78. DOI: 10.2753/MIS0742-1222240302.

Petri, Carl Adam (1966): Communication with Automata. *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 February 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 on 17 April 2017.

Radziwon, Agnieszka; Bilberg, Arne; Bogers, Marcel; Madsen, Erik Skov (2014): The Smart Factory. Exploring Adaptive and Flexible Manufacturing Solutions. In: *Procedia Engineering* 69, pp. 1184–1190. DOI: 10.1016/j.proeng.2014.03.108.

Ramchandani, Chander (1974): Analysis of Asynchronos Concurrent Systems by Timed Petri Nets. In: *PhD Thesis, Massachusetts Institute of Technology*.

Sadeghi, Ahmad-Reza; Wachsmann, Christian; Waidner, Michael: Security and Privacy Challenges in Industrial Internet of Things. In: *Design Automation Conference*, pp. 1–6.

Sathanur, Arun V.; Haglin, David J. (2016): A Novel Centrality Measure for Network-wide Cyber Vulnerability Assessment. In: *IEEE Symposium on Technologies for Homeland Security*, pp. 1–5.

Schuh, Günther; Potente, Till; Wesch-Potente, Cathrin; Weber, Anja Ruth; Prote, Jan-Philipp (2014): Collaboration Mechanisms to Increase Productivity in the Context of Industrie 4.0. In: *Procedia CIRP* 19, pp. 51–56. DOI: 10.1016/j.procir.2014.05.016.

Simon, Herbert Alexander (1996): The Sciences of the Artificial: MIT Press.

Smith, Grafton Elliot; Watson, Kevin J.; Baker, Wade H.; Pokorski II, Jay A. (2007): A Critical Balance. Collaboration and Security in the IT-enabled Supply Chain. In: *International Journal of Production Research* 45 (11), pp. 2595–2613. DOI: 10.1080/00207540601020544.

Sonnenberg, Christian; Vom Brocke, Jan (2012): Evaluation Patterns for Design Science Research Artefacts. In: *Markus Helfert and Brian Donnellan (eds.): Practical Aspects of Design Science*, Springer Berlin Heidelberg (Communications in Computer and Information Science), pp. 71–83.

Sridhar, Siddharth; Hahn, Adam; Govindarasu, Manimaran (2012): Cyber–Physical System Security for the Electric Power Grid. In: *Proceedings of the IEEE* 100(1), pp. 210–224. DOI: 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 on 17 April 2017.

Tupa, Jiri; Simota, Jan; and Steiner, Frantisek (2017): Aspects of risk management implementation for Industry 4.0, in *Procedia Manufacturing* (11), pp. 1223 – 1230.

van der Aalst, W. M. P. (1998): The Application of Petri Nets to Workflow Management. In: *Journal of Circuits, Systems and Computers* 8 (01), pp. 21–66. DOI: 10.1142/S0218126698000043.

Venable, John; Pries-Heje, Jan; Baskerville, Richard (2012): A Comprehensive Framework for Evaluation in Design Science Research. *In: David Hutchison, Takeo Kanade, Josef Kittler, Jon M. Kleinberg, Friedemann Mattern, John C. Mitchell et al. (eds.): Design Science Research in Information Systems. Advances in Theory and Practice*, Springer Berlin Heidelberg (Lecture Notes in Computer Science), pp. 423–438.

Vladimir, A. Bashkin (2011): On the Modularity in Petri Nets of Active Resources. In: *Proceedings of CompoNet and SUMo*, pp. 33–48.

Wagner, Stephan M.; Neshat, Nikrouz (2010): Assessing the Vulnerability of Supply Chains Using Graph Theory. In: *International Journal of Production Economics* 126 (1), pp. 121–129. DOI: 10.1016/j.ijpe.2009.10.007.

Wan, Jiafu; Yan, Hehua; Liu, Qiang; Zhou, Keliang; Lu, Rongshuang; Di Li (2013): Enabling Cyber-Physical Systems with Machine-to-Machine Technologies. In: *International Journal of Ad Hoc and Ubiquitous Computing* 13 (3/4), pp. 187–196. DOI: 10.1504/IJAHUC.2013.055454.

Wang, Shiyong; Wan, Jiafu; Li, Di; Zhang, Chunhua (2016): Implementing Smart Factory of Industrie 4.0: An Outlook. In: *International Journal of Distributed Sensor Networks*, pp. 1–10.

Washington Post (2008): Cyber Incident Blamed for Nuclear Power Plant Shutdown. Unter Mitarbeit von Brian Krebs. http://www.washingtonpost.com/wp-dyn/content/article/2008/06/05/AR2008060501958.html. Accessed on 17 April 2017.

Weill, Peter; Vitale, Michael (2002): What IT infrastructure capabilities are needed to implement e-business models?. In: *Management Information Systems Quarterly* 1(1), pp. 17-34.

Wengert, Andre; Graham, James; Ribble, Eli (2016): A New Approach to Cyberphysical Security in Industry 4.0, in *L. Thomas and D. Schaefer (eds.): Cybersecurity for Industry 4.0 - Analysis for Design and Manufacturing*. Springer, Cham, pp. 59-72.

Wu, Teresa; Blackhurst, Jennifer; O'grady, Peter (2007): Methodology for Supply Chain Disruption Analysis. In: *International Journal of Production Research* 45 (7), pp. 1665–1682. DOI: 10.1080/00207540500362138.

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

Yoon, Joo-Sung; Shin, Seung-Jun; Suh, Suk-Hwan (2012): A Conceptual Framework for the Ubiquitous Factory. In: *International Journal of Production Research* 50 (8), pp. 2174–2189. DOI: 10.1080/00207543.2011.562563.

Zambon, Emmanuele; Etalle, Sandro; Wieringa, Roel J.; and Hartel, Pieter (2011): Model-based Qualitative Risk Assessment for Availability of IT Infrastructures. In: *Software & Systems Modeling* 10 (4), pp. 553–580.

Zuehlke, Detlef (2010): Smart Factory—Towards a Factory-of-Things. In: *Annual Reviews in Control* 34 (1), pp. 129–138. DOI: 10.1016/j.arcontrol.2010.02.008.

III.2 Research Paper 5: "Assessing IT Availability Risks in Smart Factory Networks"[8]

Authors:	Björn Häckel[a,e], Florian Hänsch[b], Michael Hertel[c], Jochen Übelhör[d,e] [a] University of Applied Sciences Augsburg, Germany bjoern.haeckel@hs-augsburg.de [b] Finalix Business Consulting, Zurich, Suisse florian.haensch@finalix.ch [c] BMW Financial Services, Munich, Germany michael.hertel@bmw.de [d] Research Center Finance & Information Management, Department of Information Systems Engineering & Financial Management (Prof. Dr. Hans Ulrich Buhl), University of Augsburg jochen.uebelhoer@fim-rc.de [e] Project Group Business & Information Systems Engineering of the Fraunhofer FIT, Augsburg, Germany

In:	Business Research, 2019, 12 (2), pp. 523-558

Abstract: *Emerging smart manufacturing technologies combine physical production networks with digital IT systems, resulting in complex smart factory networks, which are especially vulnerable to IT security risks, such as IT component non-availabilities. Companies must employ extensive IT security measures to secure their production facilities. However, complex network structures and inherent dependencies of smart factory networks complicate corresponding investment decisions and increase the need for appropriate decision support. We develop a risk assessment model that supports companies in the investment decision making process regarding IT security measures by identifying and evaluating the most critical areas of the information network while considering the underlying production network. For*

[8] This is a post-peer-review version of an article published in Business Research. The final authenticated version is available online at: https://doi.org/10.1007/s40685-018-0071-5

this purpose, IT availability risks are quantified by means of graph theory, matrix notation, and Value-at-Risk. Our model provides a structured approach, and considers network structures and interdependencies. The insights gained by our model present a profound economic basis for investment decisions on IT security measures. By applying our model in an exemplary real world setting, we analyze various IT security measures and their risk reduction effect.

III.2.1 Introduction

Technological trends, such as the *Internet of Things* (IoT), *cyber-physical systems* (CPS), and other smart manufacturing technologies turn conventional production facilities into so-called *smart factories* (Lasi et al. 2014). There, CPS enable machinery and products to control and monitor production processes collaboratively, and to optimize themselves and the production processes (Yoon et al. 2012, Schuh et al. 2014, Hessman 2013). Suppliers, customers, and vendors are increasingly integrated into the production infrastructure, resulting in IT-dependent, intercompany *smart factory networks*, with complex interdependencies. Thereby, the connection of physical production and digital information enables the flexible production of individualized goods, while simultaneously increasing efficiency (Radziwon et al. 2014). Besides manifold potential benefits, a number of new risks arise in smart factory networks. For instance, the digital transformation of production facilities bears considerable investment risks considering the substantial investment volumes that are often required. At the same time, technological risks arise due to the fast development cycles of digital technologies. Given the coordinative role of humans in complex production processes, the importance of humans as a possible source of error for operational risks but also as an object to be protected in the context of safety is also increasing (Hertel 2015). This is accompanied by the increasing complexity of the overall socio-economic system of the smart factory network, which increases the criticality of random and negligent errors and disturbances (Tupa et al. 2017, Geisberger and Broy 2015). Besides these general risks, especially IT security risks are of central importance as smart factory networks rely on communication and real-time information synchronization and, thus, depend on the underlying IT systems, which are mandatory for the reliable operation of the production infrastructure (Zuehlke 2010, Yoon et al. 2012, Tupa et al. 2017). Therefore, smart factory networks are concurrently increasingly vulnerable to IT security risks as they are no longer isolated and closed systems (Yoon et al. 2012, Smith et al. 2007, Tupa et al. 2017). Besides other dimensions of IT security risks

including access, accuracy, or accountability, this involves especially IT availability risks. These are becoming one of the most critical threats for companies, as non-availabilities of IT systems significantly hamper the reliable operation of dependent production components, and eventually cause their complete failure (Amiri et al. 2014). Although many companies are extensively engaged in digital transformation, the associated risks are often underestimated or not considered. However, this is of utmost importance as the consequences of IT availability risks in form of business interruptions might lead to considerable damage potentials. These damage potentials are increased by just-in-time and just-in-sequence production principles and ultimately result in severe monetary losses. This especially holds true for highly integrated, interdependent supply networks in which the failure of one company can cause interruptions in the entire supply network. Accordingly, companies must assign considerable investment volumes to IT security measures to secure their production facilities against IT availability risks and to prevent economic harm. However, the variety of potential measures, the increasing complexity of smart factory networks, and especially the inherent dependency structures significantly complicate the identification of the most critical areas of IT systems with regard to potential threat scenarios. Thus, companies require well-founded approaches that support a comprehensive assessment of IT availability risks and, based on that, enable well thought out investment decisions regarding IT security measures in the course of their IT security strategy.

Due to the outlined complex interdependencies in smart factory networks, a corresponding risk assessment model for IT availability risks must consider – besides specific characteristics of smart factory networks – that non-availability of IT systems interrupts the operation of the dependent production infrastructure (Lee 2008, Lucke et al. 2008, Zuehlke 2010). Additionally, increasing interconnectedness contributes to this increased vulnerability as local failures causing non-availabilities of IT systems can lead to disruptions in the entire value network (Amin et al. 2013, Hallikas et al. 2004). Local failures include, amongst others, simple technical failures, incorrect capacity planning, human errors, natural disasters, or intentional attacks on IT systems. For example, targeted denial-of-service attacks can cause a non-availability of IT components, affecting the functionality of the production network and reducing its productivity (Lucke et al. 2008, Zuehlke 2010, Amin et al. 2013). Numerous examples illustrate this threat potential. First, the German Federal Office for Information Security (abbreviated as BSI) mentions in its status report on information security that hackers

attacked a steel plant by intruding its office network. After advancing into the production control network and attacking the control components of the blast furnace, the blast furnace was left in an "undefined status" and could not be shut down in a controlled manner. As a result, the blast furnace and other parts of the plant were severely damaged (BSI 2014). This illustrates that due to ongoing interconnectedness, investments in IT security measures are of critical significance, even in traditional production facilities. Another example is the Stuxnet worm attack in 2010, which targeted industrial control systems in high-security infrastructures, such as atomic plants. The Stuxnet incident revealed that the interconnectedness of applications presents a serious security issue, and demonstrated that even the control system's disconnection from the Internet as well as personal access restrictions are insufficient as protection for industrial control systems (Karnouskos 2011). Considering these threat scenarios, companies must employ IT security measures to secure their CPS infrastructure against IT availability risks. Appropriate IT security measures include, but are not limited to, redundancies through backup components, industrial hardware with integrated IT security mechanisms, intrusion detection systems, or appropriate service-level agreements (Byres and Lowe 2004, Cardenas et al. 2008, Yadav and Dong 2014, Zambon et al. 2007).

Given the variety of potential IT security measures, in combination with limited personal and financial resources, the corresponding investment decisions regarding IT security measures must be based on a profound economic basis, considering costs, benefits, and risk aspects (Cavusoglu et al. 2004, Gordon et al. 2003, Huang 2010). For this, the most critical areas of a smart factory network's IT system must be identified and evaluated with a structured approach, to invest available funds in the most effective way (i.e., reducing IT availability risks to the best possible extent). Thereby, an analysis must consider the diverse, complex network structures and dependencies between the physical production world and the digital IT systems of the smart factory network. To support companies in their corresponding decision processes, we develop a structured approach for the identification and evaluation of a smart factory network's most critical areas regarding IT availability risks and formulate the following two research questions:

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

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

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

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

respective damage potentials, utilization of production components, and compensation effects influence the criticality of IT components and have to be considered.

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

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

III.2.2 Theoretical Background and Research Methodology

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

III.2.2.1 Smart Factory Networks and corresponding IT Availability Risks

Given the advancements of smart manufacturing technologies and the innovative nature of smart factory networks, scientific literature is constantly evolving and contains a diverse body of literature (e.g. see Haller et al. 2009, Iansiti and Lakhani 2014, Turber and Smiela 2014,

Strozzi et al. 2017). Further, there are numerous studies and application-oriented examples of research institutes exploring and describing the implementation of smart manufacturing technologies (e.g. see Hessman 2013, Lucke et al. 2008, Radziwon et al. 2014, Yoon et al. 2012, Zuehlke 2010, Shariatzadeh et al. 2016, Zhong et al. 2017). In corporate practice, we can observe that IoT-based technological solutions such as radio frequency identification (RFID) are widely implemented enabling, for example, the real-time acquisition of data and the real-time monitoring of objects within production processes (Lucke et al. 2008, Fleisch and Thiesse 2007, Zhong et al. 2017). However, the comprehensive and holistic implementation of smart manufacturing technologies in production facilities serving as test-beds remains object to laboratory research facilities, such as *SmartFactory*^{KL}, or pilot facilities, such as the *Siemens Electronic Works Facility* or the *WITTENSTEIN bastian' Production Facility* (Hessman 2013, Zuehlke 2010, Schlick et al. 2014). This was also found in a dynamic literature review performed by Strozzi et al. (2017). To structure the diverse body of literature on smart factories, they performed a combination of systemic literature review and bibliographic network analysis. Thereby, they revealed that the biggest literature stream focusses on RFID technology and agent-based intelligent decision support system architecture, both aspects concerning monitoring and scheduling of production processes. Further, they found that research focusses on "models, frameworks, and architectures related to the implementation of the Smart Factory […], along with high-level 'landscape' analyses." A recent example of such research is the work of Jung et al. (2017), in which a reference factory design and improvement activity model is introduced for designing new and improving existing factories. The model highlights interrelationships of implemented technologies and provides an indication for further improvements through sensors, software tools, or gathered data. Another finding of the study by Strozzi et al. (2017) is that research focuses more on topics related to the development and adoption of software tools and cloud applications instead of topics related to the adoption of new technologies in manufacturing processes. For instance, Shariatzadeh et al. (2016) develop an IoT platform-based system architecture and a generic framework for communication interfaces between the digital factory and the smart factory. Other researchers address the potential of the digital twin concept in regard to near-real time data acquisition and analysis (e.g. see Uhlemann et al. 2017, Borodulin et al. 2017, Qi and Fao 2018). In summary, it can be concluded that scientific contributions "propose conceptual works and experiments, and rarely actual test-beds and lessons learned from the practice are described and discussed" (Strozzi et al. 2017).

Another shortcoming of current literature is the lack of a common definition of the term *smart factory*, although widely used in both scientific literature and practice (Radziwon et al. 2014). Based on a collection of different definitions, Radziwon et al. (2014) define the smart factory as a "manufacturing solution that provides such flexible and adaptive production processes that will solve problems arising on a production facility […]." Hermann et al. (2015) define the smart factory as a "factory where CPS communicate over the IoT and assist people and machines in the execution of their tasks". They further describe, that "within the modular structured Smart Factories [...], CPS monitor physical processes, create a virtual copy of the physical world and make decentralized decisions". Based on *SmartFactory*^{KL} and adopting the idea of IoT, Zuehlke (2010) describes that a "factory-of-things will be composed of smart objects which interact based on semantic services". Yoon et al. (2012) describe a smart factory as a "factory system in which autonomous and sustainable production takes place". And Lucke et al. (2008) envision the smart factory as a "real-time, context-sensitive manufacturing environment that can handle turbulences in production using decentralized information and communication structures for an optimum of production processes."

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

The characteristics of smart factory networks are facilitated through concepts such as IoT and production-oriented CPSs, which involve *smart objects,* such as intelligent machinery and products. CPS integrate computing and communication capabilities in physical production

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

Due to the high level of interconnectedness between production and IT components, the operation of the physical production process depends on the flawless operation of IT services. Consequently, smart factory networks face new IT security threats that concern the four dimensions of IT security risks *availability*, *access*, *accuracy*, and *accountability* (Westerman and Hunter 2009). Thereby, the threats stem from four channels: (1) software bugs and hardware malfunctions, (2) open Internet protocols and shared networks, (3) the numerous parties involved, and (4) a large number of field devices that can be accessed (Amin et al. 2013). IoT and smart manufacturing technologies change requirements on IT security (Wegner et al. 2017) and "the concept of Industry 4.0 generates new categories of risks […] because of the increase of vulnerabilities and threats" (Tupa et al. 2017). Tupa et al. (2017) argue that "the connection of cyber-space, sophisticated manufacturing of technologies and elements, and using outsourcing of services [are] the main factors increasing vulnerability" and that "the implementation of Industry 4.0 has shown that the connections between humans, systems and objects have become a more complex, dynamic and real-time optimized network". For instance, central components of an IT infrastructure like an on-premise server

are no longer the only critical components of an information network. In fact, all components, including remote manufacturing equipment and internal and external sensors, become critical as "industrial control systems are becoming the target for malicious cyber intrusions" (Wegner et al. 2017). Further, SCADA systems, that control manufacturing processes, were initially designed to operate on closed networks. With IoT applications, SCADA systems are increasingly based on cloud technology resulting in increased interconnectivity and, ultimately, vulnerability (Eden et al. 2017). Therefore, "the challenge to maintain availability will increase as manufacturing evolves from a centralized system supported by external suppliers to a distributed system in which production occurs closer to the point of use" stretching potential points of failure (Wegner et al. 2017).

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

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

III.2.2.2 Approaches regarding the Assessment of IT Availability Risks

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

Based on a structured review of 125 risk assessment approaches for information systems, Shameli-Sendi et al. (2016) develop a taxonomy that structures risk assessment approaches along the four categories *appraisement*, *perspective*, *resource valuation*, and *risk measurement*. Thereby, *appraisement* differentiates risk assessment approaches from a

methodological perspective into *quantitative*, *qualitative*, and *hybrid* approaches (Shameli-Sendi et al. 2016). Quantitative methods deploy mathematical functions, objective measurements, and quantitative data to evaluate risk (Karabacak and Sogukpinar 2005, Suh and Han 2003, Sun et al. 2006). For example, the risk assessment framework developed by Jaisingh and Rees (2001) uses the quantitative risk measure VaR to assess IT security risks. The derived information can then be used to analyze the relationship between the cost of security measures and the risk reduction effects achieved. Niesen et al. (2016) develop a conceptual framework for data-driven risk assessment based on real-time operational data that becomes available in smart factory environments. By means of their approach, live monitoring of different types of risk becomes feasible. However, their approach does not allow the consideration of specific types of IT related threats, especially availability risks, as appropriate data and relevant indicators are missing. This shows that quantitative approaches often face a lack of necessary detailed data. Further, disadvantages include time-consuming and expensive calculation processes, the complex implementation in practice, and the difficult interpretation of results (Shameli-Sendi et al. 2016). In contrary, qualitative methods use descriptive variables to evaluate the likelihood of occurrence, and the impact of IT non-availability (Caralli et al. 2007, Aagedal et al. 2002). As they do not rely on accurate historical data and are much easier to understand and implement in contrast to quantitative methods, they are widely used in practice (Shameli-Sendi et al. 2016). For instance, Silva et al. (2014) develop a multi-dimensional risk management model based on Failure Mode and Effect Analysis (FMEA) and fuzzy theory that analyses five dimensions of information security risks: access to information and systems, communication security, infrastructure (hardware and networks), security management, and secure information systems development. Thereby, FMEA provides a structured approach for assessing failure modes according to three risk factors occurrence, severity, and detection that are assessed by expert estimations. The derived results provide information regarding the criticality of the investigated failures that produce vulnerabilities to the company's information system. Eom et al. (2007) develop a risk assessment approach for the evaluation of assets regarding their degree of contribution to related business processes. For this, they apply with Delphi teams a qualitative risk analysis methods. Besides the merits of qualitative approaches, shortfalls are that they often lack measurable detail and monetary results to support investment decision making considering cost-efficiency, and that results are often times subjective and prone to errors and imprecision (Shameli-Sendi et al. 2016). To overcome the weaknesses of sole quantitative or qualitative

approaches, there are hybrid methods combining both types to enable a simple and fast qualitative assessment as well as detailed quantitative analysis for more critical aspects (Yadav and Dong 2014, Rainer et al. 1991, Shameli-Sendi et al. 2016). For example, the initial quantitative risk assessment method developed by Zambon et al. (2007) considers the IT architecture and dependencies between IT constituents, based on a time-dependent model for business processes. Based on this, they extend their model to a qualitative model for the analysis of availability risks in IT architectures, requiring only commonly available input data (Zambon et al. 2011).

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

consider propagation effects, although these are essential to assess the entire damage potential caused by attacks and errors in complex network environments to provide a profound basis for economically sound investment decisions.

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

III.2.2.3 Research Approach and Applied Concepts

To answer the research questions raised in Section 1, under consideration of the requirements set forth in Section 2.1, we develop a structured approach for an appropriate assessment of IT availability risks in smart factory networks. This approach uses graph theory and matrix notation methods, as they are widely utilized methods for formalized representation and the analysis of complex and interdependent networks. For example, Wagner and Neshat (2010), Faisal et al. (2006), and Buldyrev et al. (2010) use graph theory and matrix notation to analyze risk in supply chains and critical infrastructures regarding vulnerability, risk mitigation, and cascading failures in interdependent networks. Graph theory enables a relatively simple and transparent application of our approach. These are two important characteristics, since our model represents a first approach that should be easy to use and should have a certain degree of scalability. Besides graph theory, there are other approaches for the formalized

representation of networks such as petri nets or system dynamics if other priorities are to be set. For example, if the analyses should be more detailed or more detailed stochastics (e.g., stochastic recovery times) should be used (e.g. Arns et al. 2002, Wu et al. 2007 or Fridgen et al. 2014). However, in our opinion, graph theory seems to be an appropriate method for a first attempt, especially for reasons of transparency and complexity reduction. Further, we apply the risk measure VaR for the quantification of IT availability risks, as it is a widely utilized risk measure for downside risks.

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

III.2.3 Risk Assessment Model

Our risk assessment model considers relevant smart factory characteristics, and identifies the most critical IT components of a smart factory's information network concerning IT availability risks by quantifying the corresponding threat potentials. In the following subsection, we describe the elementary steps of the model as shown in Figure III.2-1. The basic idea of our risk assessment model is to analyze the threat potential posed by the non-availability of an information network's IT component to the production network of a smart factory. This threat potential arises as the functionality and productivity of the production network depend on the reliable operation of the information network. In order to quantify the resulting threat potentials, we apply graph theory and matrix notation as well as VaR. The results gained by our model are of central importance to ensure a cost-efficient usage of

usually scarce IT budget and to support companies' investment decisions since available funds for IT security measures must be invested in the most efficient way. First, we present an abstraction of the smart factory's general setting, including its basic structures and relations (Section 3.1). Based on this abstraction, we then describe our risk quantification algorithm. At this, we model and formalize the smart factory structure by means of graph theory and matrix notation (Section 3.2). Subsequently, the threat potential of each IT component is quantified (Section 3.3).

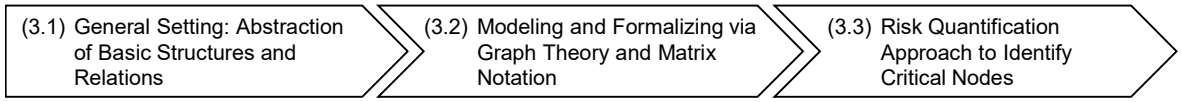


Figure III.2-1: Methodical Procedure of the Model Development – Own Illustration

III.2.3.1 General Setting

The basic structure of a smart factory consists of two connected networks: the production network and the information network, as illustrated in Figure III.2-2. First, there are different manufacturing machines in the production network performing various production procedures. These machines process products, and are organized in process steps, whereby a certain process step contains machines with identical capabilities. Manufacturing machines are equipped with *embedded systems*, which consist of electronic hardware (e.g., a microchip) and a software component. The embedded systems enable the manufacturing machines to control themselves autonomously, to a certain point, and to synchronize process information via the information network. Hence, we consider the embedded systems as parts of the *information network.* In addition to the embedded systems, the information network comprises further components performing various IT services crucial for the reliable operation of the smart factory. These IT services range from machine control and manufacturing execution, to enterprise level and machine communication applications. The different applications may be hosted on on-premise hardware or are obtained as cloud-based solutions. The respective IT infrastructure is also considered as an IT service.

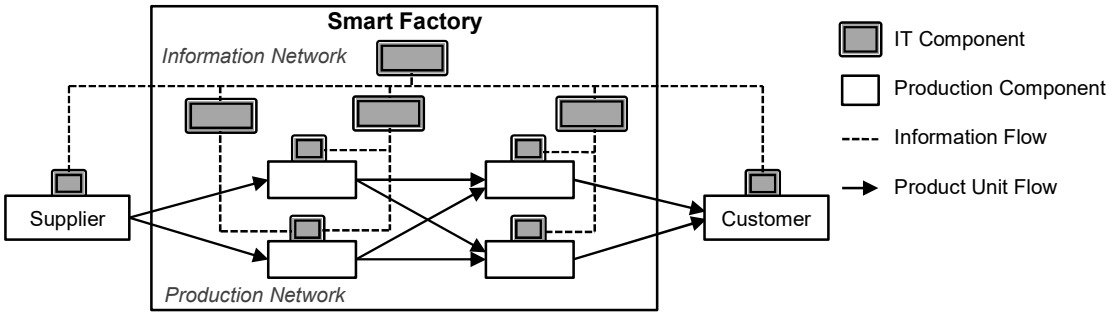


Figure III.2-2: Simplified Structure of the Smart Factory – Own Illustration

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

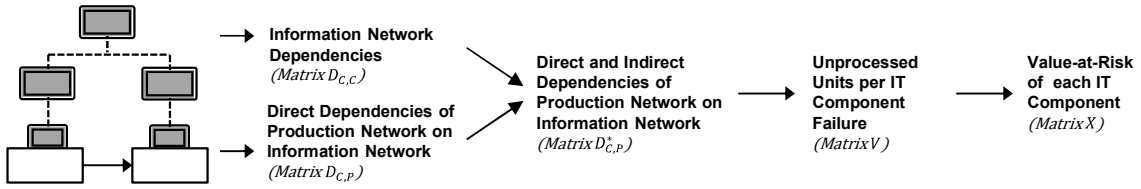


Figure III.2-3: Operational Steps of the Risk Assessment Algorithm – Own Illustration

In the following subsection, we outline the algorithm and its assumptions (see Figure III.2-3) in more detail. First, we formalize and model the basic structures of the smart factory and its networks by means of graph theory and matrix notation. The resulting smart factory dependency structure lays the groundwork for the risk quantification based on VaR, which will be discussed in the subsection afterwards.

III.2.3.2 Modeling of the Smart Factory

In the following, we describe, model, and formalize the smart factory's two connected and dependent networks. Thereby, we elaborate on the underlying assumptions regarding the basic structures and characteristics of both networks, their components, and their connections and dependencies.[9]

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

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

$$qi_i = q_i - qu_i \; with \; qu_i \leq q_i \tag{3}$$

[9] The reader might find it helpful to reference to Figure III.2-4 on page 167 while reading the following subsections to better comprehend the used notations.

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

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

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

$$D_{C,C} = \begin{bmatrix} d_{c_1,c_1} & \cdots & d_{c_1,c_k} \\ \vdots & \ddots & \vdots \\ d_{c_k,c_1} & \cdots & d_{c_k,c_k} \end{bmatrix} \tag{2}$$

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

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

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

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

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

First, we determine all direct and indirect functional dependencies within the information network by raising matrix $D_{C,C}$ to higher powers, according to the algorithm by Festinger, Perry, and Luce (Festinger 1949), and combining the resulting matrices in the binary matrix $\overline{D}_{C,C}$. Multiplying matrix $\overline{D}_{C,C}$ with the *direct functional dependency matrix* $D_{C,P}$ delivers all indirect functional dependencies of production components on IT components (matrix $\overline{D}_{C,P}$). Adding the matrices $D_{C,P}$ and $\overline{D}_{C,P}$ results in the *direct and indirect functional dependency matrix* $\overline{\overline{D}}_{C,P}$, containing both the *direct* and *indirect* functional dependencies of production components on IT components. We now adjust matrix $\overline{\overline{D}}_{C,P}$ for possible redundancies based on the number of IT components c_s available for the execution of an IT service s. In particular, if a production component depends on more than one IT component, the dependency is removed because the failure of a redundant IT component is backed up. First, we aggregate the available IT components of each IT service s in a binary matrix $Z_{S,C}$, and only the main IT components of each IT service s in matrix $\tilde{Z}_{S,C}$. Multiplying matrix $Z_{S,C}$ with matrix $\overline{\overline{D}}_{C,P}$ delivers matrix $\bar{Z}_{S,P}$, which represents the number of available IT components for each

production component in regard to an IT service s. Subsequently, all values of $\bar{Z}_{S,P}$, which do not equal one, are set to zero. This results in the binary matrix $\bar{\bar{Z}}_{S,P}$ with all production components depending only on one IT component in regard to an IT service s. Lastly, we multiply matrix $\bar{\bar{Z}}_{S,P}$ with the transposed main IT component matrix $\dot{Z}_{C,S}$ to derive the *dependency matrix* $D^*_{C,P}$, as defined by Eq. (4). The resulting *dependency matrix* $D^*_{C,P}$ defined by equation (4) contains all direct and indirect functional dependencies of production components on IT components, and considers redundancies in the information network. Thereby, the binary variable $d^*_{c_s,p_i} \in \{0; 1\}$ equals one if there is a direct or indirect functional dependency; otherwise, $d^*_{c_s,p_i}$ equals zero:

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

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

III.2.3.3 Risk Quantification Approach

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

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

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

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

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

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

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

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

The smart factory's ability to flexibly combine the production components in temporary production lines enables the compensation for initially unprocessed units v_{c_s,p_i}. However, the compensation is only possible if compensating production components possess the same production capabilities and, hence, belong to the same process step l as the affected production component. Further, compensating production components must have idle capacity left. The

compensable units w_{c_s,p_i} provided by a compensating production component are calculated as described by Eq. (7):

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

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

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

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

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

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

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

The losses caused by unprocessed units reflect the value added during the production process in the respective process steps. The losses are assigned proportionally to each process step according to the respective activities performed in each process step. Process step-specific loss values are necessary because different *impact locations* of IT component failures cause different effects in the production network. For example, a production failure in the first process step results in no processed units; in contrast, a production failure in an advanced

process step results in semi-finished units, which present a value because their time-to-market is shorter due to their advanced production state. The information about process step-specific loss values is available through accounting and performance measurement methods, such as activity-based costing, and hence, can be easily assessed and applied as exogenous input parameters to our model (Cooper and Kaplan 1991). Based thereupon, we apply the VaR to quantify the consequences of an IT component's non-availability in the considered time period. The VaR is a downside risk measure and a "standard benchmark" (Duffie and Pan 1997, p. 3) for the measurement of a company's exposure to financial risks, i.e., potential loss. For a given time period and probability (or confidence level) $(1-\alpha)$, the VaR is defined as the loss over the time period that is exceeded with probability α (Duffie and Pan 1997 and Jorion 2006). We apply the VaR in our model for risk quantification as loss values corresponding to an IT component's non-availability are not fixed and may vary due to market-induced interference factors and random effects, such as price and demand fluctuations. Therefore, we assume that losses are normally distributed with an expected loss value μ_l and a standard deviation σ_l per unprocessed unit u for each process step l, expressed in monetary units (in US$). The use of a normal distribution is justifiable because variations of the value added are driven by market parameters, causing both positive and negative deviations. However, other distributions, such as the lognormal distribution can be used, if the normal distribution is inappropriate in specific applications. The definition of a confidence level $(1-\alpha)$ takes into account the risk attitude. In most cases, no sufficient historical data basis exists to derive loss values and standard deviations solely by means of statistical analyses. Therefore, the loss extends, and probabilities must be estimated by experts (Hovav and D'Arcy 2003, Gordon and Loeb 2002, Mercuri 2003). Additionally, the excessive amounts of production-related data could be used to support these expert estimations (Lucke et al. 2008). With this information, the VaR of each IT component c_s for each process step l, denoted as $x_{c_s,l}$, can be derived by Eq. (10), with $N_{(1-\alpha)}$ being the $(1-\alpha)$ quantile of the normal distribution:

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

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

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

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

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

III.2.4 Exemplary Application

In the following section, we demonstrate the applicability of our risk assessment model in an exemplary smart factory that is oriented on a real world scenario of producing customized sports shoes. Afterwards, we conduct sensitivity analyses regarding the capacity utilization and the impact of varying loss potential estimations to evaluate the basic effects of two major influencing factors. Finally, we analyze the risk reduction effects of different IT security measures by comparing the model's results based on the *with-and-without-principle* to demonstrate the model's application in an investment decision process. We refrain from comparing our model and its results with other risk assessment methods for reasons of evaluation, as we doubt the value of such a comparison due to the lack of comparable methods. Although there are other methods for the assessment of information risks such as the discussed FMEA model by Silva et al. (2014) or the model by Zambon et al. (2007), none of them incorporates the specific characteristics of smart factory networks, such as network structures or network interdependencies. However, this would be necessary for a meaningful and conclusive comparison with our model. Instead, we believe further evaluation of our model

in concrete real world scenarios, with real world data, is a promising next step for future research activities.

III.2.4.1 Exemplary Smart Factory Setting

The smart factory in our application example is an automated production facility for the custom production of sports shoes.[10] The factory produces sports shoes, which are customized by customers online in regard to shoe type, fabrics, and colors. The company is deploying smart manufacturing technologies in the factory to produce the shoes in the shortest time possible. This enables the highly flexible custom production of sport shoes in a batch size of one, at costs comparable to mass production. Figure III.2-4 illustrates the exemplary setting of the smart factory.

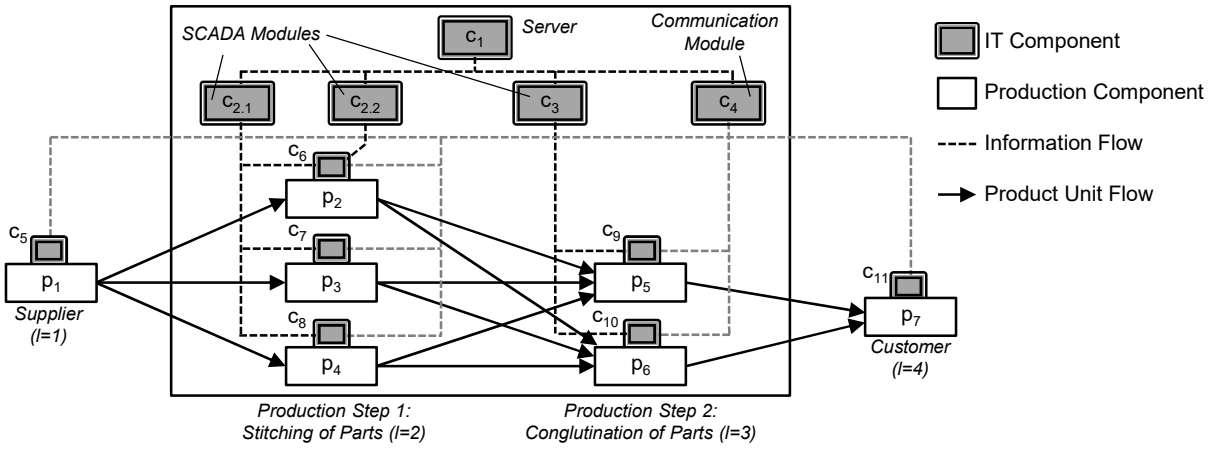


Figure III.2-4: Exemplary Smart Factory – Own Illustration

The customer (p_7) customizes a sports shoe on the sports goods manufacturer's online platform. Once completed, a data interface (c_{11}) automatically transmits the order to the smart factory. In correspondence to the customers' specifications, the necessary semi-finished parts are ordered automatically from the supplier (p_1). For this purpose, another data interface (c_5) connects the supplier with the smart factory. Once the raw materials are received, smart manufacturing machines first stitch the parts of the shoes together (p_2, p_3, and p_4), then conglutinate the stitched parts (p_5 and p_6). All machines, that is, sewing machines and conglutination machines, are equipped with embedded systems ($c_6, c_7, c_8, c_9,$ and c_{10}) connecting the machines with the information network and enabling their communication. The information network contains a communication module (c_4), facilitating information

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

synchronization between smart manufacturing machines, and providing all required optimization parameters. By synchronizing status information, such as utilization, idle capacity, and queued orders, the smart manufacturing machines optimize product flow through the production process. Further, SCADA modules ($c_{2.1}$, $c_{2.2}$, and c_3) for the manufacturing machines control and monitor the assigned machines' production activities. The SCADA module $c_{2.1}$ controls the sewing machines p_2, p_3, and p_4, and SCADA module c_3 controls the conglutination machines p_5 and p_6. Thereby, sewing machine p_2 has an additional backup module ($c_{2.2}$) securing the main module ($c_{2.1}$). Accordingly, the backup module is an existing redundancy. All software modules ($c_{2.1}$, $c_{2.2}$, c_3, and c_4) are hosted on a company-owned server (c_1), located on the premises of the smart factory. The assignment of the IT components to the respective IT services is illustrated in Table III.2-1.

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

Table III.2-1: IT component assignment

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

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

Table III.2-2: Interference degrees of IT components

Once the production of an order is completed, the sports shoes are shipped to the customer. The smart factory has a capacity of 120 units and a utilization rate of 100%. The production components' capacities, utilizations, and idle capacities are shown in Table III.2-3.

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

Table III.2-3: Capacity and utilization of production components

III.2.4.2 Analysis of Basic Scenario

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

Process Step l	1	2	3	4
Expected Loss μ_l (\$)	5	10	10	15
Standard Deviation σ_l (\$)	1.5	3	3	4.5

Table III.2-4: Loss values of process steps

The resulting *risk value matrix* $X_{C,L}$, noted in Table III.2-5, presents the total threat potential ($\sum_{l=1}^{4} x_{c_s,l}$) posed by the non-availability of each IT component c_s.

IT Comp. c_s	c_1	$c_{2.1}$	$c_{2.2}$	c_3	c_4	c_5	c_6	c_7	c_8	c_9	c_{10}	c_{11}	$\sum$
VaR $x_{(c_s,1)}$ ($)	896	0	0	0	672	448	0	0	0	0	0	0	
VaR $x_{(c_s,2)}$ ($)	1,792	896	0	0	1,344	896	299	299	299	0	0	0	
VaR $x_{(c_s,3)}$ ($)	1,792	896	0	1,344	1,344	896	299	299	299	448	448	0	
VaR $x_{(c_s,4)}$ ($)	2,688	1,344	0	2,016	2,016	1,344	448	448	448	672	672	1,344	
VaR $\sum_{l=1}^{4} x_{(c_s,l)}$ ($)	7,169	3,136	0	3,360	5,376	3,584	1,045	1,045	1,045	1,120	1,120	1,344	29,346
Rank	1	5	12	4	2	3	9	9	9	7	7	6	

Table III.2-5: Analysis Results and Risk Value Matrix

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

- The server of the smart factory (c_1) causes the *maximum possible threat potential*, with a VaR of $7,169, as its non-availability results in a complete standstill in the production network.
- The supplier data interface (c_5) ranks third, and before the SCADA modules (fourth and fifth, respectively), although the supplier data interface has a lower interference degree than the SCADA modules. This can be explained by the *impact location* of the failing IT components. The supplier data interface influences the first process step, in contrast to the SCADA modules, which influence later process steps. Therefore, an interesting insight is that the impact location in the production network is an important factor because the supplier data interface's restriction causes production failures in all subsequent process steps of our smart factory example. Further, the SCADA module for the sewing machines has a partial backup, which reduces its threat potential.
- The embedded systems of the conglutination machines (c_9 and c_{10}) rank seventh and before the sewing machines' embedded systems (c_6, c_7 and c_8), although they affect a later process step. This is due to the utilization of the conglutination machines, which with 60 units are more substantial than the sewing machines' 40 units, and hence, lead to higher threat potentials.

Of course, the complexity of the exemplary smart factory is limited and therefore, the server's first rank may seem obvious. However, smart factory networks in practice are far more complex and unmanageable because they consist of considerably more production

components and IT components, inducing a highly complex dependency structure. Further, we assumed a symmetric setting regarding the production components' capacities within a process step, meaning that all production components in a process step possess identical capacities. This might also differ in practice, as machines are constantly developed and production facilities typically grow over time, resulting in a heterogeneous machinery pool. Nevertheless, the results and insights of our application clearly indicate the need for decision support through a structured approach that assesses the availability risks of individual IT components. With the information provided by our risk assessment model, the focal company's management can discuss potential IT security measures, and can profoundly ground corresponding investment decisions.

III.2.4.3 Sensitivity Analysis

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

III.2.4.3.1.Utilization Variation

For the utilization variation, we increase the utilization of all production components gradually, from 1% to 100%, and evaluate the effects on the VaR values of the IT components and the VaR sum. Thereby, the VaR sum $\sum_{s=1}^{k}\left(\sum_{l=1}^{L} x_{c_s,l}\right)$ of the *risk value matrix* $X_{C,L}$ makes no statement regarding the information network's total threat potential because our model analyzes scenarios with individual IT component failures. However, the VaR sum can be used as an indicator of the vulnerability of the production network to IT component non-availabilities. All other parameters, such as interference degrees and loss potentials, are kept constant. The effects of an increasing utilization on our model's results can be seen in Figure III.2-5.

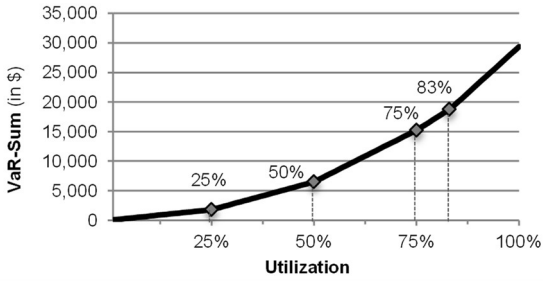


Figure III.2-5: Utilization Variation – VaR-Sum

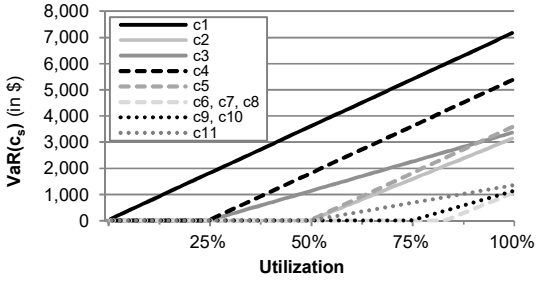


Figure III.2-6: Utilization Variation – VaR(c_s)

The VaR sum increases with an increasing utilization because more units are in the production process. However, the slope of the curve is not linear, and illustrates four kink points at which the slope increases. The kink points are caused by IT components whose non-availabilities have no effect up to a certain utilization threshold. This effect can be seen in more detail in Figure III.2-6, which shows the curve of each IT component relative to the utilization. One reason for the kink points is an interference degree less than 100%. Depending on the utilization, the restricted production components can still process some, or even all, product units with their reduced capacity. For example, the software modules (c_2, c_3, and c_4) have an interference degree of 75%. Accordingly, the non-availability of the communication module (c_4) and the SCADA module (c_3) has no effect until the threshold reaches 25%. The sewing machines' SCADA module ($c_{2.1}$) causes no losses even until the threshold reaches 50% because of its partial backup. The embedded systems have an even higher threshold. First, this is caused by the interference degree of 50%, but also by the compensation effect for utilizations less than 100%. Accordingly, the threshold of the embedded system is 75% (c_9 and c_{10}) and 83%, respectively (c_6, c_7, and c_8). Thereby, the sewing machines' embedded systems have a higher threshold because three machines are available for compensation within the stitching step, in contrast to two machines in the conglutination step.

III.2.4.3.2.Loss Potential Variation

In addition to the utilization, we analyze the impact of loss potential estimations on the results of our model in the example smart factory scenario to demonstrate the effects of inaccurate expert estimations. Thereby, we multiply the loss values μ_l and σ_l with a variable β to demonstrate the effects of an underestimation ($\beta < 1$), respectively an overestimation ($\beta > 1$). All other input parameters are constant. The effects of deviating loss potential estimations for different, higher utilizations are shown in Figure III.2-7, with $0.5 \leq \beta \leq 1.5$. The underestimation of loss potentials results in lower, and the overestimation in higher, threat potentials. Accordingly, the curves show an ascending slope. Thereby, the slope of a curve increases for higher utilizations.

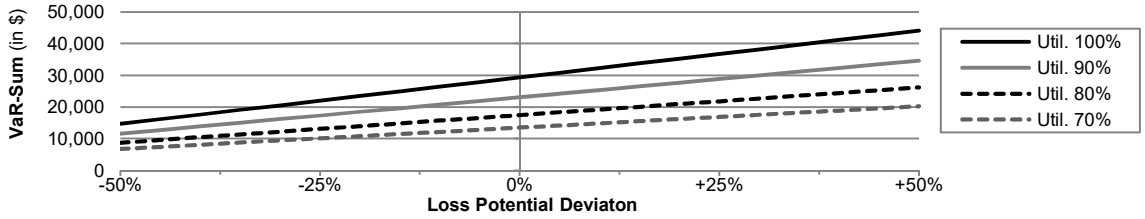


Figure III.2-7: Impact of Deviating Loss Potential Estimation

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

III.2.4.4 IT Security Measure Analysis

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

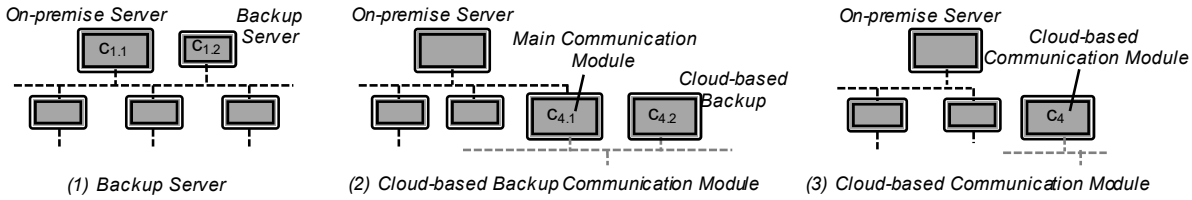


Figure III.2-8: Exemplary IT Security Measures – Own Illustration

For instance, these include redundancies in the information network. However, we also want to note other process-based measures. As we demonstrated during the sensitivity analyses, reduced loss potentials in specific process steps can reduce the overall threat potential. Thus, improving processes to reduce loss potentials is an effective way to reduce an overall threat

potential. As loss potentials are input parameters in our model, it is not possible to explain the cause-effect chain of process-based measures and the reduced loss potentials as their effect. However, our model can illustrate the impact of reduced loss potentials on the production network's vulnerability to IT component non-availabilities if the reduced loss potentials are used as adjusted input parameters. Structure-based measures are supposed to be highly effective against IT availability risks, including redundancies within the information network. Thereby, measures such as backup IT components or cloud-based applications influence dependency relations by preventing single-point failures of IT components. For example, the basic scenario of our example application contains a redundancy, securing the SCADA service for sewing machine p_2 due to the partial backup SCADA module ($c_{2.2}$). Without the redundancy, the VaR increases to \$30,915. Accordingly, the partial backup component reduces the VaR sum by 5.1%. In the following, we add further IT security measures, as illustrated in Figure III.2-8, to the information network, in addition to the already existing partial backup component ($c_{2.2}$).

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

information network are removed. However, the production components still depend on the cloud-based communication module for the corresponding communication IT service because there is no redundant backup for that service. Accordingly, the VaR only decreases by 3.1%, to $28,450.

III.2.5 Managerial Implications

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

1. The results gained in the course of our research clearly indicate the need for decision support through a structured approach. The complexity that arises from the multitude of direct and indirect dependencies in ever complex smart factory information networks and the resulting propagation effects of failures can no longer be mastered by human decision-makers alone due to an increasing lack of transparency. In this regard, our structured approach presents a risk-oriented guidance for practitioners in the course of their digital transformation.
2. There is a multitude of different IT security measures that companies can apply as part of their IT security strategy. These differ in their modes of action, but ultimately their effect on the possible extent of damage is decisive. Thereby, some IT security measures target specific critical components in the information network, in particular structural IT security measures such as redundancies through backup systems. In contrast, other IT security measures have a more holistic effect on the information network such as process-related IT security measures, e.g., reduced damage potentials through improved recovery measures. Here, our structured approach serves as guidance in the derivation of an appropriate IT security strategy. It supports investment decisions on a profound economic basis, as it helps to identify the most critical IT components and quantifies the threat potentials resulting from propagation effects.
3. A decisive lever for the IT security strategy is the degree of interconnectedness within the smart factory information network. Companies are faced with the question of where interconnectedness makes sense and creates added value and where air gaps should be deliberately made or redundancies should be created. For this, our approach

provides a risk-oriented guidance for the solid design of smart factory information networks.

4. The insights gained by the sensitivity analysis demonstrate the importance of the utilization as an influencing factor. We were able to show that the threat potential increases with an increasing utilization because risk reduction effects, such as the compensation ability, decrease gradually. Considering the high utilization of smart factories through automation and optimization technologies as key benefits, the threat potentials posed by IT availability risks will be rather high in smart factories (Radziwon et al. 2014, Schuh et al. 2014).
5. The insights gained by the loss potential sensitivity analysis demonstrate that the underestimation or overestimation of loss values has a greater effect on the model's results in application scenarios with high utilizations. Therefore, considering the probable, high utilization of smart factories, the loss potential estimation's accuracy is of crucial importance for risk quantification to derive accurate results.
6. Our risk assessment model examines IT availability risks primarily on the internal company level. In times of comprehensive, cross-company, Internet-based interconnection of information systems, however, the supply chain level becomes particularly important for companies' IT security strategy. For this purpose, our approach can also be extended across companies to make the prevailing complexity tangible and controllable.

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

III.2.6 Conclusion, Limitations, and Further Research

The increasing adoption of smart manufacturing technologies promises great potential, leading to a paradigm shift in manufacturing. The emerging smart factory networks constitute automated and flexible production facilities, and can efficiently produce individualized products in low batch sizes at a cost-efficient level. However, the criticality of IT systems and the interconnectedness of IT and production systems cause an increase in the vulnerability to IT availability risks. Considering this threat scenario, companies must employ extensive IT

security measures to secure their production facilities. However, the highly complex, interconnected, and interdependent smart factory networks complicate investment decisions regarding possible IT security measures. Thus, decision makers face significant difficulties regarding the allocation of available funds in the most efficient way.

Therefore, we develop a risk assessment model for the quantification and evaluation of IT availability risks in smart factory networks that serves as the basis for corresponding investment decisions. We first model and formalize the smart factory networks' general setting, with its basic structures and relations, by means of graph theory and matrix notation. Then, we quantify IT availability risk by applying the VaR. Our research contributes to literature and practice as it enables a structured analysis of increasingly complex smart factory networks under consideration of not only direct but also indirect dependencies. While other risk assessment approaches like multi-criteria decision models often times address different dimensions of damage and do not consider root causes, our approach focusses on propagation effects and the resulting damages within smart factory networks. Accordingly, our research is rooted in the propagation and damaging effects based on the complex interdependencies in smart factory networks. Our structured approach helps to assess the risks associated with the ever increasing interconnection within smart factories, to assess where interconnections and dependencies should be deliberately avoided and where redundancies should be deliberately created, e.g. by means of backup servers or cloud-based modules. Hence, the insights gained by our model provide practitioners with a risk-oriented guidance regarding the solid design of smart factory networks in the course of their digital transformation. Further, it helps to identify the most critical IT components, and consequently offers a profound economic basis for corresponding investment decisions regarding IT security mitigation measures. Thus, it also supports the derivation of an appropriate IT security strategy. Based on the results of our model, other subsequent approaches, such as multi-criteria decision making models, can then be applied. For example, based on a multi-criteria decision model, an optimal portfolio of IT security measures could be derived by taking into account different decision criteria and dimensions. Corresponding approaches already exist, for example, in the area of cloud computing, for which Shameli-Sendi and Cheriet (2014) propose a risk assessment model based on fuzzy multi-criteria decision-making or Akinrolabu et al. (2018) propose a cloud supply chain cyber risk assessment model which applies decision support analysis and supply chain mapping for the identification, analysis and evaluation of cloud risks. Besides the risk-

oriented guidance as the basis for subsequent decision making, our risk assessment model provides the possibility to consider a cross-company view regarding the effects of interorganizational information systems, as cross-company ecosystems increases constantly in the course of the ongoing digitalization. We demonstrate the model's applicability in a setting based on an exemplary real world scenario, and conduct sensitivity analyses. Our results demonstrate that the criticality of an IT component is determined by numerous factors: the dependency relationships to production components, the degree of productivity interference caused by the IT component failure, the IT component failure's impact location within the production process, loss potentials in the respective process steps, the utilization of dependent production components, and the extent of the possible compensation effect. The variety of these influencing factors and their complex interplay clearly indicate the need for a risk assessment model enabling a structured analysis, and supporting investment decisions.

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

Other than these limitations, we made certain model assumptions that limit the model's applicability, but that, in our opinion, are reasonable to keep the model's complexity moderate. Nevertheless, relaxing some model assumptions offers potential areas for the model's further development. First, our model assumes that IT components fail completely because technical failures and attacks result in the complete non-availability of IT components. Partial

functionality interferences of IT components are not considered. As this could occur in some specific threat scenarios, such as data manipulations, the inclusion of this aspect could be a potential extension of our model. Second, our model analyzes the event of an IT component's non-availability and its implications in a fixed time period. Thus, another substantial extension would involve including a timing component and thus, developing our approach further to a continuous-time model. Third, though our model considers individual interference degrees for the respective IT components, we assume that an IT component's non-availability causes identical interference degrees on all dependent production components. We believe that this approach is reasonable because it includes the interference degrees on a detailed IT component level. A further differentiation on the production component level would cause an increase in complexity, while the added value seems questionable. However, a further differentiation of interference degrees on a production level would be possible.

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

III.2.7 References

Aagedal, Jan Øyvind, Den Braber, Folker, Dimitrakos, Theo, Gran, Bjørn Axel, Raptis, Dimitris, and Stolen, Ketil 2002. "Model-based Risk Assessment to Improve Enterprise Security," in *Proceedings of the 5th IEEE International Enterprise Object Computing Conference*, Lausanne, Switzerland, 51–62.

Ackermann, Tobias, and Buxmann, Peter 2010. "Quantifying Risks in Service Networks: Using Probability Distributions for the Evaluation of Optimal Security Levels," in *Proceedings of the Americas Conference on Information Systems*. Lima, Peru.

Akinrolabu, Olusola, Steve New, and Andrew Martin. 2018. "Cyber Supply Chain Risks in Cloud Computing – Bridging the Risk Assessment Gap," in *Open Journal of Cloud Computing* 5 (1): 1–19.

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

Amiri, Amin Khodabandeh, Cavusoglu, Hasan, and Benbasat, Izak. 2014. "When is IT Unavailability a Strategic Risk?: A Study in the Context of Cloud Computing," in *Proceedings of the 35th International Conference on Information Systems*, Auckland, New Zealand.

Arns, Michael, Fischer, Martin, Kemper, Peter, Tepper, Carsten. 2002. “Supply Chain Modelling and its Analytical Evaluation,” in *Journal of the Operational Research Society* 53 (8): 885–894.

Borodulin, Kirill, Radchenko, Gleb, Shestakov, Aleksandr, Sokolinsky, Leonid, Tchernykh, Andrey, and Prodan, Radu. 2017. “Towards Digital Twins Cloud Platform: Microservices and Computational Workflows to Rule a Smart Factory” in *Proceedings of the10th International Conference on Utility and Cloud Computing* Austin, Texas, USA.

Brettel, Malte, Friederichsen, Niklas, Keller, Michael, Rosenberg, Marius. 2014. “How Virtualization, Decentralization and Network Building Change the Manufacturing Landscape: An Industry 4.0 Perspective”, *in World Academy of Science: Engineering and Technology International Journal of Mechanical, Aerospace, Industrial, Mechatronic and Manufacturing Engineering* 8 (1): 37–44.

Broy, Manfred, Cengarle, María Victoria, and Geisberger, Eva. 2012. "Cyber-Physical Systems: Imminent Challenges," in *Large-Scale Complex IT Systems. Development, Operation and Management,* R. Calinescu and D. Garlan (eds.), Springer Berlin Heidelberg, 1–28.

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

Buldyrev, Sergey V, Parshani, Roni, Paul, Gerald, Stanley, H. Eugene, and Havlin, Shlomo. 2010. "Catastrophic Cascade of Failures in Interdependent Networks," *Nature* 464: 1025–1028.

Byres, Eric 2013. "The Air Gap: SCADA's Enduring Security Myth," *Communications of the ACM* 56 (8): 29–31.

Byres, Eric, and Lowe, Justin. 2004. "The Myths and Facts behind Cyber Security Risks for Industrial Control Systems," in *Proceedings of the VDE Congress*, 213–218.

Caralli, Richard A., Stevens, James F., Young, Lisa R., and Wilson, William R. 2007. "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process," *Technical Report No. CMU/SEI-2007-TR-012, ESC-TR-2007-012,* 1–154.

Cardenas, Alvaro A., Amin, Saurabh, and Sastry, Shankar. 2008. "Secure Control: Towards Survivable Cyber-Physical Systems," *System* 1: 1–5.

Cavusoglu, Hasan, Cavusoglu, Huseyin, and Raghunathan, Srinivasan. 2004. "Economics of IT Security Management: Four Improvements to Current Security Practices," *The Communications of the Association for Information Systems* 14: 65–75.

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

Colombo, Armando Walter, Karnouskos, Stamatis, and Bangemann, Thomas. 2013. "A System of Systems View on Collaborative Industrial Automation," in *Proceedings of the IEEE International Conference on Industrial Technology*, Cape Town, South Africa, 1968–1975.

Cooper, Robin, and Kaplan, Robert S. 1991. "Profit Priorities from Activity-based Costing," *Harvard Business Review* 69 (3): 130–135.

Danziger, Michael M., Shekhtman, Louis M., Bashan, Amir, Berezin, Yehiel and Havlin, Shlomo. 2016. "Vulnerability of Interdependent Networks and Networks of Networks," in *Antonios Garas (ed.): Interconnected Networks*. Springer, Cham, 79–99.

Duffie, Darrell, and Pan, Jun. 1997. "An Overview of Value at Risk," *The Journal of Derivatives* 4 (3): 7–49.

Eden, Peter, Blyth, Andrew, Jones, Kevin, Soulsby, Hugh, Burnap, Pete, Cherdantseva, Yulia, and Stoddart, Kristan. 2017. "*SCADA System Forensic Analysis Within IIoT,*" *L. Thomas and D. Schaefer (eds.): Cybersecurity for Industry 4.0 – Analysis for Design and Manufacturing*. Springer, Cham, 73–101.

Eom, Jung-Ho, Park, Seon-Ho, Han, Young-Ju, and Chung, Tai-Myoung. 2007. "Risk assessment method based on business process-oriented asset evaluation for information system security." in *Proceedings of the International Conference on Computational Science*, 1024–1031.

Faisal, M. N., Banwet, D. K., and Shankar, R. 2006. "Supply Chain Risk Mitigation: Modeling the Enablers," *Business Process Management Journal* 12 (4): 535–552.

Fenz, Stefan, Ekelhart, Andreas, and Neubauer, Thomas. 2011. "Information Security Risk Management: In Which Security Solutions is it Worth Investing?," in *Communications of the Association for information Systems* 28 (1): 329–356.

Festinger, Leon. 1949. "The Analysis of Sociograms Using Matrix Algebra." *Human Relations* 2: 153–158.

Fleisch, Elgar, and Thiesse, Frédéric. 2007. "On the Management Implications of Ubiquitous Computing: An IS Perspective." *in Proceedings of the 15th European Conference on Information Systems*, St. Gallen, Switzerland, 1929–1940.

Fridgen, Gilbert, Stepanek, Christian, and Wolf, Thomas. 2014. "Investigation of Exogenous Shocks in Complex Supply Networks – A Modular Petri Net Approach," in *International Journal of Production Research* 53 (5), 1387–1408.

Geisberger, Eva, and Broy, Manfred. 2015. "Living in a networked world – integrated research agenda cyber-physical systems." Acatech National Academy of Science and Engineering, Munich, Germany.

German Federal Ministry of Economics and Energy 2015. "SPEEDFACTORY – Automatic Custom Manufacture of Sports Shoes and Textiles," http://autonomik4.pt-dlr.de/en/SPEEDFACTORY.php. Visited: March 27th, 2015.

Gordon, Lawrence A., and Loeb, Martin P. 2002. "The Economics of Information Security Investment," *ACM Transactions on Information and System Security* 5 (4): 438–457.

Gordon, Lawrence A., Loeb, Martin P., and Sohail, Tashfeen. 2003. "A Framework for Using Insurance for Cyber-Risk Management," *Communications of the ACM* 46 (3): 81–85.

Haller, Stephan, Karnouskos, Stamatis, and Schroth, Christoph. 2009. "The Internet of Things in an Enterprise Context," *in Future Internet – FIS 2008,* John Domingue, D. Fensel and P. Traverso (eds.), Springer Berlin Heidelberg, 14–28.

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

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

Hermann, Mario, Pentek, Tobias and Otto, Boris. 2015. "Design Principles for Industrie 4.0 Scenarios – A Literature Review." *Technische Universität Dortmund – Working Paper 01/2015*.

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

Hessman, Travis. 2013. "The Dawn of the Smart Factory," *Industry Week* 14: 14–19.

Hovav, Anat, and D'Arcy, John. 2003. "The Impact of Denial of Service Attack Announcements on the Market Value of Firms," *Risk Management and Insurance Review* 6 (2): 97–121.

Huang, C. Derrick. 2010. "Optimal Investment in Information Security: A Business Value Approach." in *Proceedings of the Pacific Asia Conference on Information Systems*, Taipei, Taiwan, 444–451.

Iansiti, Marco, and Lakhani, Karim R. 2014. "Digital Ubiquity: How Connections, Sensors, and Data Are Revolutionizing Business," *Harvard Business Review* 92 (11): 91–99.

Jaisingh, Jeevan, and Rees, Jackie 2001. "Value at Risk: A Methodology for Information Security Risk Assessment," in *Proceedings of the 6th INFORMS Conference on Information Systems and Technology*, Miami, USA, 1–15.

Jorion, Philippe. 2006. Value at Risk: The New Benchmark for Managing Financial Risk (3rd ed.). McGraw-Hill.

Jung, Kiwook, Choi, SangSu, Kulvatunyou, Boonserm, Cho, Hyunbo, and Morris, KC. 2017. “A Reference Activity Model for Smart Factory Design and Improvement,” in Production Planning & Control 28 (2): 108–122.

Karabacak, Bilge, and Sogukpinar, Ibrahim. 2005. "ISRAM: Information Security Risk Analysis Method," *Computers & Security* 24: 147–159.

Karnouskos, Stamatis, and Colombo, Armando Walter. 2011. "Architecting the Next Generation of Service-based SCADA/DCS System of Systems," in *Proceedings of the*

37th Annual Conference on IEEE Industrial Electronics Society, Melbourne, Australia, 359–364.

Karnouskos, Stamatis. 2011. "Stuxnet Worm Impact on Industrial Cyber-Physical System Security," in *Proceedings of the 37th Annual Conference on IEEE Industrial Electronics Society*, Melbourne, Australia, 4490-4494.

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

Lee, Edward A. 2008. "Cyber Physical Systems: Design Challenges," *in Proceedings of the 11th IEEE International Symposium on Object Oriented Real-Time Distributed Computing*, Orlando, USA, 363–369.

Lee, Jay, Bagheri, Behrad, Kao, Hung-An. 2015. "A Cyber-Physical Systems Architecture for Industry 4.0-based Manufacturing Systems," *in Manufacturing Letters* 3, 18–23.

Lucke, Dominik, Constantinescu, Carmen, and Westkämper, Engelbert. 2008. "Smart Factory – A Step Towards the Next Generation of Manufacturing," in *Manufacturing Systems and Technologies for the New Frontier – The 41st CIRP Conference on Manufacturing Systems,* M. Mitsuishi, K. Ueda and F. Kimura (eds.), Springer London, 115–118.

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

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

Niesen, Tim, Houy, Constantin, Fettke, Peter, and Loos, Peter. 2016. "Towards an integrative big data analysis framework for data-driven risk management in Industry 4.0." in *Proceedings of the 49th Hawaii International Conference on System Sciences*, 5065–5074.

Papa, Stephen, Casper, William, and Nair, Suku 2011. "Availability-based risk analysis for SCADA embedded computer systems," in *Proceedings of the World Congress in Computer Science, Computer Engineering and Applied Computing*, Las Vegas, USA.

Qi, Qinglin and Fao, Fei. 2018. “Digital Twin and Big Data Towards Smart Manufacturing and Industry 4.0: 360 Degree Comparison,” in *IEEE Access* 6, 3585–3593.

Radziwon, Agnieszka, Bilberg, Arne, Bogers, Marcel, and Madsen, Erik Skov. 2014. "The Smart Factory: Exploring Adaptive and Flexible Manufacturing Solutions," *Procedia Engineering* 9: 1184–1190.

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

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

Savola, Reijo. 2007. "Towards a Security Metrics Taxonomy for the Information and Communication Technology Industry," in *Proceedings of the 2nd IEEE International Conference on Software Engineering Advances*, Cap Esterel, France.

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

Sendi, Alireza Shameli, and Mohamed Cheriet. 2014. "Cloud Computing: A Risk Assessment Model." in *IEEE International Conference on Cloud Engineering*.

Shariatzadeh, Navid, Lundholm, Thomas, Lindberg, Lars, and Sivard, Gunilla. 2016. “Integration of Digital Factory with Smart Factory based on Internet of Things,” in Procedia CIRP 50: 512–517.

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

Schuh, Günther, Potente, Till, Varandani, Rawina, Hausberg, Carlo, and Fränken, Bastian. 2014. "Collaboration Moves Productivity to the Next Level," in *Proceedings of the 47th CIRP Conference on Manufacturing Systems*, Windsor, Canada, 3–8.

Shrouf, Fadi, Ordieres, Joapuin, and Miragliotta, Giovanni. 2014. "Smart Factories in Industry 4.0: A Review of the Concept and of Energy Management Approached in Production Based on the Internet of Things Paradigm," in *Proceedings of the IEEE*

International Conference on Industrial Engineering and Engineering Management, Selangor, Malaysia, 697–701.

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

Smith, Grafton Elliot, Watson, Kenneth, Baker, Will, and Pokorski Jon. 2007. "A Critical Balance: Collaboration and Security in the IT-enabled Supply Chain," *International Journal of Production Research* 45 (11): 2595–2613.

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

Suh, Bomil, and Han, Ingoo 2003. "The IS Risk Analysis Based on a Business Model," *Information & Management* 41: 149–158.

Sun, By Lili., Srivastava, Rajendra P., and Mock, Theodore J. 2006. "An Information Systems Security Risk Assessment Model Under the Dempster-Shafer Theory of Belief Functions," *Journal of Management Information Systems* 22 (4): 109–142.

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

Turber, Stephanie, and Smiela, Christoph. 2014. "A Business Model Type for the Internet of Things," in *Proceedings of the 22nd European Conference on Information Systems*, Tel Aviv, Israel.

Uhlemann, Thomas H.-J., Schock, Crhristoph, Lehmann, Christian, Freiberger, Stefan, Steinhilper, Rolf. 2017. “The Digital Twin: Demonstrating the Potential of Real Time Data Acquisition in Production Systems,” in *Procedia Manufacturing* 9: 113–120.

Wagner, Stephan M., and Neshat, Nikrouz. 2010. "Assessing the Vulnerability of Supply Chains Using Graph Theory," *International Journal of Production Economics* 126: 121-129.

Wang, Shiyong Wan, Jiafu, Li, Di, Zhang, Chunhua. 2016. “Implementing Smart Factory of Industrie 4.0: An Outlook,” *in International Journal of Distributed Sensor Networks* 12 (1): 1–10.

Wegner, Andre, Graham, James, and Ribble, Eli. 2017. “A New Approach to Cyberphysical Security in Industry 4.0,” in *L. Thomas and D. Schaefer (eds.): Cybersecurity for Industry 4.0 – Analysis for Design and Manufacturing*. Springer, Cham, 59–72.

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

Wu, Teresa; Blackhurst, Jennifer; O’Grady, Peter. 2007. “Methodology for Supply Chain Disruption Analysis,” in *International Journal of Production Research* 45 (7): 1665–1682.

Yadav, Surya B., and Dong, Tianxi. 2014. "A Comprehensive Method to Assess Work System Security Risk," *Communications of the Association for Information Systems* 34: 169–198.

Yoon, Joo-Sung, Shin, Seung-Jun, and Suh, Suk-Hwan. 2012. "A Conceptual Framework for the Ubiquitous Factory," *International Journal of Production Research* 50 (8): 2174–2189.

Zambon, Emmanuele, Bolzoni, Damiano, Etalle, Sandro, and Salvato, Marco. 2007. "Model-based Mitigation of Availability Risks," in *Proceedings of the 2nd IEEE/IFIP International Workshop on Business-Driven IT Management*, Munich, Germany, 75–83.

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

Zuehlke, Detlef. 2010. "SmartFactory – Towards a Factory-of-Things," *Annual Reviews in Control* 34: 129–138.

Zhong, Ray Y., Xu, Xun, and Wang, Lihui. 2017. “IoT-enabled Smart Factory Visibility and Traceability Using Laser-Scanners,“ in *Procedia Manufacturing* 10: 1–14.

III.3 Research Paper 6: "Toward Strategic Decision Support Systems for Systemic Risk Management"

Authors:	Björn Häckel[a,c], Lukas Häfner[b,c], Jochen Übelhör[b,c] [a] University of Applied Sciences Augsburg, Germany bjoern.haeckel@fim-rc.de [b] Research Center Finance & Information Management, Department of Information Systems Engineering & Financial Management (Prof. Dr. Hans Ulrich Buhl), University of Augsburg lukas.haefner@fim-rc.de jochen.uebelhoer@fim-rc.de [c] Project Group Business & Information Systems Engineering of the Fraunhofer FIT, Augsburg, Germany
Under review in:	Journal of the Association for Information Systems

Abstract: *The globalization and digitalization of production and businesses increases interdependencies and complexities of (digitized) value networks. Companies increasingly face lack of transparency issues and are therefore not able to consider their environmental and technological embedment for important management decisions. This development makes companies more and more vulnerable to systemic risks, i.e., risks that usually occur at local parts in (digitized) value networks but threaten to spread to (distant) companies' related business operations. The management of systemic risks is a complex task for companies and requires the assistance of IS technology. We believe that new decision support systems (DSS) will provide a significant tool to assist in the management of these complexities and opacities, endemic to systemic risk management by gathering, processing, and interpreting manifold information originating from internal and external sources of a focal company. In this paper, we conduct research to address the issue described above by developing a generic architecture of a strategic DSS designed specifically to manage systemic risk, and by discussing major challenges for which solutions are required in order to implement such a DSS. We pave the way for important future research by defining selected research questions*

and conclude that the realization of a strategic DSS to support systemic risk management requires joint efforts of interdisciplinary researchers, as well as practitioners.

III.3.1 Introduction

Over the past decades, the increasing globalization of production and businesses has enabled companies to open new customer markets and reduce costs by exploiting new possibilities such as offshoring, outsourcing, international joint ventures, and acquisitions. These developments have resulted in the emergence of increasingly fragmented and distant value networks in which specialized companies cooperate on a global scale. The resulting interconnections of business partners are growing due to just-in-time inventory levels, as well as just-in-sequence production, and the manifold dependencies on inter-organizational information systems (IS) and IS service providers (Basole and Rouse 2008). Hence, as lack of global transparency of value networks increases, single companies are now encountering difficulties with the complexity of their business operations related to important management decisions. This development results in a situation such that the business is increasingly vulnerable to risks from correlated defaults, which stem from a focal company's value network. We refer to those risks that originate at a small number of nodes and move to the entire value network as "*systemic risks.*" Systemic risks are located within the structural composition of a value network as well as the inherent interdependencies (Neitzke 2007), and "are mostly based on cascade spreading effects in networks" (Helbing 2012, p. 276). Such risks may occur at any node on the value network and affect other business partners due to interdependencies in flows of goods, financial flows and flows of information. The term "*systemic risk*" is closely related to "*supply chain risk,"* commonly used within the supply chain (risk) management literature. Supply chain risks comprise "any risks for the information, material, and product flows from the original supplier to the delivery of the final product to the end user" (Jüttner et al. 2003, p. 203). In contrast to systemic risks, which are (to date) especially researched in the context of interbank markets (Bartle and Laperrouza 2009) and supposed to impose large-scale economic impacts (Roengpitya and Rungcharoenkitkul 2011), supply chain risks may also be limited to operational risks with (usually) less economic impact (Tang 2006). Yet, our focus in this paper is on strategic levels of networked (non-financial) companies, i.e., we focus on risks that may jeopardize the existence of a focal company due to major dependencies and interconnections within a dynamic value network. In addition, although existing definitions of supply chain risks are

widely used, we regard this term as neither intuitive nor suitable to describe risks beyond immediate value creation and supply chain management. In particular, certain risks such as dependencies of focal companies on their (IT) service providers or on financial institutions are usually not included within the context of supply chain risks. For this reason, we continue to use the broader terms "*value networks*" and *"systemic risks*" instead of "*supply chains*" and "*supply chain risks*."

There are already some examples of systemic risks in value networks, which have resulted in large economic damages. In October 2011, a flood in Thailand caused production outages in the local hard disk industry that produced 70% of all hard disk motors (a central hard disk component) worldwide. Consequently, hard disk producers such as Seagate and Western Digital halted production for weeks and thus, these manufacturers were not able to meet their customer demand of computer manufacturers like Dell or Lenovo, or online sellers such as Newegg. As a result, market prices for hard disks rose threefold and, a year later, prices were still up 60% to 90% relative to prices prior to the flood (Randewich 2011). Another example is the recall of 7.8 million vehicles in the US in 2014 due to defective driver-side airbags manufactured by the Japanese component supplier, Takata that affected at least the following ten automobile manufacturers: Toyota, Honda, Mazda, BMW, Nissan, Mitsubishi, Subaru, Chrysler, Ford, and General Motors. The defective airbags exploded when an automobile was involved in an accident, dispersing metal shards. The linkage of the defective air bags to at least five customer deaths and several serious customer injuries resulted in the filing of Class-action lawsuits naming several automobile manufacturers (besides Takata) as defendants. This litigation cost the defendants substantial financial penalties; in addition, the defendant manufacturers incurred costs to replace the defective airbags and they suffered from damage to their quality brand images (Bennett et al. 2014). According to a study of Hendricks and Singhal (2005) of 885 disruptions of value networks, the occurrence of (systemic) risks negatively affected the operating performance (mostly sales) as well as the return of the stock price of the affected companies that continued for a period of up to two years. Accordingly, the management of systemic risks in complex and interconnected value networks is of great strategic importance. More recently, emerging trends in technology such as digitalization, the internet-of-things, and cyber-physical (production) systems have accelerated the intensity of these vulnerabilities. There is an increase in integration of value networks within information and communication technology that connects physical production systems, products, services,

business partners, and customers across business (local and global) borders. Despite the numerous benefits of digitized value networks such as the flexible production of custom products at costs comparable to those for mass production ("lot size one"), this development leads to even more value network interconnections, complexity, and therefore vulnerability of single companies. Moreover, new kinds of security risks emerge, since IS are increasingly opened and integrated across company-borders to enable collaboration and thus, allow for peripheral activities with criminal intentions on a high degree of anonymity. This threat was exemplified by a cyber-attack on a steel plant in 2014 reported by the German Federal Office for Information Security (BSI 2014). After they intruded the office network of the plant, the hackers manipulated critical control components, which allowed them to access the separated production network. In the course of the attack, the state of the blast furnace was undefined and it was not possible to shut it down in a controlled manner. The situation resulted in severe damage to the blast furnace and other machinery of the plant (BSI 2014). This example describes a conventional, low-digitized production facility. The threat potential significantly increases in businesses that are dependent on just in time and just-in-sequence production, and participate in highly interconnected, digitized value networks.

Traditionally, a corporate risk management comprises different steps of a risk management process, such as risk identification, evaluation, control, and monitoring. Though spreadsheet calculations created by applications such as Microsoft Excel provide custom solutions for specific risk management purposes (Power and Sharda 2007; Jüttner and Ziegenbein 2009), the resulting diverse and silo structured application landscapes are often inconsistent, do not share an integrated database, and thus, possess functional limitations so they cannot support comprehensive risk management activities. In particular, such IT applications are not capable of handling the increasing complexities and opacities caused by the dynamics of digitized value networks. This is also concluded in the "*governance, risk, and compliance report*" (GRC) by SAP (2015) which interviewed 1,010 executives with responsibilities for GRC in their organizations. The survey states that the increasingly complex business and risk environment is severely challenging companies and that only one in ten organizations are fully satisfied with their current GRC tools, technologies, and processes. A helpful first step for many focal companies would be the integration of different risk management processes as well as corresponding application systems in order to optimize collaboration between risk managers relative to sharing of important (systemic) risk relevant information. Such an

integration enables the design, development and implementation of decision support systems (DSSs), i.e., an IS that supports complex decision making by providing solutions to semi-structured or unstructured problems through accessible user interfaces (Shim et al. 2002; Huang et al. 2010). In particular, a custom DSS is required to manage complexities and opacities of systemic risk management by gathering, processing and interpreting manifold information from inside and outside a focal company. A customized DSS has the potential to improve decision quality, reduce response times, lower risk management costs, and establish new forms of collaboration within company boarders as well as with external business partners. The creation of such a DSS, however, creates several challenges and open-end questions, which have to be approached by both researchers as well as practitioners. In this paper, we address these challenges and open-end questions by developing a generic architecture for a strategic DSS designed specifically to support systemic risk management, a prerequisite effort to the creation of such a DSS:

RQ: *What is an appropriate generic architecture for a DSS that is capable of identifying systemic risks, analyzing those risks, and providing strategic decision support in digitized value networks?*

Following Broniatowski (2015), we define a generic architecture as "generalized structure that may be applied to a technical system […] in order to indicate how information flows between system components" (p.1547). Therefore, our generic architecture is a template for a future DSS that abstractly relates necessary technological components of a risk management IS, based on (systemic) risk relevant information flows. It is the first step within a larger project that requires joint efforts from both (interdisciplinary) researchers as well as practitioners in order to enable companies whose business operations are dependent on digitized value networks to deal with systemic risks. The organization of the remainder of our paper is as follows. Section 2 provides an overview of the various directions of existing research on the topic. In Section 3, we derive the generic DSS architecture based on an appropriate functional design. In Section 4, we discuss challenges and selected research questions regarding the future realization of a strategic DSS for systemic risk management. Finally, Section 5 presents the conclusion, identifies limitations, and provides an outlook for future research.

III.3.2 Related Work

Shang et al. (2008) define DSS as "a class of information systems intended to assist managers in decision-making" (p. 2). Traditionally, a DSS provides "more comprehensive support for human control systems [...] while maintaining and strengthening human qualities" (Strohmaier and Rollett 2005, p. 4). Since the concept of a DSS emerged in the 1970s, supporting human qualities to control decisions has been more important in this field of research than replacing the humans with computers (Arnott and Pervan 2008). DSS is a fast growing field of IS research (Suduc et al. 2010) and we continue to analyze DSS literature within the special application field of corporate and public risk management in order to locate our research subset. Second, we present literature on supply chain risk management, which investigates topics closely related to our objective, and further elaborate why this discipline, however, is insufficient to develop measures against systemic risks. Moreover, this part illustrates the importance of IS research and our approach in particular. Third, we extend previous arguments by identifying additional challenges in the emerging field of digitized value networks.

III.3.2.1 Decision Support Systems in Risk Management and Methodology

In general, literature that researches DSS within the application field of risk management addresses different areas of application. On an operational level of business-management, Fang and Marle (2012) built a simulation-based DSS approach for project risk management, which integrates risk identification, risk evaluation, risk control, and risk monitoring. Similar, Dey (2001) develops a DSS for project planning by using "*analytical hierarchy process*" as a structured technique to analyze project risks as well as decision trees for deriving appropriate risk responses. Mahdi and Alreshaid (2005) use analytical hierarchy process to build a DSS for the proper selection of project delivery methods that integrates risk and performance measures. To prevent production system failures, Puente et al. (2002) developed a DSS based on the qualitative failure mode and effect analysis. Their method is built on structured expert knowledge and establishes risk priority categories. Li and Liao (2007) proposed a decision support framework for operations in dynamic alliances, which combines core competences of different companies. Their approach is capable of identifying and evaluating various types of risk factors in multi-attribute decision-making.

On a tactical level of business-management, Hong and Lee (2013) proposed a DSS for procurement risk management. By considering correlated demand, yield, and price uncertainties, their approach includes the design of a robust purchasing plan for supplier selection and order allocation. Converging toward our objectives, Güller et al. (2015) proposed a decision support model of supply chain risk management. Their framework integrates an agent-based simulation model, real-time databases as well as risk management processes and is suited to manage disruption risks proactively before they occur. However, we want to go beyond those authors' application area, which is restricted to directly observable flows of goods and business collaborations (i.e., operational and tactical levels of business-management). Our objective is to set a direction for a strategic DSS that is capable of capturing systemic risks that arise from widely ramified as well as complex network structures and (informational) interdependencies. In particular, we want to contribute to this area of literature by developing a generic DSS architecture that defines the foundation for an intelligent IS, which is capable of supporting risk managers by deriving risk information for strategic corporate decisions.

Literature on strategic DSS, as applied to risk management, is limited to critical infrastructure and large-scale public construction projects, i.e., applications to public authorities which are usually in possession of (or are able to obtain) crucial information about important (spatial) properties, involved parties, and interdependencies. To prioritize renewal of water pipeline projects, Moglia et al. (2006) built a DSS that contains a risk management approach to predict cost as well as pipeline failures. Snediker et al. (2008) developed a spatial DSS to mitigate disruption risks in (critical) network infrastructures, identified from several sources such as natural disasters, terrorism, human errors, etc. Their approach facilitates the examination of "*what-if*" planning scenarios in public disaster management by examining geographic and topologic implications. Levy (2005) discussed advances in multiple criteria decision making and respective implementations of DSS for flood risk management. He presents a DSS architecture that he applies to the flood planning and management of the Yangtze River, China. Horita et al. (2015) developed another spatial DSS for flood risk management. Their approach combines data sources from wireless sensor networks with geographic information volunteered from ordinary citizens in high-risk areas. Kumar and Viswanadham (2007) focus on risk management in major construction supply chains and suggest a DSS framework by

applying a case-based reasoning approach. This IT-enabled solution is useful in preventive and reactive risk management.

Although these are just examples that illustrate the scope of existing research on DSS in risk management, we were, despite intensive efforts, not able to identify literature on any strategic DSS applied to systemic risk management. In our opinion, this situation is not surprising, primarily because of the fact that external information, i.e., information from outside of the company that is necessary to monitor and analyze (inter-) dependencies of business operations and associated systemic risks, is usually incomplete or unavailable. We want to contribute to this research gap by proposing a generic architecture for a strategic DSS in systemic risk management and by conducting a subsequent discussion on necessary future research with particular emphasis on the gathering and processing of unstructured (external) input information. We chose to conduct a comprehensive interdisciplinary approach, although this has not allowed our research to study fine-grained details of every related research discipline. In particular, we did not conduct a structured state-of-the-art approach, since this would not have enhanced the explanation of our artifact. An interdisciplinary approach is reasonable, considering that no research discipline (e.g., finance, supply chain management, and operations research) can solely manage the many challenges of systemic risk management. IS and especially DSS research, however, have the ability to merge interdisciplinary knowledge as we particularly demonstrate in Section 4.

III.3.2.2 Supply Chain Risk Management

In order to enable corporate risk management to include risks beyond company boundaries, a new line of research was already established called "*Supply Chain Risk Management*" (SCRM). Literature on this topic has increased significantly since the beginning of the 21th century (Ceryno et al. 2013; Colicchia and Strozzi 2012; Sodhi et al. 2012; Tang and Nurmaya Musa 2011). This may be due to catastrophes related to supply chains such as the 9/11 attacks (USA 2001), hurricane Katrina (USA 2005) and the big earthquake as well as tsunami (Indian Ocean 2004) (Thun and Hoenig 2011; Qazi et al. 2015), and from current developments in globalized, interconnected and dependent industries as stated in our introduction. Ho et al. (2015) define SCRM as "an inter-organisational collaborative endeavour utilising quantitative and qualitative risk management methodologies to identify, evaluate, mitigate and monitor unexpected macro and micro level events or conditions, which might adversely impact any part of a supply chain" (p. 5036). The essence of this definition emphasizes the need to extend

traditional risk management processes through more intensive inter-organizational collaboration in order to include adverse effects that may be due to organizational or environmental parameters that are external to a focal company ("*externalities*"). SCRM literature has already developed several approaches to account for such risk management extensions (Nishat Faisal et al. 2006; e.g. Giunipero and Aly Eltantawy 2004; Manuj et al. 2014; Manuj and Mentzer 2008b; Norrman and Jansson 2004; Peck 2006; Nyoman Pujawan and Geraldin 2009; Ritchie and Brindley 2007).

There are three important research gaps that systematically appear throughout this line of research. First, Qazi et al. (2015) conducted a comprehensive and systematic review of SCRM literature for the years 2000 to 2014 and concluded that existing SCRM approaches predominantly use qualitative methodologies rather than quantitative techniques. A review of SCRM literature between the years 2000 to 2010 (Ghadge et al. 2012) identified this result. The researchers state, "the preferred methodology has been qualitative" (p. 324). To illustrate this first research gap from a practitioner's perspective, Blackhurst et al. (2005) conducted a multi-industry empirical study in which all interviewed supply chain managers emphasized the need for quantitative assessment of critical nodes in the supply chain. Second, the few existing quantitative models for risk assessment usually do not include dependencies between several supply chain risk factors (Qazi et al. 2015; Badurdeen et al.). However, a literature review of Colicchia and Strozzi (2012) for the years 1994 to 2010 revealed that the consideration of dynamic interactions among risk sources and supply chain partners is a "*key challenge*" for effective supply chain risk identification and assessment. Third, most quantitative models are inappropriate for strategic decisions. Tang (2006) reviewed various quantitative models of mitigating supply chain risks. He states that most existing approaches focus exclusively on the management of operational rather than strategic supply chain risks (such as customer demand and supply risks, or price risks) and are therefore not capable of capturing the complexity of an entire supply-chain. However, this is a necessary precondition in order to be able to manage systemic risks such as threats of major disruptions. We conclude that there is a lack of appropriate quantitative risk management approaches for strategic decision support.

An explanation of this lack is because circumstances necessary to create quantitative models for risk management usually require (historical) information for appropriate calculations. Though information gathering is already challenging within company boundaries, creating

quantitative models of a supply chain level is an even more difficult task. The SCRM literature actually emphasizes the importance of (external) information management and, in particular, information sharing between supply-chain partners, which is a shift toward inter-organizational learning (Manuj and Mentzer 2008a). Peck (2006) states that "few would dispute the almost universally held belief […] that […] information sharing […], is a route to more effective supply chain risk management" (p. 134). Yet, Christopher and Peck (2004) state that "there has not been a history of sharing information either with suppliers or customers" (p. 17). Manuj et al. (2014) conducted a survey of supply chain managers in which many interviewees express the desire to evaluate SCRM strategies, external information gathering; however, remains an open challenge. Blackhurst et al. (2005) observe supply chain managers' need for "relevant, timely and credible information" (p. 4075), since supply chain visibility "is the new battleground" (Blackhurst et al. 2005, p. 4073) in competitive environments and "core element of supply chain risk mitigation" (Blackhurst et al. 2005, p. 4073). Besides mitigating risks, supply chain managers must implement information sharing in order to develop competitive advantages (Giunipero and Aly Eltantawy 2004), especially when the technology or market environment change rapidly (Fynes et al. 2005). In particular, researchers found either theoretically (Lee et al. 2000; Cachon and Fisher 2000; Ha and Tong 2008; Li et al. 2006; Lin et al. 2002; Christopher and Lee 2004) or empirically (Zhou and Benton jr. 2007; Wong et al. 2015; Rai et al. 2006) that information sharing can be very beneficial in contractual and operational terms which do not directly affect risk management.

In summary, literature on SCRM emphasizes the importance and benefits of (external) information management and, in particular, information sharing, but usually lacks solutions to the corresponding difficulties that, to date, "do not feature within the core" of SCRM research (Ghadge et al. 2012, p. 328). Hence, although SCRM is already an interdisciplinary field of research (Manuj and Mentzer 2008b; Peck 2006), there remains the need for further integration of interdisciplinary knowledge (Tang and Nurmaya Musa 2011). The use of IS could improve information sharing and therefore risk management across the supply chain (Gupta and Nandan 2014). In particular, the research field of IS enables the creation of a strategic DSS in systemic risk management and is therefore essential for our objective. Such a DSS must possess the capability to quantify systemic risks as well as interdependencies between risk factors; this represents a "*grand challenge*" of IS research (Mertens and Barbian 2015) and a major research requirement in SCRM.

III.3.2.3 Digitalized Value Networks

The concurrent digitalization of value networks, which comprises technological trends such as the Internet-of-Things or cyber-physical (production) systems, promises business potential but also imposes significant challenges for corporate risk management (Lasi et al. 2014). For instance, the increasing organizational and technological interconnectivity between companies leads to ever-complex business dependency structures as well as information-based dependencies, which decrease transparency of business operations and hence, complicate risk management efforts. Further, the real-time constraint of highly optimized, flexible and automated production infrastructures increases the importance of accurate information flows for proper operation of production processes (Hessmann 2013; Schuh et al. 2014a; Yoon et al. 2012) and digitized value networks become increasingly vulnerable to information-based risks such as unavailability, inaccessibility, inaccuracy and unaccountability of information (systems) (Yoon et al. 2012a; Smith et al. 2007). Information-based risks can spread through the entire digitized value network due to informational dependency structures that are independent of the physical connections. Hence, information-based risks can take the property of systemic risks by possessing high damaging potential and must be included in operative and strategic risk management approaches in order to derive (preventive) risk mitigation measures. Further, in the course of digitalization, the importance of (digital) service providers increases significantly, as digital services enable key functionalities for digitized value networks such as real-time information sharing, communication, data storage, and processing. However, digital service providers, not directly involved in the value creation of a company, are inadequate included in existing SCRM approaches.

Literature on systemic risks, so far, is focusing on interbank markets in response to the financial crisis of 2007 (e.g. Acharya et al. 2010; Adrian and Brunnermeier 2009; Bartram et al. 2007; ECB – European Central Bank 2010; Huang et al. 2009; Lehar 2005). The transfer of developed concepts and the adaption to the application field of digitized value networks is still missing. There are first publications that already deal, at least to some extent, with digitalization and the effects on risk management. For example, Keller and König (2014) develop a reference model for service oriented value networks based on actors, risks, and dependency structures of digital cloud networks. Hertel (2015) presents a framework for structuring threat scenarios and risk sources in digitized production infrastructures, i.e., so-

called smart factories. Becker et al. (2013) developed a conceptual modeling language to specify interaction routines in service networks and a modeling method based on social construction of networks. Further, taking advantage of the tremendous amounts of data becoming increasingly available, Caron et al. (2013) exploit the potential of data measures and process mining in the field of risk management. Pika et al. (2016) use event logs of information systems that record execution of business processes to evaluate the overall process risk and to predict process outcomes. However, similar to most SCRM literature, those authors apply qualitative approaches for structuring risks. Quantitative methods of risk identification, evaluation and mitigation as well as economic risk measures are still not developed, and therefore, are subject to future research. Digitalization requires the consideration of the many dimensions of both corresponding potentials and threatening risks.

III.3.3 Generic RMSS Architecture

The previous section provides a sufficient indication that in order to be capable of counteracting systemic risks, researchers, and practitioners must think beyond the capabilities of existing risk management approaches. Inter-organizational information sharing is already used to facilitate procurement as well as delivery processes, reduce storage costs, and to enable outsourcing as well as customer-specific products. However, besides objectives of cost reduction and business development, information sharing and gathering can generate benefits in terms of corporate risk management. The objective of this paper is to derive a generic architecture toward a strategic DSS in systemic risk management. In the following, we refer to such a system as "*Risk Management Support System*" (RMSS) and we begin by presenting an appropriate functional design (Figure III.3-1) that integrates a technological interface for external information sharing and gathering. Then we use this perspective to motivate the components of our generic DSS architecture.

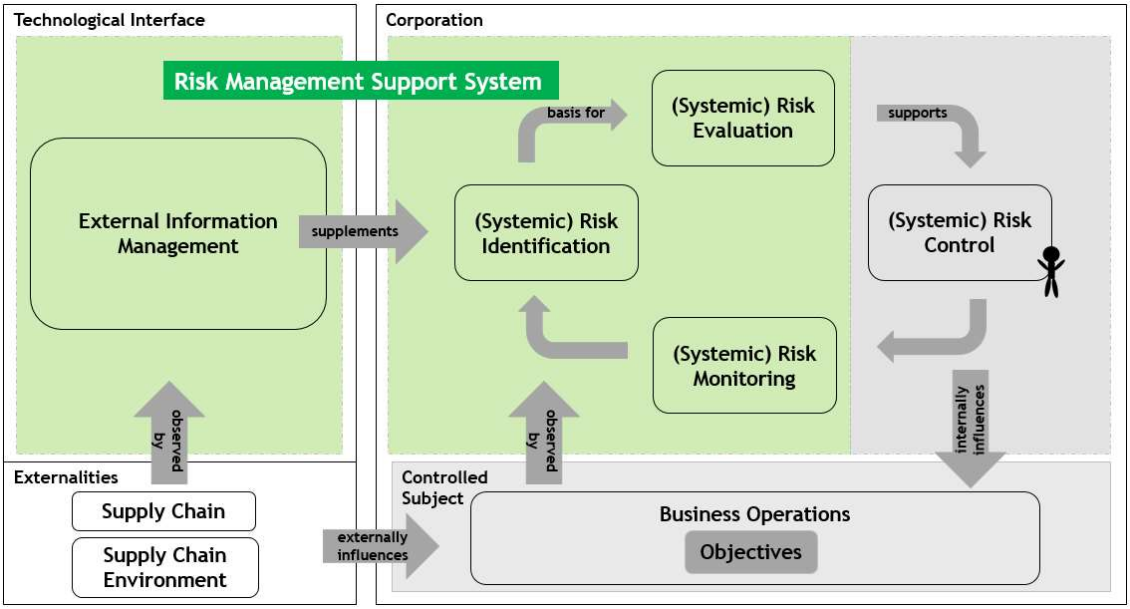


Figure III.3-1: RMSS Functional Design – Own Illustration

A RMSS is the vision of a comprehensive IT-based DSS for systemic risk management, which emphasizes the need for human-driven risk control and decision-making. DSS assist the (human) risk controller to "discover what would happen if a series of decisions are taken" (Arán Carrión et al. 2008, p. 2360). Therefore, a RMSS must provide the risk controller with an opportunity to select specific "*what if*"-scenarios. For example, if the focal company intends to award new delivery contracts to suppliers, the risk manager should be able to request risk estimates of different sourcing strategies by using an appropriate user interface. While risk control is a function executed solely by humans, conduction of other actions of the RMSS occurs autonomously, following human frame conditions. Human experiences and estimations, however, can be provided as additional input to enrich the data set (e.g., expert knowledge for closing data gaps). We build the RMSS functional design exemplar using a common 4-step risk management process for the observation and control of business operations. Thereby, business operations "comprise the dealings of an organization with its stakeholders including customers, suppliers, and employees with regards to everyday activities" (Okoe et al. 2015, p. 345). In addition, we propose a new step in the risk management process, called "*External Information Management*" (EIM). The objective of EIM is to share and gather information with and about supply chain participants, and (digital) service providers as well as their surrounding environment. The technological components of EIM can be located inside as well as outside a focal company, integrated as a monitoring component of the RMSS, with the function to enable an automated information input stream.

Therefore, EIM supplements the RMSS with additional input information processed to identify, evaluate, and monitor (systemic) risks. Provision is made for the human risk controller to provide information about externalities and their (potential) influence on business operations. Based on this new process step, (in particular) strategic decisions such as choices about new business partners, product diversification and international site selection, can be supported in terms of integrated risk and return management. To summarize, the RMSS has to be an extensively networked online system, which is able to execute queries, analyze new as well as previously stored information, and conduct computations in real-time.

To converge to a definition of RMSS, we classify and design a generic RMSS architecture, a template for a future DSS and therefore a fundamental requirement for the development of applicable IS to support systemic risk management. The objective of the generic RMSS architecture is to create abstract relationships among the necessary technological components based on (systemic) risk relevant information flows. In order to appropriately classify and design a generic RMSS architecture, we follow the "*Expanded DSS Framework*" of Power (2002) and Power (2008), who distinguish five categories of DSS technologies depending on their main purposes:

- **Communications-driven DSS:** "use network and communications technologies to facilitate decision-relevant collaboration and communication" (Power 2008, p. 129).
- **Data-driven DSS**: "provide tools for access and manipulation of large databases or data warehouses storing large amounts of data" (Hassan et al. 2015, p. 26). Input data is already structured (Power and Sharda 2007).
- **Document-driven DSS:** use "computer storage and processing technologies to provide document retrieval and analysis" (Power 2008, p. 130). Input data is still unstructured (Power 2008).
- **Knowledge-driven DSS:** "suggest or recommend actions based upon knowledge that has been stored using Artificial Intelligence or statistical tools" (Power and Sharda 2007, p. 1045). They approach problems "which are normally resolved by a human expert" (Hassan et al. 2015, p. 26).
- **Model-driven DSS:** provide decision support with "algebraic, decision analytic, financial, simulation, and optimization models" (Power and Sharda 2007, p. 1044). They "use limited data and parameters provided by decision makers to aid decision makers in analyzing a

situation, but in general large databases are not needed for model-driven DSSs" (Power 2008, p. 126).

In accordance with Power and Sharda (2007) who stated that an IS may also include several of the above approaches, we conceive our RMSS to be an "*integrated system*." This is because none of the outlined categories is sufficiently comprehensive to grasp RMSS complexity, which is necessary to deal with systemic risks. The integrated system combines components from different DSS categories as illustrated in Figure III.3-2.

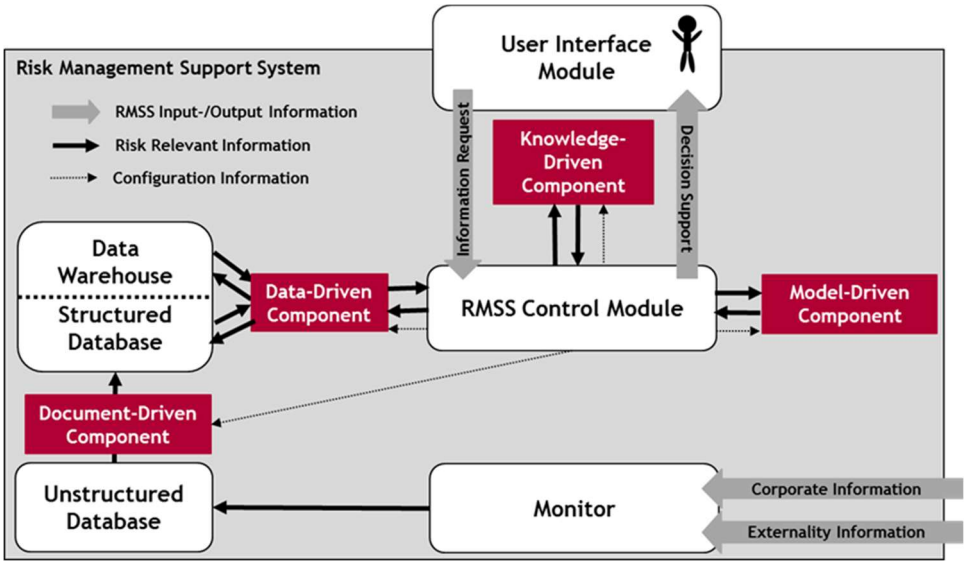


Figure III.3-2: RMSS Generic Architecture – Own Illustration

The RMSS collects input from three sources: First, the objective of the "*Monitor*" is to observe internal influences on business operations, i.e., information within company boundaries. In an example of new procurement contracts, this could comprise order details (e.g., business volumes, time schedules, and requirements specification), corporate information (e.g., strategic goals, balance sheet numbers, and regulations), and existing supplier information (e.g., offering prices, delivery times, existing collaborations, and mutual trust). Second, the Monitor integrates (or is connected with) a technological interface that supports EIM in order to share and gather information from outside the focal company that might influence business operations. In the case of our example, the latter may consist of market information (e.g., supplier competition, product sourcing alternatives, and currency and commodity price fluctuations), supplier vulnerability and criticality information (e.g., natural hazard and country risk indices, credit ratings, supplier product diversification, and supplier dependencies including dependencies on (digital) service providers). Third, the human risk controller

describes the decision problem to the system by specifying an information request within the "*User Interface Module*." Those three input sources initialize the system to create decision support, which is the output of the RMSS. Since the Monitor works independent of specific support requests, it must be preconfigured to support a broad range of search patterns, with access to a variety of data sources. Moreover, it may be necessary to create additional user interfaces to manually enter information. The Monitor passes input information to an "*Unstructured Database*," which gathers all delivered (meta) data. Such information can be manifold and provided in different data formats. Since database capacities are limited, there must be a first step of data processing, which filters, structures and stores required information for further usage. Performance of this task occurs via an intelligent component, which we refer to as the "*Document-driven Component*." Although this component is not a DSS in terms of the Expanded DSS Framework, we attribute special properties of a Document-driven DSS to it. The Document-driven Component extracts, categorizes and summarizes information qualitatively from the Unstructured Database (similar to a Document-driven DSS of (Power 2002)), which can subsequently be used for special (e.g. numeric) purposes. The output o6f the Document-driven Component is structured information (managed by a Structured Database) that can be accessed on demand by a "*Data-driven Component*," which is the connecter to the central "*RMSS Control Module*." Following the concept of a Data-driven DSS, this intelligent component enables the RMSS to "analyze, display and manipulate large structured data sets" (Power 2002, p. 124). In addition, the Data-driven Component can assess information from a Data Warehouse, which (in general) provides long-term storage of historical and consolidated data to improve decision support (Dewan et al. 2013). While an arbitrary number of Structured Databases can exist (e.g., for separately managing structured internal and external information), the Data Warehouse must be unique. Since the RMSS frequently receives new input information, detailed designs of Document-driven and Data-Driven Components have to build on Big Data and Semantic Web Research. The RMSS Control Module receives information requests from the User Interface Module and coordinates the creation of appropriate decision support. After receiving an information request, this intelligent component compares the inquiry to existing knowledge, which is stored within a "*Knowledge-driven Component*." Similar to a Knowledge-driven DSS, such a component provides basic expertise (e.g., rules or procedures) that is derived from historical data (i.e., from previous information requests) or manually implemented default knowledge. In addition, it is capable of conducting qualitative risk analysis by applying human expert

knowledge and visualization measures (e.g., risk matrix, or risk maps). The Knowledge-driven Component informs the RMSS Control Module regarding required input information for qualitative (systemic) risk analysis. For modeling and quantifying (systemic) risks, however, the RMSS Control Module submits an inquiry to the "*Model-driven Component*," a derivative of a Model-driven DSS. Depending on the specific information request, this component chooses appropriate analytical or simulation models and requests required input information from the RMSS Control Module. The RMSS Control Module in turn passes input information requests of the Model-driven and Knowledge-driven Components to the Document-driven and Data-driven Components. These components apply their analytic algorithms to the (Un-) structured Database(s) and the Data Warehouse and respond. After receiving the required input information, the Model-driven Component executes the computations to generate the quantitative risk identification, evaluation, and monitoring while the Knowledge-driven Component performs the qualitative analysis defined by those three steps of the risk management process. The processing of input information requests, subsequent computation as well as analytic procedures iterate for each of the three risk management process steps and cannot be performed concurrently (risk evaluation, for example, postulates previous risk identification). If necessary, the RMSS Control Module configures other intelligent components in order to adapt them to the user's specific information request (e.g. adapting semantic search terms within the Document-Driven and the Data-driven Components). Finally, the RMSS Control Module aggregates and delivers decisions support to the User Interface Module, thereby completing the decision support request. The information request as well as the system's response, recorded within the Knowledge-driven Component, extends the systems knowledge base. The RMSS is now ready to process the next human request for decision support. It is reasonable to implement a feedback function in which the user can assess the relevance and completeness of the decision support response in order to improve the RMSS knowledge database. Note that we did not implement a "*Communications-driven Component*" in our generic RMSS architecture, as we do not focus on distributed decision support; however, respective extensions may be reasonable in future designs. We believe that the first applications of the RMSS will be limited to very specific purposes (e.g., the estimation of tier-one supplier risk exposure for different single- and dual-sourcing strategies of key components) but we expect that the RMSS will evolve to a more complex DSS in the future.

III.3.4 Challenges and selected Research Questions toward future detailed designs

To date, our generic RMSS architecture is a rough concept of a risk management IS that is becoming a necessary tool for many (global) companies. Since many challenges must be addressed, the full implementation of such an IS remains into the future. To address these challenges, it requires joint efforts of researchers, representing interdisciplinary knowledge from diverse research disciplines, and practitioners, to demonstrate practical feasibility. In the following, we provide our contributions to such joint efforts by discussing some major RMSS challenges and selected research questions, thereby providing an orientation for future (IS) research. We structure our discussion along the following dimensions of our RMSS architecture: (1) information sharing and gathering, (2) information analysis, (3) information processing, and (4) decision support.

III.3.4.1 Technological Interfaces for External Information Sharing and Gathering

The RMSS Monitor integrates (or is connected with) a technological interface for EIM, i.e., an interface to obtain information about externalities and their (possible) influence on a focal company. Such a technological interface may be a shared digital database such that each supply chain participant can share its data and obtain external information from other participants. However, even if companies in a digitized value network are willing to share their data (c.f. next research question), it will be necessary that a central unit of organization exists, which provides the necessary coordination and IT infrastructure. Hence, a major challenge emerges from the fact that some organization must invest resources and effort to create and manage the necessary databases. It would be necessary to either form a supply chain board for coordination, or possibly commission an independent service provider. Regardless of the method preferred, most digitized value networks are opaque, complex, interconnected with other digitized value networks and heavily exposed to dynamic changes in composition and boundaries. This fact complicates communication and increases the costs of coordinating such a project. Assuming digitized value networks with several participants, the outlined situation is a perfect example of a "*public good game*," because a single company would prefer others to bear the costs and organizational effort. To summarize, shared digital databases are hardly appropriate for EIM.

In order to communicate with direct business partners, companies have already implemented so-called "*Inter-Organizational Information Systems*" (IOIS). IOIS, which were first

mentioned by Barrett and Konsynski (1982), serve as a technological interface between (two or more) business partners, and support sharing of risk-relevant information. Prominent examples of IOIS are systems for vendor-managed inventory as well as collaborative planning, forecasting, and replenishment systems. However, the nature of systemic risks particularly requires communication beyond direct business partners. Existing approaches to enable communication between distant supply chain participants are product centric technological interfaces such as the EPCglobal Network. "*Product centric*" means that information is embedded within each single product, and not shared through digital databases. Although there are different product centric approaches, "the EPCglobal Network stands out among the rest because in 2003 it was authorized as a Global Standards I (GS1)" (Muñoz-Gea et al. 2010, p. 480). The EPCglobal Network uses RFID tags (with unique identifiers) and readers to read and write product codes affixed to (semi) finished products. For example, Bi and Lin (2009) develop a methodology to discover digitized value networks by using the EPCglobal Network. They analyze information within a four-dimensional matrix and support the capability to map the network structure, quantities of the flows of goods and the time that individual goods remain at and move between digitized value network participants. However, the information that is available from EPCglobal, is not sufficient to manage systemic risks, since a focal company reads only product codes and related information of incoming and outgoing commodities. In particular, information about the flow of goods that is non-physical (e.g. IT services) and/or not directly connected with the focal company (e.g. competitors, and suppliers' customers in different industries) cannot be accessed. While product centric approaches focus on decentralized information of individual products, other technological interfaces can build on bilateral information sharing between distant supply chain participants. Yao (1986) and Goldreich et al. (1987) provide the foundation for the so-called "*Secure Multiparty Computation*" (SMC), a subfield of cryptography, which enables the creation of information exchange software using peer-to-peer networks. "SMC allows mutually distrustful parties to jointly compute a functionality while keeping their inputs private" (Dachman-Soled et al. 2011, p. 130). This technology can enable simultaneous information sharing without leakage of critical information and therefore increase the willingness of companies to participate in information sharing. For example, Fridgen and Garizy (2015) provide a first approach to use SMC in a digitized value network to discover networking structures by simultaneously preserving individual privacy. However, there remains the problem that some organization must (initially) bear the costs and organizational effort to

develop and distribute the corresponding software. To date, technological interfaces that support information sharing and gathering are rarely developed, applied as well as researched upon frame conditions and capabilities. We state the following research question:

Q1: To support EIM, what are the technological interfaces that must be designed to appropriately enable and coordinate the (remote) sharing and gathering of (systemic) risk relevant information?

III.3.4.2 Information Sharing Incentives

Besides enabling and coordinating EIM, appropriate technological interfaces must ensure information sharing incentives. Companies usually have concerns regarding security, privacy and intellectual property (Li et al. 2006). In particular, the concern that information sharing primarily benefits a counterparty is a major disincentive (Mishra et al. 2007; Lee and Whang 2000). Moreover, information sharing may require "the release of confidential and closely guarded financial and strategic information to partners who might have been or may later be competitors" (Du et al. 2012, p. 91). Even if those partners were confidential, there is a thread of information leakage to third parties. Li (2006) refers to this problem as the "*leakage effect*" as competitors may discover confidential information based on the actions of the informed parties. In particular, customers or suppliers of a focal company can use leaked information within upcoming negotiations. For these reasons, companies are frequently reluctant to share information with their network partners.

Q2: How can technological interfaces that support EIM limit a focal company's concerns regarding security, privacy, as well as intellectual property and incentivize information sharing?

III.3.4.3 RMSS Database Systems

One purpose of the monitoring component of our generic RMSS architecture is the intention to collect unstructured (meta) information regarding the company and external influences. Depending on this component's configuration, this may result in huge amounts of push-based data within short time periods. On the one hand, continuous data input streams might lead to data overflow errors and therefore possible loss of critical input information if data storage capacities are not sufficiently large. On the other hand, traditional database management systems are static, which means that information has to be stored before that data can be processed. Therefore, information within the database might be outdated or inaccurate. To

cope with these challenges, a detailed design of our Document-driven Component must integrate modern database systems. In the early years of this millennium, research on "*Data Stream Management Systems*" (DSMS) raised with the objective to create administration software for continuous queries on large data streams (Chen et al. 2000; Babcock et al.; Abadi et al. 2003). DSMS "allow user to analyze the data-in-motion" (Gupta et al. 2012, p. 50) and, in particular, the continuous extraction of risk relevant information. For example, a DSMS in our Document-driven Component can query unstructured input information from the Monitor according to the RMSS control module's configuration input. By using a DSMS, unstructured (static) databases might be dispensable and extracted input information can be stored directly in a Structured Database component as well as the Data Warehouse for further use. Another promising technology, "*Real-Time Database Systems*" (RT-DBS), are "an amalgamation of a conventional database management system and a real-time system" (Bestavros, A., Lin, K. J., & Son, S. H. 2012, p. 1). A RT-DBS not only optimizes for logical correctness (i.e., querying the required information) but also for temporal correctness which means that information has to be processed at the correct time under special consideration of deadlines (Safaei et al. 2011). Although both objectives are important, such a system usually favors timeliness, a property that can be especially valuable in situations such that a risk manager requires contemporary decision support (Diallo et al. 2012). In contrast to a DSMS, a RT-DBS is only approximately real-time, since queries are highly frequented but not continuous, and data must be stored in an (unstructured) database prior to processing. However, if data input streams from the Monitor are highly volatile, a DSMS may encounter damaging traffic congestion in times of high activity (Gürgen et al. 2008), which is less a problem for a RT-DBS. A third kind of modern database system is an "*In-Memory Database"* (IMDB) which stores information within main memory. This enables fast access to the large volumes of data (Buhl et al. 2013). In particular, applications for data processing can access the in-memory data directly (without disk access) and therefore increase transaction performance significantly. Yet, limited capacity is still (likewise in our case) a big problem for IMDB (Nishida and Nishi 2012). Modern relational and multidimensional database systems are indispensable for managing input information within the RMSS. However, more research is required in order to clarify which technology (or combination of technologies) is preferable in order to cope with volatile amounts of unstructured input information. We state the following research question:

Q3: What are the appropriate database architectures that can support specific RMSS purposes?

III.3.4.4 RMSS Data Processing

By executing queries submitted by the RMSS control module, both the Document-Driven Component and the Data-driven Component must process risk relevant information from data that is resident within the (Un-) structured Database(s) and the Data Warehouse. A detailed design of both Components can consist of two types of software: Online transaction processing (OLTP) and online analytical processing (OLAP). OLTP is suited for executing ordinary and highly repetitive queries on detailed and current information (Chaudhuri and Dayal 1997; Park et al. 2015). For example, information transactions submitted to the Data-driven Component, backed by the Structured Database(s), may focus on recent financial figures and key performance indicators of the focal company, or exchange rates with foreign currencies. OLAP, on the other hand, is suited for complex queries and analysis of data. For example, if the RMSS control module requires a time-series and comparison of several exchange rates, then the Data-driven Component can use the OLAP capability to query the Data Warehouse and its long-term historical data. However, since misinterpretation of (especially unstructured) information is frequent, depending on vocabulary choice, the context, and data quality, the benefit offered by decision support is dependent upon the analytic capabilities of both software types. Today, there is still a need for OLTP and OLAP to integrate more accurate semantic data analysis (Gulić 2013) which is particularly important for the RMSS, since correct interpretation of input data is a key to strategic decision support. Semantic data analysis is also an important and fast growing IS research field with the objective to manage the challenges posed by Big Data (Englmeier 2015; Patel and Madia 2016). Standards such as Linked Data are delivered by a larger number of data providers; these data providers create the foundation for more successful semantic data analysis activities in the future (Bizer et al. 2009). We emphasize the need to transfer research of semantic data analysis to the creation of Document-Driven and Data-driven Components.

Q4: What is the appropriate data processing software for RMSS to support a robust level of OLTP and OLAP in order to enable the system to conduct semantic data analysis on risk-relevant input information?

III.3.4.5 Risk Modeling Languages

We believe that a RMSS enables the user to obtain strategic decision support. Such decision support may be both qualitative and quantitative statements regarding risk exposure due to different options of action. The creation of quantitative statements requires the system to

possess risk modeling and assessment techniques, which our RMSS utilizes within the Model-driven Component. The modeling of systemic risks is crucial for subsequent risk assessment, and influenced by the selection of appropriate modeling languages. In the case of RMSS, an appropriate modeling language must fulfill three basic requirements. First, it has to be "*complete"* in terms of representing all relevant components and their relationship in a comprehensive model of risk origination and propagation. Second, it has to be "*consistent"* which means that rules and procedures do not yield contradictory results. Two identical basic situations with identical parameter settings must result in two identical outcomes. Third, it has to be "*simplifying"* in terms of reducing real-world problems to manageable complexity. In particular, a simplifying modeling language should allow for abstraction, formalization and modularization (Fridgen et al. 2014). Modeling languages that support (inter-) organizational risk management purposes have already been used in conjunction with the related research field of SCRM. Neiger et al. (2009) develop a modeling methodology to identify supply chain risks, based on value-focused process engineering (VFPE), a modeling language that "creates links between business processes and business objectives at the operational and strategic levels" (Neiger et al. 2009, p. 155). Mahfouz and Arisha (2010) use integrated modeling approaches (IDEF0 & IDEF3) to assess and mitigate rush order risks at both macro and micro levels of a supply chain. Their simulation model provides numerical measures as well as insights into sensitivities of relevant parameters. Fridgen et al. (2014) extend an approach of Wu et al. (2007) to model disruptions and their propagation in supply chains based on modular Petri Nets. They conclude that IS should manage the increasing complexity of value network and information flow. Wagner and Neshat (2010) build an approach to quantify and mitigate supply chain vulnerability using graph theory. To address the modeling of network interdependencies, Buldyrev et al. (2010) apply Erdős-Rényi networks (i.e., random graphs) and use their specialized model to describe cascade failures during the 2003 electrical blackout in Italy. These are only some examples that illustrate the variety of modeling languages that were already used for (inter-) organizational risk management purposes outside interbank market research. To the best of our knowledge, literature that provides a comparative analysis of modeling languages, their development potential with respect to completeness, consistency, simplicity, and general applicability to modeling systemic risks in digitized value networks does not exist. Therefore, with regard to our purposes, we state the following research question:

Q5: What comprehensive, consistent, and simplifying modeling languages are most appropriate in the sense that they have the most development potential for modeling systemic risks?

III.3.4.6 Risk Assessment Measures

Another important objective of the Model-driven Component is risk assessment. The quantification of risks within the RMSS might be twofold: First, since digitized value networks abstractly consist of companies (nodes) and their connections and dependencies (edges), we must consider the network analytic metrics, generally referred to as "*centrality measures.*" These are metrics that evaluate "the level of importance or influence of a node in a graph" which reflects "certain topological characteristics" (Chen et al. 2016, p. 2). In other words, topological characteristics of a digitized value network provide information regarding the critical and vulnerable nature of certain companies within the network. For example, "*degree centrality*" can quantify the critical attribute ("*out-degree*") and vulnerable attribute ("*in-degree*") of a company, while "*closeness centrality*" as well as "*betweenness centrality*" provide information regarding both properties. Second, the quantification of (systemic) risks can be computed by applying "*risk measures*," a "functional that assigns a numerical value to a random variable which is interpreted as a loss" (Rachev et al. 2008, p. 4). A popular risk measure, because of its simplicity, is the "*value-at-risk*" (VaR) that quantifies a threshold loss value for a given confidence level and period of time. The VaR is the most widely applied risk measure in finance (Peterson and Boudt 2008) and has already been transferred into the context of SCRM (Sanders and Manfredo 2002; Lodree Jr and Taskin 2008; Zhang et al. 2013). However, VaR approaches have several disadvantages, which occur commonly for systemic risks. First, this risk measure does not account for the average extent of damage beyond the given confidence level. This is a serious problem, since it would not be possible to calculate worst-case impacts from systemic risks. Second, many VaR approaches assume normally distributed losses, whereas systemic risks (such as natural disasters) usually exhibit heavy-tailed distributions, i.e., the probability for worst-case scenarios is higher than is assumed by a normal distribution of losses (Kousky and Cooke 2010). Third, VaR approaches require historical data to estimate parameter values and/or perform historical simulations. This data is often not available due to the rarity and manifold nature of systemic risks and/or the absence of external information access. Fourth, VaR measures are not necessarily sub-additive, which means that the VaR of an entire company might exceed the sum of VaR of all

business units. However, there is no evidence that systemic risks exhibit negative diversification effects. Another financial risk measure, which quantifies "the expected loss given that the loss is greater than or equal to the VaR" (Rockafellar and Uryasev 2002, p. 1445), is the "*conditional-value-at-risk*" (CVaR) or "*expected shortfall*." Therefore, in contrast to the VaR, the CVaR would be able to account for worst-case impacts of systemic risks. Moreover, this risk measure is sub-additive, therefore eliminating two of the mentioned VaR disadvantages. Similar to the VaR, researchers suggest the transfer of CVaR to the (non-financial) context of SCRM, especially to support procurement decisions (Chen et al. 2014; Sawik 2013; Zhang et al. 2013). The remaining issues with normally distributed losses and little historical data may be addressed using "*extreme value theory*" (EVT), a research field that provides methods to quantify risks with heavy-tailed distributions based on VaR and CVaR (Allen et al. 2013; Singh et al. 2013). EVT has already been transferred to SCRM (Ravindran et al. 2010) and may be well suited for rare events such as systemic risks (Zhang et al. 2009), characterized by a small amount of available information. However, if no information is available or it is not possible to guarantee information validity, a common occurrence in risk management practice, none of the mentioned centrality metrics or risk measures is able to provide reliable results. We state the following research question:

Q6: What centrality metrics and risk measures are most appropriate or possess the most development potential to quantify (systemic) risks; how do these metrics address missing or inaccurate information?

III.3.4.7 RMSS Learning Capabilities

Finally, we introduce an important research challenge to the development of a Knowledge-driven Component. A detailed design of this intelligent component may include concepts from the IS research field of machine learning with the objective of allowing a system to generalize beyond existing knowledge (Domingos 2012). Existing knowledge within the RMSS may originate from two sources. First, a training set can be used (offline) to initialize machine learning during the development or maintenance of the system. Second, decision support during RMSS operation may be assigned (ex-post) with fitness values, for example, by analyzing human feedback and/or backtesting functions, which enable the system to continuously improve the quality of decision support (online) for individual user requirements. Following Domingos (2012), machine learning consists of three components. First, "*Representation*," which comprises the formal language for the hypothesis space (e.g.

neural networks, support vector machines); second, "*Evaluation*," to compute fitness values for different options for action; and third, "*Optimization*," for actual action selection, i.e., decision support in our case. To date, many different approaches for machine learning exist, even for purposes of supply chain management (Carbonneau et al. 2008). However, there is no evidence in the literature that documents the techniques that might be most suited for the purposes of systemic risk management. Hence, we state the research question:

Q7: What machine learning techniques are most appropriate or have the most development potential to allow the RMSS to enable continuous improvement in decision support?

III.3.5 Conclusions and Discussions

The globalization and digitalization of production and businesses continues to increase interdependencies and complexities within (digitized) value networks. Hence, focal companies' exposure to their dynamic environment is increasing, also increasing systemic risks, which jeopardizes their business operations and therefore their very existence. DSS can assist managers to manage the complexities and opacities in systemic risk management by gathering, processing and interpreting manifold information from inside and outside a company. The creation of such a DSS, however, creates challenges and unanswered questions, which require resolution by researchers and practitioners, working together.

In this paper, we contribute to the development of a strategic DSS created to support systemic risk management by developing a generic architecture and by discussing open challenges as well as selected research questions. The generic architecture is a template for future IS and therefore, a fundamental requirement, which relates necessary technological components, based on systemic risk relevant information flows. Our discussion of open challenges and selected research questions provides an orientation for future research and is another contribution to this interdisciplinary endeavor.

One limitation of our approach is the gap between our generic architecture and future practical implementations, which are, to date, merely a vision. Currently, we have not conducted a detailed study of requirements and possible use cases with practitioners that will be necessary to develop a RMSS detailed design. Moreover, the quantification of systemic risks with missing, incomplete, or inaccurate information is a major research challenge that will determine the performance capability of any future RMSS. To date, we are only able to pose corresponding research questions. Therefore, we especially encourage researchers in

quantitative risk management to join our efforts in order to develop appropriate risk measures. However, we regard this paper as an important first step to motivate interdisciplinary and, in particular, IS research in systemic risks as well as to identify an initial approach to resolution that can be further developed and serve as a foundation for future research.

A reasonable next step for our research is to introduce and discuss our generic RMSS architecture using risk managers from companies that have already established a risk management implementation of strategic decision support. The further development of such systems is inevitable in order to manage the increasing threat of systemic risks. This objective should empower companies to manage not only the opportunities but also the challenges of production and business globalization and digitalization.

III.3.6 References

Abadi, D. J., Carney, D., Cetintemel, U., Cherniack, M., Convey, C., Lee, S., Zdonik, S. (2003). Aurora: A new model and architecture for data stream management. *The International Journal on Very Large Data Bases*, *12*(2), 120–139.

Acharya, V. V., Pederseen, L. H., Philippon, T., & Richardson, M. (2010). Measuring Systemic Risk. *FRB of Cleveland Working Paper (10-02)*.

Adrian, T., & Brunnermeier, M. K. (2009). CoVaR. *FRB of New York. Staff Report (348)*.

Allen, D. E., Singh, A. K., & Powell, R. J. (2013). EVT and tail-risk modelling: Evidence from market indices and volatility series. *The North American Journal of Economics and Finance*, *26*, 355–369.

Arán Carrión, J., Espín Estrella, A., Aznar Dols, F., Zamorano Toro, M., Rodríguez, M., & Ramos Ridao, A. (2008). Environmental decision-support systems for evaluating the carrying capacity of land areas: Optimal site selection for grid-connected photovoltaic power plants. *Renewable and Sustainable Energy Reviews*, *12*(9), 2358–2380.

Arisha, A., & Mahfouz, A. (2010). The Analysis of Rush Orders Risk in Supply Chain: a Simulation Approach. *MODSIM World 2010*.

Arnott, D., & Pervan, G. (2008). Eight key issues for the decision support systems discipline. *Decision Support Systems*, *44*(3), 657–672.

Babcock, B., Babu, S., Datar, M., Motwani, R., & Widom, J. Models and issues in data stream systems. In S. Abiteboul, P. G. Kolaitis, & L. Popa (eds.), *the twenty-first ACM SIGMOD-SIGACT-SIGART symposium*.

Badurdeen, F., Wijekoon, K., Shuaib, M., Goldsby, T. J., Iyengar, D., & Jawahir, I. S. Integrated modeling to enhance resilience in sustainable supply chains. In *2010 IEEE International Conference on Automation Science and Engineering (CASE 2010)*.

Barrett, S., & Konsynski, B. (1982). Inter-Organization Information Sharing Systems. *MIS Quarterly*, *6*, 93–105.

Bartle, I., & Laperrouza, M. (2009). Systemic Risk in the Network Industries: Is There a Governance Gap? *5th ECPR Conference*, 1–21.

Bartram, S. M., Brown, G. W., & Hund, J. E. (2007). Estimating systemic risk in the international financial system. *Journal of Financial Economics*, *86*(3), 835–869.

Basole, R. C., & Rouse, W. B. (2008). Complexity of service value networks: Conceptualization and empirical investigation. *IBM Systems Journal*, *47*(1), 53–70.

Becker, J., Beverungen, D., Knackstedt, R., Matzner, M., Müller, O., & Pöppelbuß, J. (2013). Designing Interaction Routines in Service Networks. *Scandinavian Journal of Information Systems*, *25*(1), 37–68.

Bennett, J., Rogers, C., & Kubota, Y. (2014). *U.S. Seeks Nationwide Recall of Takata Air Bags*. Retrieved October 29th, 2016.

Bestavros, A., Lin, K. J., & Son, S. H. (2012). *Real-time database systems: Issues and applications*. *Springer Science & Business Media: Vol. 396*.

Bi, H. H., & Lin, D. (2009). RFID-Enabled Discovery of Supply Networks. *IEEE Transactions on Engineering Management*, *56*(1), 129–141.

Bizer, C., Heath, T., & Berners-Lee, T. (2009). Linked Data – The Story So Far. *International Journal on Semantic Web and Information Systems*, *5*(3), 1–22.

Blackhurst, J., Craighead, C. W., Elkins, D., & Handfield, R. B. (2005). An empirically derived agenda of critical research issues for managing supply-chain disruptions. *International Journal of Production Research*, *43*(19), 4067–4081.

Broniatowski, D. A. (2015). Does Systems Architecture Drive Risk Perception? *Proceedings of the 2015 Industrial and Systems Engineering Research Conference*.

BSI. (2014). *The State of IT Security in Germany 2014*. Retrieved October 29th, 2016, from https://www.bsi.bund.de/EN/Publications/SecuritySituation/SecuritySituation_node.html

Buhl, H. U., Röglinger, M., Moser, F., & Heidemann, J. (2013). Big Data. *Business & Information Systems Engineering*, *5*(2), 65–69.

Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E., & Havlin, S. (2010). Catastrophic cascade of failures in interdependent networks. *Nature*, *464*(7291), 1025–1028.

Cachon, G. P., & Fisher, M. (2000). Supply Chain Inventory Management and the Value of Shared Information. *Management Science*, *46*(8), 1032–1048.

Carbonneau, R., Laframboise, K., & Vahidov, R. (2008). Application of machine learning techniques for supply chain demand forecasting. *European Journal of Operational Research*, *184*(3), 1140–1154.

Caron, F., Vanthienen, J., & Baesens, B. (2013). A comprehensive investigation of the applicability of process mining techniques for enterprise risk management. *Computers in Industry*, *64*(4), 464–475.

Ceryno, P. S., Scavarda, L. F., Klingebiel, K., & Yüzgülec, G. (2013). Supply chain risk management: a content analysis approach. *International Journal of Industrial Engineering and Management*, *4*(3), 141–150.

Chaudhuri, S., & Dayal, U. (1997). An overview of data warehousing and OLAP technology. *ACM SIGMOD Record*, *26*(1), 65–74.

Chen, J., DeWitt, D. J., Tian, F., & Wang, Y. (2000). NiagaraCQ. *ACM SIGMOD Record*, *29*(2), 379–390.

Chen, P.-Y., Choudhury, S., & Hero, A. O. (2016). Multi-centrality graph spectral decompositions and their application to cyber intrusion detection. In *2016 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP),* 4553–4557.

Chen, X., Shum, S., & Simchi-Levi, D. (2014). Stable and Coordinating Contracts for a Supply Chain with Multiple Risk-Averse Suppliers. *Production and Operations Management*, *23*(3), 379–392.

Christopher, M., & Lee, H. (2004). Mitigating supply chain risk through improved confidence. *International Journal of Physical Distribution & Logistics Management*, *34*(5), 388–396.

Christopher, M., & Peck, H. (2004). Building the Resilient Supply Chain. *The International Journal of Logistics Management*, *15*(2), 1–14.

Colicchia, C., & Strozzi, F. (2012). Supply chain risk management: A new methodology for a systematic literature review. *Supply Chain Management: An International Journal*, *17*(4), 403–418.

Dachman-Soled, D., Malkin, T., Raykova, M., & Yung, M. (2011). Secure Efficient Multiparty Computing of Multivariate Polynomials and Applications. In D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, . . . G. Tsudik (eds.), *Lecture Notes in Computer Science. Applied Cryptography and Network Security,* 130–146. Berlin, Heidelberg: Springer Berlin Heidelberg.

Dewan, S., Aggarwal, Y., & Tanwar, S. (2013). Review on Data Warehouse, Data Mining and OLAP Technology: As Prerequisite aspect of business decisionmaking activity. *International Journal of Research in Information Technology*, *1*(10), 30–39.

Dey, P. K. (2001). Decision support system for risk management: A case study. *Management Decision*, *39*(8), 634–649.

Diallo, O., Rodrigues, J. J., & Sene, M. (2012). Real-time data management on wireless sensor networks: A survey. *Journal of Network and Computer Applications*, *35*(3), 1013–1021.

Domingos, P. (2012). A few useful things to know about machine learning. *Communications of the ACM*, *55*(10), 78.

Du, T. C., Lai, V. S., Cheung, W., & Cui, X. (2012). Willingness to share information in a supply chain: A partnership-data-process perspective. *Information & Management*, *49*(2), 89–98.

ECB – European Central Bank. (2010). *Financial Stability Review*. Retrieved November 26th, 2015, from http://www.ecb.int/pub/pdf/other/financialstabilityreview201006en.pdf?265c395590ffde04e21f3ce67b7dab0e

Englmeier, K. (2015). Role and Importance of Semantic Search in Big Data Governance. In M. Trovati, R. Hill, A. Anjum, S. Y. Zhu, & L. Liu (eds.), *Big-Data Analytics and Cloud Computing*, 21–35. Cham: Springer International Publishing.

Fang, C., & Marle, F. (2012). A simulation-based risk network model for decision support in project risk management. *Decision Support Systems*, *52*(3), 635–644.

Fridgen, G., & Garizy, T. Z. (2015). Supply Chain Network Risk Analysis – A Privacy Preserving Approach. *Proceedings of the 23nd European Conference on Information Systems.*

Fridgen, G., Stepanek, C., & Wolf, T. (2014). Investigation of exogenous shocks in complex supply networks – a modular Petri Net approach. *International Journal of Production Research*, *53*(5), 1387–1408.

Fynes, B., B'Urca, S. d., & Voss, C. (2005). Supply chain relationship quality, the competitive environment and performance. *International Journal of Production Research*, *43*(16), 3303–3320.

Ghadge, A., Dani, S., & Kalawsky, R. (2012). Supply chain risk management: Present and future scope. *International Journal of Logistics Management*, *23*(3), 313–339.

Giunipero, L. C., & Aly Eltantawy, R. (2004). Securing the upstream supply chain: A risk management approach. *International Journal of Physical Distribution & Logistics Management*, *34*(9), 698–713.

Goldreich, O., Micali, S., & Wigderson, A. (1987). How to play ANY mental game. In A. V. Aho (ed.), *ACM Conference,* 218–229.

Gulić, M. (2013). Transformation of OWL ontology sources into data warehouse. *36th International Convention on Information & Communication Technology Electronics & Microelectronics (MIPRO)*,

Güller, M., Koc, E., Hegmanns, T., Henke, M., & Noche, B. (2015). A simulation-based decision support framework for real-time supply chain risk management. *International Journal of Advanced Logistics*, *4*(1), 17–26.

Gupta, P. K., & Nandan, T. (2014). Managing Risk in Supply Chain: Review of Approaches and Emerging Trends. *Apeejay Business Review*, *13*(1&2), 6–16.

Gupta, R., Gupta, H., & Mohania, M. (2012). Cloud Computing and Big Data Analytics: What Is New from Databases Perspective? In D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, . . . V. Bhatnagar (eds.), *Lecture Notes in Computer Science. Big Data Analytics*, 42–61. Berlin, Heidelberg: Springer Berlin Heidelberg.

Gürgen, L., Roncancio, C., Labbé, C., Bottaro, A., & Olive, V. (2008). SStreaMWare: a Service Oriented Middleware for Heterogeneous Sensor Data Management. *Proceedings of the 5th International Conference on Pervasive Services*, 121–130.

Ha, A. Y., & Tong, S. (2008). Contracting and Information Sharing Under Supply Chain Competition. *Management Science*, *54*(4), 701–715.

Hassan, M., Eldin, A. B., & El-Ghazali, A. (2015). A Decision Support System for Subjective Forecasting of New Product Sales. *International Journal of Computer Application*, *126*(2), 25–30.

Helbing, D. (2012). Systemic Risks in Society and Economics. In D. Helbing (ed.), *Understanding Complex Systems. Social Self-Organization,* 261–284. Berlin, Heidelberg: Springer Berlin Heidelberg.

Hendricks, K. B., & Singhal, V. R. (2005). An Empirical Analysis of the Effect of Supply Chain Disruptions on Long-Run Stock Price Performance and Equity Risk of the Firm. *Production and Operations Management*, *14*(1), 35–52.

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

Hessmann, T. (2013). The Dawn of the Smart Factory. *Industry Week*, *14*, 14–19.

Ho, W., Zheng, T., Yildiz, H., & Talluri, S. (2015). Supply chain risk management: A literature review. *International Journal of Production Research*, *53*(16), 5031–5069.

Hong, Z., & Lee, C. K. (2013). A decision support system for procurement risk management in the presence of spot market. *Decision Support Systems*, *55*(1), 67–78.

Horita, F. E., Albuquerque, J. P. d., Degrossi, L. C., Mendiondo, E. M., & Ueyama, J. (2015). Development of a spatial decision support system for flood risk management in Brazil that combines volunteered geographic information with wireless sensor networks. *Computers & Geosciences*, *80*, 84–94.

Huang, G. H., Sun, W., Nie, X.-h., Qin, X.-s., & Zhang, X.-d. (2010). Development of a decision-support system for rural eco-environmental management in Yongxin County, Jiangxi Province, China. *Environmental Modelling & Software*, *25*(1), 24–42.

Huang, X., Zhou, H., & Zhu, H. (2009). A framework for assessing the systemic risk of major financial institutions. *Journal of Banking & Finance*, *33*(11), 2036–2049.

Jüttner, U., Peck, H., & Christopher, M. (2003). Supply chain risk management: outlining an agenda for future research. *International Journal of Logistics Research and Applications*, *6*(4), 197–210.

Jüttner, U., & Ziegenbein, A. (2009). Supply Chain Risk Management for Small and Medium-Sized Businesses. In F. S. Hillier, G. A. Zsidisin, & B. Ritchie (eds.), *International Series in Operations Research & Management Science. Supply Chain Risk,* 199–217. Boston, MA: Springer US.

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,* Retrieved from www.fim-rc.de/Paperbibliothek/Veroeffentlicht/457/wi-457.pdf

Kousky, C., & Cooke, R. (2010). Adapting to Extreme Events: Managing Fat Tails. *Resources of the Future – Issue Brief 10-12*,

Kumar, V., & Viswanadham, N. (2007). A CBR-based Decision Support System Framework for Construction Supply Chain Risk Management. In *2007 IEEE International Conference on Automation Science and Engineering,* 980–985.

Lasi, H., Fettke, P., Kemper, H.-G., Feld, T., & Hoffmann, M. (2014). Industry 4.0. *Business & Information Systems Engineering*, *6*(4), 239–242.

Lee, H. L., So, K. C., & Tang, C. S. (2000). The Value of Information Sharing in a Two-Level Supply Chain. *Management Science*, *46*(5), 626–643.

Lee, H. L., & Whang, S. (2000). Information sharing in a supply chain. *International Journal of Manufacturing Technology and Management*, *1*(1), 79–93.

Lehar, A. (2005). Measuring systemic risk: A risk management approach. *Journal of Banking & Finance*, *29*(10), 2577–2603.

Levy, J. K. (2005). Multiple criteria decision making and decision support systems for flood risk management. *Stochastic Environmental Research and Risk Assessment*, *19*(6), 438–447.

Li, J., Sikora, R., Shaw, M. J., & Woo Tan, G. (2006). A strategic analysis of inter organizational information sharing. *Decision Support Systems*, *42*(1), 251–266.

Li, Y., & Liao, X. (2007). Decision support for risk analysis on dynamic alliance. *Decision Support Systems*, *42*(4), 2043–2059.

Lin, F., Huang, S., & Lin, S. (2002). Effects of information sharing on supply chain performance in electronic commerce. *IEEE Transactions on Engineering Management*, *49*(3), 258–268.

Lodree Jr, E. J., & Taskin, S. (2008). An insurance risk management framework for disaster relief and supply chain disruption inventory planning. *Journal of the Operational Research Society*, *59*(5), 674–684.

Mahdi, I. M., & Alreshaid, K. (2005). Decision support system for selecting the proper project delivery method using analytical hierarchy process (AHP). *International Journal of Project Management*, *23*(7), 564–572.

Manuj, I., Esper, T. L., & Stank, T. P. (2014). Supply Chain Risk Management Approaches Under Different Conditions of Risk. *Journal of Business Logistics*, *35*(3), 241–258.

Manuj, I., & Mentzer, J. T. (2008a). Global Supply Chain Risk Management. *Journal of Business Logistics*, *29*(1), 133–155.

Manuj, I., & Mentzer, J. T. (2008b). Global supply chain risk management strategies. *International Journal of Physical Distribution & Logistics Management*, *38*(3), 192–223.

Mertens, P., & Barbian, D. (2015). Beherrschung systemischer Risiken in weltweiten Netzen. *Informatik-Spektrum*, *38*(4), 283–289.

Mishra, B. K., Raghunathan, S., & Yue, X. (2007). Information sharing in supply chains: Incentives for information distortion. *IIE Transactions*, *39*(9), 863–877.

Moglia, M., Burn, S., & Meddings, S. (2006). A decision support system for water pipeline renewal prioritisation. *ITcon: Electronic Journal of Information Technology in Construction*, *11*, 237–256.

Muñoz-Gea, J. P., Malgosa-Sanahuja, J., Manzanares-Lopez, P., & Sanchez-Aarnoutse, J. C. (2010). Implementation of traceability using a distributed RFID-based mechanism. *Computers in Industry*, *61*(5), 480–496.

Neiger, D., Rotaru, K., & Churilov, L. (2009). Supply chain risk identification with value-focused process engineering. *Journal of Operations Management*, *27*(2), 154–168.

Neitzke, H.-P. (2007). Systemische Risiken. *AACCrisk Report 3/2007*,

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

Nishida, Y., & Nishi, H. (2012). Implementation of a Hardware Architecture to Support High-speed Database Insertion on the Internet. *Proceedings of the International Conference on Engineering of Reconfigurable Systems and Algorithms (ERSA)*,

Norrman, A., & Jansson, U. (2004). Ericsson's proactive supply chain risk management approach after a serious sub-supplier accident. *International Journal of Physical Distribution & Logistics Management*, *34*(5), 434–456.

Nyoman Pujawan, I., & Geraldin, L. H. (2009). House of risk: A model for proactive supply chain risk management. *Business Process Management Journal*, *15*(6), 953–967.

Okoe, A. F., Amartey, R., & Arkorful, H. (2015). Community Sanitation and Corporate Image in the Hospitality Industry:: A Case of Ghana's Top Rated Hotels. In Margaret A. Goralski (ed.), *QRBD – Quarterly Review of Business Disciplines* 1(4).

Park, K., Park, C. S., & Won, H. S. (2015). Dynamic Page Layout Management for Efficient Big Data Analytics. In : *Advanced Science and Technology Letters, Green and Smart Technology 2015,* 735–741. Science & Engineering Research Support soCiety.

Patel, G. A., & Madia, N. (2016). A Survey : Ontology Based Information Retrieval For Sentiment Analysis. *International Journal of Scientific Research in Science, Engineering and Technology*, 2(2), 460–465.

Peck, H. (2006). Reconciling supply chain vulnerability, risk and supply chain management. *International Journal of Logistics*, 9(2), 127–142.

Peterson, B. G., & Boudt, K. (2008). Component VaR for a Non-Normal World.

Pika, A., van der Aalst, W., Wynn, M. T., Fidge, C. J., & ter Hofstede, A. (2016). Evaluating and predicting overall process risk using event logs. *Information Sciences*, *352,* 98–120.

Power, D. (2002). Decision Support Systems: Concepts and Resources for Managers. *Greenwood Publishing Group*,

Power, D. J. (2008). Decision Support Systems: A Historical Overview. In F. Burstein & C. W. Holsapple (eds.), *Handbook on Decision Support Systems 1,* 121–140. Berlin, Heidelberg: Springer Berlin Heidelberg.

Power, D. J., & Sharda, R. (2007). Model-driven decision support systems: Concepts and research directions. *Decision Support Systems*, *43*(3), 1044–1061.

Puente, J., Pino, R., Priore, P., & La Fuente, D. de. (2002). A decision support system for applying failure mode and effects analysis. *International Journal of Quality & Reliability Management*, *19*(2), 137–150.

Qazi, A., Quigley, J., & Dickson, A. (2015). Supply Chain Risk Management: Systematic literature review and a conceptual framework for capturing interdependencies between risks. In *2015 International Conference on Industrial Engineering and Operations Management (IEOM),* 1–13.

Rachev, S., Ortobelli, S., Stoyanov, S., Fabozzi, F. J., & Biglova, A. (2008). Desirable Properties of an Ideal Risk Measure in Portfolio Theory. *International Journal of Theoretical and Applied Finance*, *11*(01), 19–54.

Rai, A., Patnayakuni, R., & Seth, N. (2006). Firm Performance Impacts of Digitally Enabled Supply Chain Integration Capabilities. *MIS Quarterly*, *30*(2), 225–246.

Randewich, N. (2011). *Thai floods, hard drive shortage threaten PC sales*. Retrieved October 3rd, 2016, from http://www.reuters.com/article/us-thailand-floods-tech-idUSTRE79K76Z20111021

Ravindran, A. R., Ufuk Bilsel, R., Wadhwa, V., & Yang, T. (2010). Risk adjusted multicriteria supplier selection models with applications. *International Journal of Production Research*, *48*(2), 405–424.

Ritchie, B., & Brindley, C. (2007). Supply chain risk management and performance. *International Journal of Operations & Production Management*, *27*(3), 303–322.

Rockafellar, R., & Uryasev, S. (2002). Conditional value-at-risk for general loss distributions. *Journal of Banking & Finance*, *26*(7), 1443–1471.

Roengpitya, R., & Rungcharoenkitkul, P. (2011). Measuring Systemic Risk and Financial Linkages in the Thai Banking System. *SSRN Electronic Journal*,

Safaei, A. A., Haghjoo, M. S., & Abdi, F. (2011). PFGN: A Hybrid Multiprocessor Real-Time Scheduling Algorithm for Data Stream Management Systems. In H. Cherifi, J. M. Zain, & E. El-Qawasmeh (eds.), *Communications in Computer and Information Science. Digital*

Information and Communication Technology and Its Applications, 180–192. Berlin, Heidelberg: Springer Berlin Heidelberg.

Sanders, D. R., & Manfredo, M. R. (2002). The Role of Value-at-Risk in Purchasing: An Application to the Foodservice Industry. *The Journal of Supply Chain Management*, *38*(2), 38–45.

SAP. (2015). *Managing risk in an age of complexity*. Retrieved October 3rd, 2016, from http://go.sap.com/docs/download/2015/07/08e10861-357c-0010-82c7-eda71af511fa.pdf

Sawik, T. (2013). Integrated selection of suppliers and scheduling of customer orders in the presence of supply chain disruption risks. *International Journal of Production Research*, *51*(23-24), 7006–7022.

Schuh, G., Potente, T., Varandani, R., Hausberg, C., & Fränken, B. (2014). Collaboration Moves Productivity to the Next Level. *Procedia CIRP*, *17*, 3–8.

Shang, J., Tadikamalla, P. R., Kirsch, L. J., & Brown, L. (2008). A decision support system for managing inventory at GlaxoSmithKline. *Decision Support Systems*, *46*(1), 1–13.

Shim, J. P., Warkentin, M., Courtney, J. F., Power, D. J., Sharda, R., & Carlsson, C. (2002). Past, present, and future of decision support technology. *Decision Support Systems*, *33*(2), 111–126.

Singh, A. K., Allen, D. E., & Robert, P. J. (2013). Extreme market risk and extreme value theory. *Mathematics and Computers in Simulation*, *94*, 310–328.

Smith, G. E., Watson, K. J., Baker, W. H., & Pokorski II, J. A. (2007). A critical balance: Collaboration and security in the IT-enabled supply chain. *International Journal of Production Research*, *45*(11), 2595–2613.

Snediker, D. E., Murray, A. T., & Matisziw, T. C. (2008). Decision support for network disruption mitigation. *Decision Support Systems*, *44*(4), 954–969.

Sodhi, M. S., Son, B.-G., & Tang, C. S. (2012). Researchers' Perspectives on Supply Chain Risk Management. *Production and Operations Management*, *21*(1), 1–13.

Strohmaier, M., & Rollett, H. Future Research Challenges in Business Agility – Time, Control and Information Systems. In *Seventh IEEE International Conference on E-Commerce Technology Workshops,* 109–115.

Suduc, A.-M., Bizoi, M., Cioca, M., & Filip, F. G. (2010). Evolution of Decision Support Systems Research Field in Numbers. *Informatica Economica*, *14*(4), 78–86.

Tang, C. S. (2006). Perspectives in supply chain risk management. *International Journal of Production Economics*, *103*, 451–488.

Tang, O., & Nurmaya Musa, S. (2011). Identifying risk issues and research advancements in supply chain risk management. *International Journal of Production Economics*, *133*(1), 25–34.

Thun, J.-H., & Hoenig, D. (2011). An empirical analysis of supply chain risk management in the German automotive industry. *International Journal of Production Economics*, *131*(1), 242–249.

Wagner, S. M., & Neshat, N. (2010). Assessing the vulnerability of supply chains using graph theory. *International Journal of Production Economics*, *126*(1), 121–129.

Wong, C. W., Lai, K.-h., Cheng, T., & Lun, Y. V. (2015). The role of IT-enabled collaborative decision making in inter-organizational information integration to improve customer service performance. *International Journal of Production Economics*, *159*, 56–65.

Wu, T., Blackhurst, J., & O'grady, P. (2007). Methodology for supply chain disruption analysis. *International Journal of Production Research*, *45*(7), 1665–1682.

Yao, A. C.-C. (1986). How to generate and exchange secrets. In *27th Annual Symposium on Foundations of Computer Science,* 162–167.

Yoon, J.-S., Shin, S.-J., & Suh, S.-H. (2012). A conceptual framework for the ubiquitous factory. *International Journal of Production Research*, *50*(8), 2174–2189.

Zhang, A. N., Goh, M., Terhorst, M., Lee, A. J. L., & Pham, M. T. (2013). An Interactive Decision Support Method for Measuring Risk in a Complex Supply Chain under Uncertainty. In *2013 IEEE International Conference on Systems, Man and Cybernetics,* 633–638.

Zhang, L., Zhang, Y., & Zhou, W. (2009). Floating-point to Fixed-point Transformation Using Extreme Value Theory. In *2009 Eighth IEEE/ACIS International Conference on Computer and Information Science,* 271–276.

Zhou, H., & Benton jr., W. (2007). Supply chain practice and information sharing. *Journal of Operations Management*, *25*(6), 1348–1365.

IV Results, Future Research, and Conclusion

This chapter contains the key findings of this doctoral thesis in Section IV.1 and an outlook on future research areas in Section IV.2. It also provides a short conclusion in Section IV.3.

IV.1 Results

The main objective of this doctoral thesis was to contribute to risk and return management in the context of digitized value networks. After motivating the relevance of appropriate risk and return management methods to successfully master the challenges of digitalization and digital transformation in the industrial sector, this thesis presented insights and approaches for the targeted transformation of companies affecting all levels of the enterprise architecture considering the three fields of action: digital business, digital transformation, and digital disruption.

Regarding return management, the research papers provide practical guidance for the targeted transformation of business models in the context of digital hybrid value creation and insights concerning the resulting impacts and challenges associated with the development of digital business models. Further, the research papers support the transformation process by analyzing and categorizing the potential benefits of digital technologies for smart manufacturing environments and by providing an investment decision support model by means of an Expanded Net Present Value approach utilizing real options for the evaluation of investments in flexible on-demand production capacity (Chapter II).

Regarding risk management, the research papers provide a novel modeling approach for smart manufacturing information networks as well as a risk assessment model for smart factory networks enabling the simulation and analysis of inherent IT availability risks. Further, a generic architecture for the management of systemic risk is presented providing strategic decision support in digitized value networks (Chapter III).

In the following, the key findings of the research papers of this doctoral thesis are presented. At the end, future research opportunities are discussed and a short conclusion is provided.

IV.1.1 Results of Chapter II: Return Management in Digitized Value Networks

Chapter II focusses on providing insights and appropriate approaches for return management in the context of digitalization and digitized value networks by examining three concrete

research topics: First, the impacts and resulting challenges associated with the development of digital business models in the context of digital hybrid value creation are investigated and practical recommendations for the targeted transformation of business models are derived (Section II.1). Second, the potential benefits of digital technologies in the context of smart manufacturing are analyzed by means of a structured literature review and categorized in an established framework for information systems (IS) benefits (Section II.2). And third, investments enabling the usage of flexible on-demand production capacity are evaluated with the help of a real options approach (Section II.3).

- In Section II.1, research paper P1 investigates impacts and challenges resulting from the development of digital business models in the context of digital hybrid value creation (Objective II.1). In this context, the primary goal, the thematic focus, and the characteristics of digital hybrid value creation of industrial companies and of innovative, data-based product-service bundles are presented. Based on a literature review, real-world examples, and five interviews with experts from leading companies in different key industries, the impacts and resulting challenges on business models are investigated and presented in a structured manner by means of the Business Model Canvas (BMC) as an established method for the representation and development of business models (Osterwalder and Pigneur 2010). As a first result, it can be stated that the development of data-based product-service bundles causes numerous impacts (and subsequently challenges) discussed in the following. First, the value proposition, and, thus, the core of value creation, increasingly shifts from the sale of physical products towards multiple, customer-specific solution offerings on the basis of multiple digital services. Accordingly, the complexity increases as multiple value propositions have to be tailored to individual customer preferences. Second, digital services require the development of new capabilities like software development and data analytics, new resources like cloud infrastructure, and the cooperation with value chain partners like cloud providers in increasingly interconnected, digital ecosystems. In sum, the development of data-based product-service bundles affects all segments of the business model. Thus, a holistic perspective on the overall business model is required in the course of digital transformation. To demonstrate the transformation of a business model, research paper P1 presents a case study based on the example of Mitsubishi Electric. Subsequently, as the last result of this research paper, recommendations for

practitioners are presented by proposing different starting points for the digital transformation of a business model. In this context, the central starting point for the development of digital service offerings should always be the customer and the customer problem as well as the establishment of a long-term customer relationship. Only by creating a real added value for customers, a long-term customer relationship and a sustainable win-win-setting can be created. Regarding the various possibilities for the design of new revenue sources and types, the complexity has to remain manageable in terms of transparency, and mutual benefits for both, providers and customers have to be ensured. Additionally, companies should seek the cooperation with value chain partners in closely interconnected digital ecosystems and pursue approaches like cocreation as companies are not able to build and maintain all necessary capabilities and resources by themselves. Summarizing, Section II.1 provides insights and practical guidance for the development of digital business models in the context of digital hybrid value creation.

- In Section II.2, research paper P2 investigates the anticipated benefits of digital technologies in the context of smart manufacturing enabling new business models and success practices and provides a structured overview of benefits by means of a benefits framework (Objective II.2). For this, a structured literature review was conducted in accordance with established methods for literature reviews in IS research (e.g., Bandara et al. 2011; Fettke 2006; Levy and J. Ellis 2006; Vom Brocke et al. 2009; Webster and Watson 2002). Based on a keyword search in different scientific databases, 57 scientific publications were selected for a full-text analysis resulting in a list of 365 obtained benefits. This shows the magnitude and diversity of benefits in literature and underlines the importance of a structured overview to support investment decision processes with a comprehensive picture. The obtained benefits were assigned to one of the four dimensions *operational*, *managerial*, and *strategic organizational* of an established framework for IS benefits initially proposed by Anthony (1965) and clustered to 21 benefits including, for instance, *production flexibility*, *resource efficiency*, or *product innovation & improvement*. The classification into one of the four dimensions supports the differentiation of the impact of benefits and, thus, facilitates their subsequent evaluation as the dimensions consider the hierarchical levels of decision-making in organizations. Despite the structured benefits framework as the central artefact of research paper P2, further insights and managerial

implications are derived in the course of the research. First, there are interdependencies between certain benefits as digital technologies applied to enable benefits on the operational level often times serve as the basis for the realization of benefits on the managerial or strategic level (e.g., the alignment of production to changing, individual customer demands requires the realization of production flexibility or an accelerated product development process). Second, the operational and managerial level are partly fading regarding certain benefits like utilization or problem handling as production systems are able to self-control the production process in real-time. This influences traditional planning processes and requires management to adapt managerial processes. Third, the gained results indicate that operational benefits of digital technologies might appear earlier, whereas strategic benefits might materialize on a longer time horizon. Accordingly, the comprehensive evaluation of benefits of digital technologies and the assessment by means of appropriate measures is of crucial importance for value-based management and the development of a sound digitalization strategy.

- In Section II.3, research paper P3 presents a mathematical model based on real options analysis in a discrete-time binomial tree model to evaluate investments enabling the commissioning of flexible on-demand production capacity in digitized production infrastructures (Objective II.2). The model economically evaluates upfront investments required for the commissioning of external capacity providers by means of an Expanded Net Present Value approach and integrates the value of the resulting volume flexibility. For this, a real options approach is applied as it is an established valuation method designed to capture flexibility of action and, thus, enables investment evaluations under uncertainty. Thereby, the approach models and evaluates the volume flexibility as an expansion option. Against the backdrop of increasingly volatile customer demand due to shorter product life cycles and changing customer preferences towards the instant availability of non-storable, individualized products, the approach supports investment decisions of companies in the context of production capacity planning. Based on the results, it can be stated that the possibility to commission on-demand production capacity can be of considerable value. Thereby, the conducted sensitivity analyses revealed that this holds true especially for longer framework contracts with external capacity providers. Further, insights gained by the sensitivity analyses include that the volatility of customer revenue is another strong

value driver for volume flexibility. Accordingly, flexible on-demand capacity is especially valuable for companies in fast-moving industries that exhibit ever shorter product life cycles, rapidly changing customer preferences, and, thus, highly volatile demand. Furthermore, the commissioning of non-permanent on-demand production capacity represents a valuable option for small and medium enterprises with rather limited investment budgets, as the commissioning of on-demand capacity requires smaller investment volumes in comparison to costly investments into new internal production capacities with amortization periods of several years. Summarizing, Section II.3 presents an approach for the sound economic evaluation of investments enabling flexible on-demand production capacity and, thus, supports the strategic decision making of companies in the context of their digital transformation.

IV.1.2 Results of Chapter III: Risk Management in Digitized Value Networks

Chapter III focusses on providing appropriate approaches for risk management in the context of digitalization and digitized value networks by examining two concrete research topics: On the one hand, approaches for the modeling and simulation of smart factory networks are developed that consider information networks and production networks, both exhibiting complex informational interdependencies. Thereby, it is demonstrated how these approaches can support management on analyzing inherent informational risks as a means for sound decisions on appropriate IT security strategies (Section III.1 and Section III.2). On the other hand, a generic architecture for a strategic decision support system for systemic risk management is presented and areas for future research are introduced (Section III.3).

- In Section III.1, the presented modeling approach contributes to the modeling and structured depiction of smart factory information networks and the simulation and analysis of IT availability risks (Objective III.1). For this, as a first result, design objectives for the development of an appropriate modeling approach are derived from literature. These include the formal and mathematical representation of information networks enabling a simulation-based analysis of IT availability risks and a graphical representation of the modeling approach enabling the transparent depiction of the modeled components. Further, the scalable depiction of components, subnetworks, and the entire information network should enable the inclusion of a varying number of information network components. And lastly, characteristics of different threats

including attacks and errors as well as corresponding propagation effects have to be captured. Based on these design objectives, six requirements for an adequate modeling approach are derived and petri nets, more precisely, stochastic generalized petri nets with immediate and exponentially distributed firing times, deterministic and stochastic preselection of transitions as well as guard functions, are selected as the basis for the modeling approach. Building on these results, a generalized modeling module for the depiction of single components and their interdependencies is developed as the central artefact. By means of this modularization approach, complex information networks can be modeled and simulated. Thereby, the modeling module is designed to enable different types of threat scenarios including timing failures, errors, and attacks as well as their propagation within the information network. To evaluate the developed modeling approach, different threats comprising a smart factory information network are simulated. Thereby, the data generated by the simulation regarding the states and the operational capabilities of the respective components can be used to analyze the information network and IT availability risks over time in more detail by means of key figures such as (operational) availability rates. Additionally, interviews with experts from both practice and academia are conducted to evaluate the modeling approach from a naturalistic perspective. In sum, the developed modeling approach facilitates the risk-oriented analysis of information networks and enables the analysis of different network design patterns regarding certain threat scenarios as well as the analysis of propagation effects regarding their occurrence and spread. This allows the identification of weak points and critical dependencies within the information network and, thus, provides insights for the sensible design of smart factory information networks, for instance, regarding the degree of interconnectivity, and the derivation of targeted IT security measures to reduce risks associated with IT availability.

- In Section III.2, a risk assessment model for the modeling of smart factory networks and the quantification of IT availability risks is presented that enables the identification of critical nodes and supports corresponding investment decisions in IT security measures (Objective III.2). For this, the general setting of smart factory network is abstracted first. This results in a basic structure consisting of two connected networks: information network and production network. Both networks contain different components like smart machinery equipped with embedded systems or servers and software components. As the production network depends on the reliability of the

information network and its components, there are direct and indirect functional dependencies within both networks and between them. Accordingly, smart factories contain diverse and complex dependency structures in which production components depend on various components of the information network regarding their functionality. The developed risk assessment model uses this dependency structure as the basis for the quantification of IT availability risks. For this, the smart factory network is modeled and formalized by means of graph theory and matrix notation, and the threat potential of each IT component caused by non-availability is quantified by means of Value at Risk under consideration of utilization rates, different interference degrees of IT components, and compensation effects in case of idle capacity. The applicability of the developed model is demonstrated through an exemplary real-world scenario in which different IT security measures are investigated regarding their risk reducing effects. Further, sensitivity analyses are conducted revealing that the criticality of IT components are determined by numerous influencing factors including the underlying dependency relations to production components, the degree of caused production interferences, the impact location in terms of process steps, the utilization of dependent production components, and the resulting possible compensation effect of unaffected production components. Accordingly, the variety of influencing factors in combination with the complex interdependencies in smart factory networks demands for structured approaches supporting investment decisions in the context of IT security strategies. For this, the developed risk assessment model presents an approach for the structured analysis of increasingly complex smart factory networks under consideration of not only direct but also indirect dependencies. It considers propagation and damaging effects caused by IT availability risks based on complex dependency structures. Accordingly, the presented risk assessment model provides risk-oriented guidance for the solid design of smart factory networks and an economic basis for corresponding investment decisions regarding IT security measures.

- In Section III.3, a generic architecture for a strategic decision support system for systemic risk management in digitized value networks is developed (Objective III.3). Against the backdrop of globalization and the digitalization of the industrial sector, companies are increasingly confronted with interdependencies and complexities within digitized value networks. At the same time, increasing systemic risks jeopardize companies as failures of distant value chain partners can disturb business operations

even in the absence of direct dependencies. However, complexity of value networks and the lack of transparency complicate risk management. A potential solution can be provided by decision support systems that extend the capabilities of existing risk management approaches by automatically gathering, processing, and analyzing information from manifold sources from inside and outside a company (inter-organizational information sharing). Accordingly, a generic architecture for such a decision support system as a template for future information systems is developed. As a first step, a functional design is presented that integrates a technological interface for external information sharing and gathering. The functional design is based on the established risk management processes containing the four phases for the observation and control of business operations. The four phases of risk management are extended by an external information management step that gathers and shares information with and about supply chain partners, digital services providers, and the surrounding environment, and that enables an automated information input stream. Accordingly, additional input information becomes available to identify, evaluate, and monitor systemic risk. Based on this functional design, a generic architecture for the decision support system containing different components is derived. The components include a monitor for the observation of internal and external information, unstructured and structured databases as well as a data warehouse. Further components like a document-driven component, a data-driven component, a knowledge-driven component, and a model-driven component facilitate the processing of information and the execution of qualitative and quantitative risk analyses. A central control module coordinates all components and is connected to the user interface module for human decision-makers. To develop and implement corresponding risk management information systems on the basis of the developed generic architecture, different challenges must be addressed by combining interdisciplinary knowledge from diverse research disciplines. These challenges include technological interfaces for external information sharing and gathering, information sharing incentives, database systems, data processing, risk modeling languages, risk assessment measures, and learning capabilities of risk management support systems. For each of these challenges, selected research questions are presented as orientation for future research.

IV.2 Future Research

To provide a concluding outlook on the research topics in this doctoral thesis, potential aspects for future research are highlighted for each chapter in the following.

IV.2.1 Future Research in Chapter II: Return Management in Digitized Value Networks

The limitations of research paper P1 that provide opportunities for future research regarding digitalization and digital transformation of business models are:

- The paper presents impacts and resulting challenges of the development of digital business models in the context of digital hybrid value creation on the basis of a literature review and five interviews with experts from companies in different key industries. These present a generic framework for the digital transformation of companies. However, due to the diversity of possible business models and the just beginning spread of digital business models in the industrial sector, this work does not represent a final view on the topic. To obtain a more complete overview on the impacts and challenges and to investigate the body of both scientific and practical literature in a structured manner, a structured literature review should be conducted as proposed, for instance, by Bandara et al. (2011), Fettke (2006), or Webster and Watson (2002). Additionally, further interviews with experts from various industries and companies of different sizes, especially small and medium companies, should be conducted to include practical insights that may only occur in specific industries or in companies with a specific size.
- The development and implementation of digital business models is an ongoing, iterative transformation process. Especially the question of when a business model can be described as "digital" remains a major challenge that cannot be clearly deduced solely on the basis of the research carried out in research paper P1, since the transition from traditional business models to digital ones appears to be rather fluid and is highly company-specific. Accordingly, this represents a starting point for future research and the development of corresponding approaches such as maturity models for assessing the degree of digitalization of business models to provide companies with further assistance in the transformation process.

Regarding the evaluation of benefits of digital technologies in the context of smart manufacturing, opportunities for future research based on the limitations of research paper P2 are:

- The structured literate review conducted in research paper P2 only included scientific literature. Accordingly, potential findings that are yet only included in practical-oriented literature and, thus, not considered by researchers, are not considered. To overcome this limitations and to include findings that might not been published in scientific literature due to timely review processes, future research should conduct a structured literature review including literature like white papers or real-world application case studies published in both scientific and practical-oriented publication media.
- With respect to interdependencies between different potentials and their realization, it would be valuable to comprehensively investigate cause-effect-relations of digital technologies and resulting benefits as well as causal relations among complementary benefits. This is especially important as benefits are often times only mentioned in literature for motivational reasons and are not set in context with concrete enabling technologies. For this, established methods from the field of benefits management like benefits dependency networks could serve as appropriate means (Peppard et al. 2007). This would present a comprehensive guidance for the targeted implementation of digital technologies and the development of robust transformation roadmaps in the course of a digitalization strategy.
- The development of appropriate measures for the ex-post assessment of ex-ante pursued benefits represents another aspect for future research. As benefits enabled by digital technologies are manifold and affect different aspects of an organization considering the four dimensions of the developed benefits framework, management is required to critically review and accompany the implementation of investments in digital technologies. For this, a robust system of key performance indicators should be developed that supports management in the ongoing evaluation of digital initiatives.

The limitations of research paper P3 that provide opportunities for future research regarding the evaluation of investments in the context of digitized production infrastructures are:

- The presented investment evaluation model only considers the resulting volume flexibility of flexible on-demand capacity as a benefit of the evaluated upfront investments. As these investments are likely to be made in innovative digital technologies like inter-organizational information systems or flexible and expandable production infrastructures, there might be further benefits that should be considered in the investment evaluation in correspondence to value-based management principles (cf. Section II.2). Accordingly, future research should aim on developing a holistic evaluation model for investments in the context of digital transformation.
- The presented model contains some assumptions that restrict its applicability. These include the assumption of infinite on-demand production capacity of external production providers that might not hold true in reality. Further, the model assumes constant internal and external production costs for the planning horizon and, thus, neglects the possibility of changing prices due to macro-economic or market developments affecting both input parameters.
- Finally, the model should be examined empirically with real-world data. So far, the model's application in the simulation was based on exemplary parameters as the provision of on-demand production capacity represents a new, still evolving business model lacking a widespread application in practice, yet. In this context, the parametrization of intervals and the selection of appropriate distributions should be investigated and based on real-world data to improve robustness of results.

Taken together, these potential research opportunities provide various starting points for further contributions toward enhanced return management in digitized value networks.

IV.2.2 Future Research in Chapter III: Risk Management in Digitized Value Networks

The major limitations that represent opportunities for future research regarding the modeling of smart factory information networks and the analysis of inherent information-based risks as shown in research paper P4 are:

- The modeling approach is restricted to the modeling and analysis of information networks and its components. Accordingly, and in contrast to the risk assessment model developed in research paper P5, it does not allow the explicit consideration of the production environment of smart factories. Therefore, future research should

investigate extensions that allow the consideration of production components such as smart machinery or products to analyze interdependencies between information networks and production environments in more detail. Moreover, extensions could include components of an information network that are not considered in the presented modeling approach like broken cables.

- As the developed modeling approach distinguishes between the four different operational states *operational*, *on hold*, *failed-after-attack*, and *failed-after-error*, it is not able to depict components with reduced functionality. Future research should focus on incorporating different intensities and propagation velocities of threats to extend the range of depictable threat scenarios and to include, for instance, the effectiveness and skills of an adversary.
- As interconnections within the information network contain both positive and negative effects, the identification of a sensible degree of interconnection in smart factories represents a major challenge. For instance, there is a tradeoff between increased flexibility and efficiency of production through enhanced interconnection and an increased vulnerability to IT availability risks as threats can spread due to informational interdependencies. Therefore, future research should develop approaches for the determination of a sensible degree of interconnection considering aspects of both risk and return management.
- In this regard, future research should develop appropriate methods for the quantification of economic loss potentials and expected benefits resulting from interconnection in smart factories as necessary steps towards the determination of a sensible degree of interconnection.

The analyses of IT availability risks in smart factory networks by means of the developed risk assessment model presented in research paper P5 comes along with the following limitations that represent areas for future research:

- The presented risk assessment model does not consider the possibility of negative, upward effects within the information network, for instance, in case a failing machine of the production network is not able to provide and share information regarding its operational status. However, this negatively affects the overall production system considering the real-time requirement regarding information synchronization.

Therefore, future research should extend the presented risk assessment model to incorporate unilateral effects of failing components.

- Although IT availability risks represent a highly critical threat for smart factories due to the importance of the information system for the proper functioning of the production infrastructure, the developed model does not allow the consideration of other dimensions of IT security risks such as confidentiality, accuracy, or access. As smart factories are also highly vulnerable to these risks, it would be beneficial to incorporate other dimensions of risks to enable a holistic perspective on IT security risks regarding the criticality of IT components.
- To improve the investment decision support regarding IT security measures, future research should develop an optimization model that addresses the tradeoff between risk-reducing effects of idle capacity and the accompanying costs under consideration of IT security risks as compensation effects enabled by idle capacity significantly influence the loss potentials of IT components' non-availabilities.
- The relaxation of some model assumptions would further improve the model's applicability. For instance, future research should extend the model to consider partial functional interferences of IT components as this could occur in some cases (e.g., data manipulations). Additionally, regarding the consideration of timing, future research should further develop the presented model to a continuous-time or discrete-time model as the current model only analyzes the effects of IT components' non-availability in a fixed time period.
- The model should be applied in different real-world scenarios to examine it empirically with real-world data. So far, the model was only applied in an exemplary scenario based on a close-to-reality setting to demonstrate its applicability and basic functionality. Through this, the parametrization of the required parameters and the gathering of the necessary data can be validated and tested in different real-world scenarios.

Regarding the developed generic architecture for a strategic decision support system for systemic risk management and the discussion of open challenges for future research presented in research paper P6, the aspects for future research are:

- Future research should investigate the gap between the developed generic architecture and the practical implementation of a risk management information system in more

detail. Thereby, especially the involvement of risk managers and practitioners are important to study requirements and use cases necessary for the development of a detailed design.

- The quantification of systemic risk remains a major challenge for research as missing, incomplete, or inaccurate information negatively impact the capabilities of future strategic decision support systems. Accordingly, future research should investigate the quantification of systemic risk and develop appropriate risk measures. For this, interdisciplinary research regarding systemic risks should be conducted especially by researchers from the field of quantitative risk management and IS.

Taken together, these potential research opportunities provide various starting points for further contributions toward enhanced risk management in digitized value networks, for instance, in respect to the dependencies of return and risk.

IV.3 Conclusion

Summarizing the research papers presented in Chapter II and III, this doctoral thesis contributes to the existing literature in Finance and Information Management by investigating specific aspects of risk and return management in digitized value networks. They especially investigate fundamental aspects of the digital transformation of companies affecting all levels of the enterprise architecture, address specific challenges regarding digital business models, digital transformation, and digital disruption, and provide approaches for investment evaluation and risk management. Although this doctoral thesis certainly can only answer some selected questions, it contributes to previous work in this area. As risk and return management will continue to play an important role in the course of the digital transformation of companies in all industrial sectors, this doctoral thesis hopefully can provide valuable theoretical and practical insights for some specific aspects of risk and return management in digitized value networks.

IV.4 References

Anthony, Robert Netwon (1965): Planning and Control Systems: A Framework for Analysis. Boston.

Bandara, Wasana; Miskon, Suraya; Fielt, Erwin (2011): A Systematic, Tool-supported Method for Conducting Literature Reviews in Information Systems. In Virpi Tuunainen (Ed.): Proceedings of the 19th European Conference on Information Systems. Helsinki, Finland, June 9–11, 2011.

Fettke, Peter (2006): State-of-the-Art des State-of-the-Art. In *Business & Information Systems Engineering* 48 (4), pp. 257–266.

Levy, Yair; J. Ellis, Timothy (2006): A Systems Approach to Conduct an Effective Literature Review in Support of Information Systems Research. In *Informing Science* 9, pp. 181–212.

Osterwalder, Alexander; Pigneur, Yves (2010): Business Model Generation. A Handbook for Visionaries, Game Changers, and Challengers. Hoboken, NJ: Wiley.

Peppard, Joe; Ward, John; Daniel, Elizabeth (2007): Managing the Realization of Business Benefits from IT Investments. In *MIS Quarterly Executive* 6 (1), pp. 1–11.

Vom Brocke, Jan; Simons, Alexander; Niehaves, Bjoern; Reimer, Kai; Plattfaut, Ralf; Cleven, Anne (2009): Reconstructing the Giant: On the Importance of Rigour in Documenting the Literature Search Process. In *Proceedings of the 17th European Conference on Information Systems*.

Webster, Jane; Watson, Richard T. (2002): Analyzing the Past to Prepare for the Future: Writing a Literature Review. In *MIS Quarterly* 26 (2), pp. xiii–xxiv.