Management of Security and Systemic Risk in IT Projects

Dissertation

zur Erlangung des akademischen Grades eines
Doktors der Wirtschaftswissenschaften der
Rechts- und Wirtschaftswissenschaftlichen Fakultät
der Universität Bayreuth

Vorgelegt von

Florian Guggenmos

aus Kaufbeuren

Dekan:	Prof. Dr. Jörg Schlüchtermann
Erstberichterstatter:	Prof. Dr. Gilbert Fridgen
Zweitberichterstatter:	Prof. Dr. Torsten Eymann
Tag der mündlichen Prüfung:	26. Oktober 2021

Copyright Statement

The following sections are partly comprised of content taken from the research papers embedded in this thesis. To improve the readability of the text, I omit the standard labeling of these citations.

Abstract

The steady advance of digitization is presenting organizations with significant challenges. Not only does it offer opportunities in the form of new business models and optimized business processes, but it also reveals new risks and points of attack, mainly through the increased use and storage of personal data. Organizations must, therefore, always ensure an adequate level of IT security and data security. Overall, this leads to a sharp increase in IT projects, which organizations have to manage individually and across the board as part of an IT project portfolio. However, since IT projects are generally not independent of each other, organizations must also manage these dependencies. These interdependencies mean that in such IT project portfolios, systemic risks must also be considered in addition to project-specific risks. Research and practice already know a few such systemic risk measures. However, not all of them are equally suitable for every organization. Therefore, the organizations must select suitable systemic risk measures based on the available data and the preferred target dimension.

This doctoral thesis aims to sensitize organizations to the interdependence of digitization and IT security and the resulting implications for managing systemic risks in IT project portfolios and to identify possible solutions. I mainly based this thesis on five research articles, which provide deeper insights into individual aspects of the topics covered in this thesis.

Table of Contents

Introduction

1.1 Motivation

Digitalization amplifies that 'information technology has become a critical success factor in many industries' (Wolf 2015, p. 1). Thus, in recent years, the importance of information technology (IT) has risen sharply. Gartner (2021a) forecasts that in 2021 the worldwide spendings on IT will increase by 8.4% to a total amount of 4 trillion US dollars.

On the one hand, digitization enables organizations to develop new business models and is associated with beneficial effects on the overall performance, competitive advantage, or organizational effectiveness and efficiency (Devaraj and Kohli 2003; Goldfarb and Tucker 2019). On the other hand, digitalization is commonly regarded as a double-edged sword for established businesses (Legner et al. 2017; Vial 2019). To capitalize on the numerous advantages of digitalization, organizations strive to develop IT capabilities enhancing their digital maturity (Röglinger et al. 2018), regarded as the process of digital transformation (Berghaus and Back 2016). However, digitalization also poses concomitant challenges for organizations. One challenge considers the rising concerns on IT security (Whitmore et al. 2015) and its costs. For example, IBM (2019) estimates the average cost of 3.92 million $ per data breach. Among other things, the COVID-19 pandemic and the associated increase in home offices have led to IT security taking on a more significant role. Gartner (2021b) estimates that total spending in 2021 on IT security and risk management will exceed 150 billion US dollars, an increase of 12.4% compared to 2020. Further, in the German industry, the damage caused by IT attacks between 2016 and 2018 amounted to 43 billion Euros (Berg and Haldenwang 2018). As a result, even small steps towards digitization will require adapting other areas as well. Vial (2019) points out that aligning digitalization and IT security still represents a significant challenge for organizations and therefore calls for research to investigate this interplay.

The mutual dependence on IT security and the economic pressure to increase digitalization results in the challenge of organizations to manage the increasing number of IT projects to maximize their economic benefits (Reyck et al. 2005). In recent years particularly disruptive technologies like blockchain or artificial intelligence fostered digitalization (Schweizer et al. 2020). Primarily the blockchain technology supports organizations in offering new innovative products and, at the same time, increases essential aspects of IT security due to the inherent properties of the blockchain technology (e.g., unchangeability and transparency) (Paper 2.1, Paper 2.2). However, in addition to these disruptive technologies, many other areas of digitization have a significant impact on the competitiveness of organizations. Especially during the beginning of the COVID-19 pandemic in early 2020, it became apparent that many organizations were not sufficiently digitalized. To contain the pandemic, organizations moved their operational business from the office to the homes. While some organizations were able to make this transition without any problems, others had to quickly implement digital solutions for collaboration (e.g., Microsoft Teams or Zoom) without neglecting their IT security standards and operating business (Barnes 2020). Besides, organizations whose product was previously hardly digital have increasingly turned to digital services (Barnes 2020). Therefore, the pandemic also rapidly in-

creased the number of IT projects, focusing on digitalization and IT security, that had to be processed in a short time.

Nevertheless, IT projects are associated with a high risk. The so-called 'Chaos Report' by the Standish Group (2018) emphasizes the prevalence of IT project failures and the importance of project management. According to this study, 64% of all IT projects are only partly implemented or even fail. Furthermore, Flyvbjerg and Budzier (2011) specify that approximately 16% of all IT projects exceed their budget by 200%. A survey by the Radar Group (2012) concludes that opaqueness arising from dependencies between various projects of an IT project portfolio is one reason for these budget overruns. Among others, projects depend on each other since they use the same infrastructure, require limited resources, or depend on previous projects' results. In practice, organizations must not consider IT projects as isolated since they are embedded in the organizations' IT project portfolio and the IT landscape (Beer et al. 2015). Thus, an IT project portfolio also interacts with different IT infrastructures, such as legacy systems, IT services, or applications (Paper 4). To consider these dependencies research regards IT projects as elements of complex IT project networks (Beer et al. 2015; Guo et al. 2019; Neumeier et al. 2018; Radszuwill and Fridgen 2017; Wehrmann et al. 2006; Wolf 2015). The interconnectedness in such complex networks can trigger cascade failures (Beer et al. 2015). Thus, the failure of one IT project can lead to additional failures in other dependent IT projects. So, the failure of one IT project may collapse an entire IT project portfolio, resulting in substantial financial losses or even bankruptcy (Beer et al. 2015; Wolf 2015; Paper 4). Research knows the phenomena of cascading failures in networks as systemic risk. Organizations must be aware of these risks and manage them. However, until today, literature only knows a few approaches to consider dependencies between IT projects and deliver corresponding risk measures (e.g., Beer et al. 2015; Ellinas 2019; Guo et al. 2019; Wolf 2015; Paper 4). The management of systemic risk in IT projects and project portfolios still represents a significant challenge for organizations and requires future research.

1.2 General Research Approach

In this doctoral thesis, I will illustrate how IT security and systemic risk interact and how organizations should consider and manage both domains within their IT project and IT project portfolio management.

The strategic alignment and focus of IT security and the management of systemic risk in IT projects represent the practical needs of organizations due to digitalization. Since digitalization has been the core discipline of Information Systems (IS) research (Legner et al. 2017), the question arises whether and how research on IS or Strategic Information Systems (SIS), a substream of IS (Buhl et al. 2012a), can contribute to relevant knowledge in order to solve these issues. SIS research faces the challenge that managerial or organizational behavior in practice often differs from academic expectations (Buhl et al. 2012a). For organizations, "in contrast to scientific research, the fact *that* a particular problem is solved typically outvalues the question of *how* a class of problems can be solved" (Buhl et al. 2012a, p. 174). To bridge this gap, IS research should collaborate with organizations.

While research focusing on the digitization of organizations in the international environment and especially the USA is known as IS research, in German-speaking coun-

tries, the term Wirtschaftsinformatik (WI) respectively Business Information Systems Engineering (BISE) has become established. However, Buhl et al. (2012b) stated that these existing communities, which both focus on IS research, have developed quite differently and can learn from each other. According to Buhl et al. (2012b), the BISE community differed significantly from the North American Information Systems (NAIS) community in their research approach. While the NAIS strongly focuses on building theory, it struggles to investigate practical implications. In contrast, the research of the BISE community draws substantial fundings from collaborations with organizations. However, it lacks in abstracting the results to contribute to scientific theory.

We can also observe this different focus on research by analyzing the established research methodologies in the IS and the BISE community. According to Buhl et al. (2012a) and Buhl et al. (2012b), Wilde and Hess (2007) stated that “while the Anglo-American discipline equivalent "Information Systems Research" (ISR) works rather behavioral-scientific with similar content orientation, the opinion is often held in the WI community that the German-speaking WI before its basic position strongly tends to construction-oriented methods such as, e.g., the creation and evaluation of prototypes” (Wilde and Hess 2007, p. 280). Based on a literature review Wilde and Hess (2007) concluded that ISR research completely avoids practically oriented research methods (e.g., prototyping, reference modeling, and action research). Case studies, as well as conceptual and formal-deductive analyses, are conducted in roughly equal proportions. ISR uses quantitative and qualitative empirical analyses and laboratory experiments much more frequently than the BISE community. However, I want to note that the analysis of Wilde and Hess (2007) only considered IS literature till 2004, and many things have changed since then.

In 2004, Hevner et al. (2004) established a design-oriented methodology, the so-called design science research (DSR), in the IS community. DSR focus on building artifacts based on a good mix of building theory and gaining practical implication as illustrated by the three cycle view of design science introduced by Hevner (2007). Hevner (2007) distinguishes relevance, rigor, and a design cycle. The relevance cycle ensures the artifact’s practical relevance by deriving design requirements from practice and evaluating the artifact using a field test. Supplementary, the rigor cycle requires grounding the artifact on existing research and finally contributing to the existing knowledge base by abstracting the results. Finally, the design cycle focuses on iterative design and evaluation iterations with practitioners by developing the artifact. Due to the focus on theoretical and practical implications, DSR also became an established research approach in the BISE community.

I focused my research on contributing to the BISE community. In addition to the abstract knowledge generation, I mainly investigated topics relevant to practice and developed solutions for their problems. Therefore, I focused on design-oriented research methods, like the already mentioned DSR. Besides, I also used Action Research (AR), which describes a cyclical process to investigate the organizational implications of theoretically derived practices (Baskerville and Myers 2004; Davison et al. 2012). DSR and AR pursue the same goal by combining theoretical and practical implications. Nevertheless, there is a broad scientific discourse about their similarities and differences (Järvinen 2007; Iivari and Venable 2009). Hevner (2007), for example, suggests using AR as a method to execute the field study as part of the relevance cycle in DSR.

1.3 Structure of the Thesis and Overview of Embedded Research Papers

The following section provides an overview of the structure of this thesis and briefly describes the five research papers that constitute its basis. Figure 1 depicts the embedding of the research papers. In this doctoral thesis, I will focus on how organizations should manage IT security in IT projects while they progress the digital transformation to ensure the strategic alignment of IT security to the level of digitalization. Further, I will illustrate that this alignment leads to more complex IT projects and IT project portfolios which induce systemic risk. Therefore, I will also address how organizations should manage systemic risk in IT projects and IT project portfolios to ensure a comprehensive and successful project and project portfolio risk management.

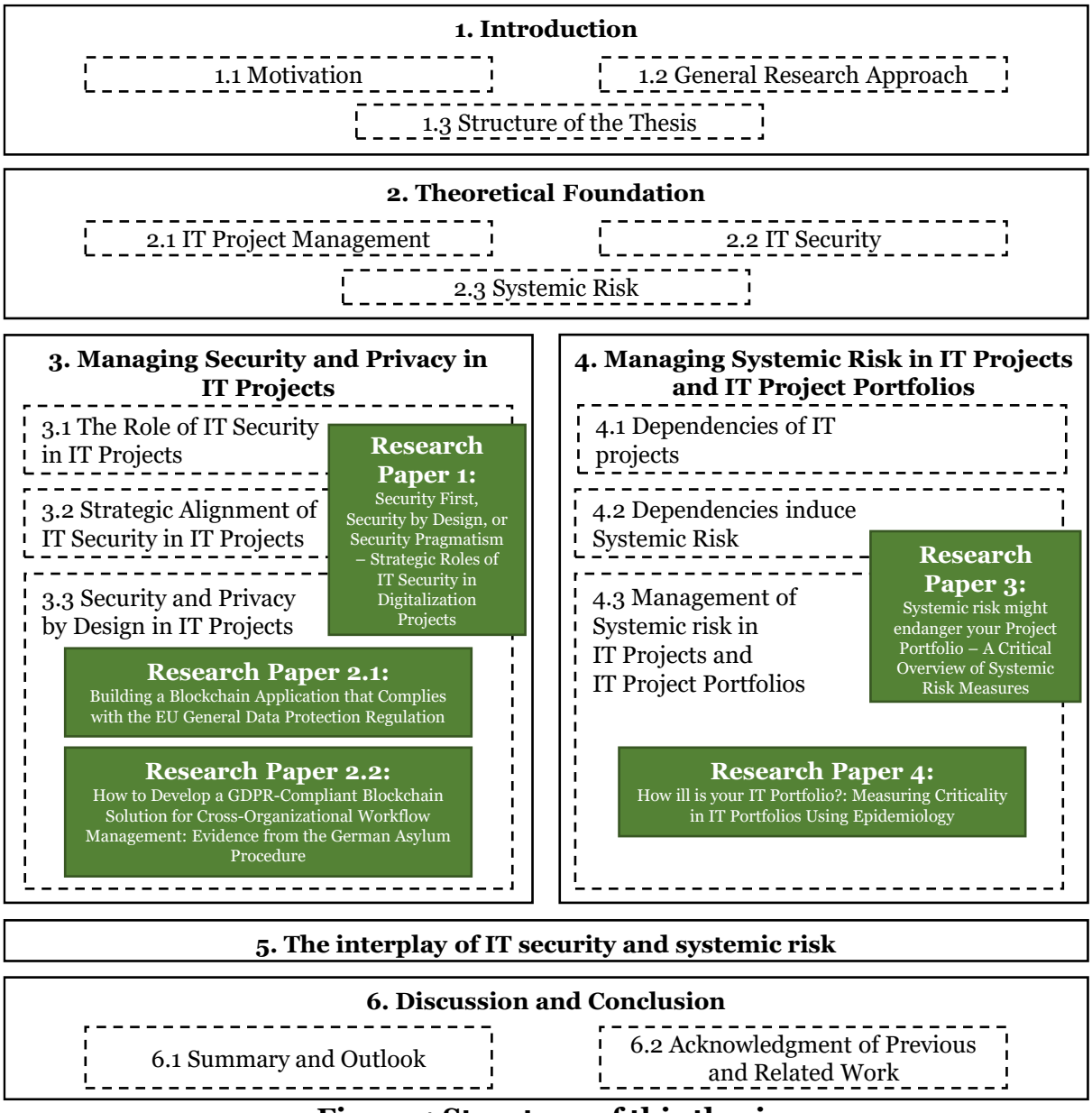

Figure 1 Structure of this thesis

The doctoral thesis is cumulative and refers to five research articles. The research papers provide insights into the context of IT security, data privacy, and systemic risk. The document at hand refers to these research articles in the different subchapters but does not contain them in full length. Figure 1 provides an overview of the order of the corresponding research articles and illustrates the embedment in the chapters of this thesis. The appendix contains detailed information and the extended abstracts of the research articles. In the following, I refer to each research article as 'paper'.

Following the introduction (section 1), section 2 provides theoretical foundations of IT security, IT project management, and systemic risk. In section 3.1, I illustrate that organizations progress digital transformation through IT projects and discuss how organizations should manage IT security and data privacy in these IT projects. Section 3.2 demonstrates possible ways to align IT security to the organization's level of digitalization. Based on that, section 3.3 focuses on security-by-design, one possible alignment path introduced in section 3.2 und Privacy-by-Design, which transfers the idea of security-by-design to data privacy. Section 3 illustrates that depending on the followed alignment path, considering IT security in IT projects may lead to a complex structure of IT projects or complex IT project portfolios due to dependent IT projects. Section 4.1 provides an overview of existing dependencies in IT projects and IT project portfolios. Section 4.2 points out that complex networks, like complex IT project portfolios, induce a special type of risk, namely systemic risk, due to the existing dependencies. Therefore, section 4.3 focuses on how to manage systemic risk in IT projects and IT project portfolios. To do this, first, I model IT projects and IT project portfolios as graphs (section 4.3.1), a subtype of complex networks, to illustrate their complexity. Based on that, in section 4.3.2, I point out the essential properties of systemic risk in IT projects and IT project portfolios, which differ significantly from systemic risk in other domains. Finally, section 4.3.3 provides an overview of existing approaches to managing systemic risk in IT projects and IT project portfolios. Thereby also briefly introduce three promising approaches and discuss their strengths and weaknesses. Section 5 closes the loop and discusses the interaction of IT security in It projects and systemic risk that occur during the implementation of these IT projects. In section 6, I finally discuss the insights of this doctoral thesis and the applicability of aligning IT security and managing systemic risk in practice. This section also concludes the contribution of the thesis and presents an outlook on future research.

While I listed the references in Section 7, Section 8 forms the appendix of the thesis, as it contains detailed information on the embedded research papers by providing, among others, the corresponding abstracts, respectively, extended abstracts. The supplementary material includes the full texts of all seven research papers (not for publication).

2 Theoretical Foundation

2.1 IT Security

During the last decades, IT security has evolved and gained managerial attention (Dor and Elovici 2016; Kane et al. 2015). It has become a strategic investment option (Cardholm 2016). The term 'IT security' basically refers to protecting the technical processing of information and information processing systems. However, today, IT

security is no longer limited to digital assets' bare security (Gordon and Loeb 2002). According to Saltzer and Schroeder (1975), IT security ensures three main principles: confidentiality, integrity, and availability. Literature knows these principles as 'CIA-triad' (e.g., Agarwal and Agarwal 2011; Mosenia and Jha 2016; Cherdantseva and Hilton 2013).

First, confidentiality aims to prevent unauthorized disclosure of information. Organizations ensure confidentiality through network security protocols, network authentication services, and data encryption services (Agarwal and Agarwal 2011). Second, in the context of IT security, integrity ensures that nobody alters the message in transit. Organizations can ensure integrity by firewall services, communication security, and intrusion detection (Agarwal and Agarwal 2011). Third, availability means to guarantee that information will be available to the consumer in a timely and uninterrupted manner when it is needed, regardless of the user's location. This means, for example, that the cloud infrastructure, the security controls, and the networks connecting the clients and the cloud infrastructure always run correctly. Organizations can ensure availability by fault tolerance, authentication, and network security (Agarwal and Agarwal 2011).

Research already addressed and discussed the insufficiency of the CIA-triad in the context of current requirements on IT security (e.g., Cherdantseva and Hilton 2013). Therefore, literature has refined and extended the CIA triad throughout the years in response to the constant and dynamic development of IT and IT security threats. Nevertheless, until today, there has been no agreed-upon set of goals exceeding the CIA-triad (Bitomsky et al. 2020).

Thus, among other things, technological development requires a continuous readjustment of IT security management to assess the opportunities and risks of digitalization. For instance, disruptive technologies like the Internet of Things (IoT), artificial intelligence (AI), or the blockchain technology and their implications on IT security drove research in this area on profound comprehension (e.g., Kankanhalli et al. 2019; Wang et al. 2019). Although IT projects do not necessarily contribute primarily to a more efficient IT security, they still offer an excellent opportunity to securely 'design in' cybersecurity to the IT components (Payette et al. 2015). Literature refers to this procedure as 'security-by-design' (Paper 1). Therefore, the discourse of IT security shifted its focus towards a holistic, managerial discipline called IT security governance (Rastogi and Solms 2004; Solms and Solms 2005). IT security governance not only covers bare technology as a driver of business security but takes into account human behavior, individual skills, and social factors (Ashenden 2008).

Further, the increasing digitalization leads to an increased amount of stored and processed data and an increased amount of stored and processed personal data. Therefore, organizations do not only have to secure their IT systems against unauthorized access. They also have to secure these data. Data security, a subarea of IT security (Paper 2.2), requires adequate protection of any data of any kind against loss, manipulation, and other threats from a technical point of view. Organizations must consider data protection regulations to protect this data against misuse (Paper 2.1; Paper 2.2). Analogous to Security-by-Design, Privacy-by-Design indicates an approach to design in data security while managing and implementing IT projects (Paper 2.1).

2.2 IT Project Management

The term ‘project’ has become part of everyday language and is used in various business areas (Wieczorrek and Mertens 2007). The Project Management Institute (PMI) defines a project as ‘a temporary endeavor undertaken to create a unique product, service or result’ (Project Management Institute 2017, p. 4) The International Project Management Association (International Project Management Association 2015) and, specifically for Germany, the DIN 69901 (German Institute for Standardization 2009) defines a project similarly. According to these definitions, each project aims to achieve a specific goal through coordinated activities while adhering to defined resources (e.g., personnel, budget, time) (Munns and Bjeirmi 1996). Literature uses the term ‘IT project’ for projects which aim to develop and implement software or IT infrastructure. Examples of IT projects are database restructuring projects and software development projects for business system applications (Beer et al. 2015). In the following, I will always refer to IT projects and use ‘project’ and ‘IT project’ as synonyms.

In practice and literature, different approaches exist that aim to control the achievement of the project objectives (Munns and Bjeirmi 1996). ‘Project management’ includes requirement analysis, resource allocation, progress planning, progress scheduling, progress monitoring, and deviation adjustment in terms of time and costs (Munns and Bjeirmi 1996; Project Management Institute 2017). Thereby, especially monitoring and analysis of deviations contribute to project risk management, which is an essential aspect of IT project management since efficient risk management has a significant impact on the success of IT projects (Bakker et al. 2010). According to the so-called risk management process, risk management aims to identify or analyze (potential) risks at an early stage, to evaluate them in terms of economic indicators, to control risks by taking targeted action, and ultimately to monitor them to improve future risk management (Project Management Institute 2017).

Literature and practice know various guidelines to manage projects adequately and to reduce their risks. Literature divides these guidelines into sequential and incremental (agile) methods. For example, the so-called waterfall model, introduced by Royce (1987), is a famous example of a sequential method widely used in government projects and many major organizations (Alshamrani and Bahattab 2015). It divides the development process into individual, fixed phases. The results of one phase always serve as binding guidelines for the next phase. Besides, each phase must be completed entirely before the next phase can start. In the basic model, it is not possible to steps back to previous phases. Royce (1987) concludes that implementing software based on a strictly sequential method is risky and invites failures. Therefore, Royce (1987) suggested allowing jumps back to previous phases. However, to step back, in most cases, means that the entire work of the current phase must be discarded. We can compare sequential methods with the process of physical projects like, for example, the construction of a building. In the beginning, we start with the foundation, followed by building the walls and finally the roof. But the walls and the roof depend on the foundation. This example makes it clear: It is even more critical and expensive to correct failure the later a faulty specification is detected.

Organizations also use sequential models to manage their IT projects. In this context, the same reasoning applies. In case of incorrect assumptions or ambiguities which become known in late phases during the analysis phase, organizations often must abort a project to limit the damage (Alshamrani and Bahattab 2015). Sequential pro-

ject management is particularly critical in extensive software development projects since a complete run-through of the waterfall model can take several years, and it is not possible to react sufficiently to changing requirements.

However, the requirements of various stakeholders can change continuously, especially in IT projects (Zowghi and Nurmuliani; Cao and Ramesh 2008). For this reason, the use of agile project management methods in IT projects increased significantly in recent years. The probably best-known representative of agile process models is Scrum. In agile methods, the project timeframe is fixed, but the result is variable. (Schwaber and Beedle 2002). While using Scrum, project teams develop fully functional (intermediate) results (called increment) in each iteration. In doing so, they can consider new or adapted requirements in the next iteration. Therefore, agile project management contributes significantly to risk reduction. For more details about agility and Scrum, I refer to Conboy (2009) and Schwaber and Beedle (2002).

2.3 Systemic Risk

Risk management is an essential aspect of successfully managing digitalization and IT security projects (Bakker et al. 2010). However, literature knows various definitions of 'risk'. Therefore, depending on the case of application, it is useful to define it differently. For example, March and Shapira (1987) define risk as 'reflecting variation in the distribution of possible outcomes, their likelihoods, and their subjective values'. According to that, in the context of IT project management, we can define risk as an unexpected event or a failure in a project that results in only partially successful implemented or even wholly canceled projects. In the following, I will use the term 'failed' for both cases (partial success and canceled). However, the question arises whether and how the risk of one project can affect the risk of other projects in case the projects depend on each other.

The existence of dependent elements leads to complex networks. A complex network describes a specific network type (Paper 4), mostly represented by graphs, that is neither random nor regular (Strogatz 2001). Complex networks consist of nodes and edges. These edges can be directed or undirected and describe an existing dependency between two nodes (start and end nodes). Three of the most represented complex networks in literature are random networks (Erdős and Rényi 1960), scale-free networks (Barabási and Albert 1999; Barabási and Bonabeau 2003) and the so-called small-world networks (Watts and Strogatz 1998). Since the detailed properties of these networks are not relevant for this thesis, I refer to Erdős and Rényi (1960), Barabási and Albert (1999), Barabási and Bonabeau (2003), and Watts and Strogatz (1998) for more details.

In such complex networks, there exists a specific type of risk, called 'systemic risk', which arises due to the existing dependencies. Systemic risks became popular the first time, especially during the financial crisis, and are well investigated in the financial sector (e.g., Freixas et al. 2000; Acharya et al. 2017; and Eisenberg and Noe 2001). In the financial sector, complex networks represent financial institutions (nodes) and their dependencies (edges) to other financial institutions, e.g., through lending and other business relationships. According to Kaufman and Scott (2003), the term 'systemic risk' refers to 'the risk or probability of breakdowns in an entire system, as opposed to breakdowns in individual parts or components, and is evidenced by comovements (correlation) among most or all the parts' (Kaufman and

Scott 2003, p. 371). We know these phenomena from the shock of Leman Brothers, whose bankruptcy caused an enormous effect for several other banks and triggered a domino effect. Literature knows this kind of domino effect as 'cascade failure' (Ash and Newth 2007). Although this definition refers to the financial system, we can also observe systemic risks in other types of networks. For instance, we also observed such domino effects during the COVID-19 pandemic when the initial infections of only a few people led to a global pandemic.

In contrast to a 'simple' failure in a network, which only leads to the failure of the element affected, cascade failures 'can trigger a recursive process of error cascades, which [...] can completely fragment networks' (Huang et al. 2011, p. 2). Figure 2 illustrates a schematic view of a cascade effect.

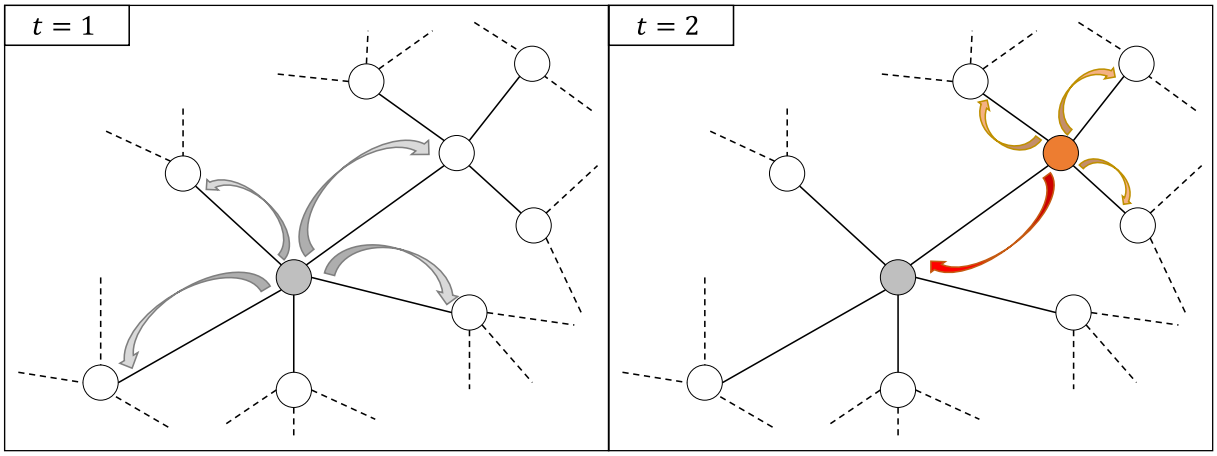

Figure 2 Schematic illustration of cascading effects based on Wang and Rong (2009)

In $t = 1$, a failure or a targeted attack on a node (illustrated as a white dot) leads to its failure (grey dot). Since the nodes depend on each other, this failure can also affect other nodes (grey arrows). In the case that a dependent node can compensate for this failure, no error cascades occur. However, if there is at least one dependent node that cannot handle the failure, it will fail, too (orange dot in $t = 2$), and the failure cascade starts (orange arrows in $t = 2$). If we assume that a node does not fail entirely but only reduces its performance, the node affected in $t = 2$ can also weaken the initially affected node (red arrow). Thus, these two nodes may weaken each other until one or both suffer a total failure. This cascade effect continues to spread until the entire network is affected, or the effect can be stopped at some point. The domino-like spread of the error demonstrates that systemic risk measures not only have to consider directly dependent elements but also their dependent elements. Literature knows these dependencies as indirect or transitive dependencies.

Literature investigated systemic risk measures that regard these indirect dependencies in different areas. For instance, we can find so-called cascade failure models, for example, in the area of critical infrastructures. Buldyrev et al. (2010) and Gao et al. (2011) introduced an algorithm that simulates cascade failures in power grids considering interdependent networks (networks of networks). Ash and Newth (2007) introduce a general cascade failure algorithm used for network analysis in various fields, for example, supply chain networks. In social research, Watts (2002) introduced an algorithm that, as one example, can simulate the spread of innovations within a population. In epidemiology, Kermack and McKendrick (1927) introduce a model

considering cascade effects to simulate the spread of diseases within populations. Also, Brockmann and Helbing (2013) introduce an approach to model the spread of diseases as a kind of systemic risk complex network. In context of IT security Miehle et al. (2019) and Bürger et al. (2019) analyze the spread of cyber-attacks in digitalized manufacturing organizations (smart factories). Besides, literature also uses other measures, e.g., centrality measures, to analyze systemic risks in different fields. Nevertheless, in the context of IT projects and IT project management, research on systemic risk (measures) is still in its infancy (Paper 4). For a detailed analysis and review of existing systemic risk measures in this field, I refer to section 4.

3 Managing Security and Privacy in IT Projects

3.1 The Role of IT Security in IT Projects

Since the ongoing digitalization requires a continuous readjustment of management to assess the opportunities and risks of digitalization, research and practice do not limit IT projects to the development of new software solutions or digital business models. In the context of digitalization, I refer to IT projects, as they include the use of digital technologies to create added value and are primarily driven by business. Therefore, in such projects, IT primarily plays an enabling role (Paper 1). This facilitates new, profitable business models that avoid differentiation purely based on price (Pozzi et al., 2021).

However, the increase in digitalization results in an increasing strategic importance of IT security due to a higher susceptibility to IT incidents (Paper 1). Therefore, many IT projects pursue improving IT security management (Payette et al. 2015; Kane et al. 2015; Dor and Elovici 2016; Cardholm 2016). I refer to such projects in the following as IT security projects, a subtype of IT projects. Nevertheless, the question of how to strategically address IT security within digital transformation remains unsolved (Drugescu and Etges 2006; Vial 2019).

IT security governance is one possible solution to address this backdrop. It ensures a holistic direct-control cycle linking managerial directives and strategy with executing procedures and vice versa (Solms and Solms 2006). Further, it enables the strategic alignment of IT security with business objectives (Williams 2001; Johnston and Hale 2009). In practice, organizations have to create congruence strategic alignment between their business strategy and their IT strategy (Chan and Reich 2007) appropriate to their industry and market environment. IS literature proved the strategic alignment of IT by effective governance mechanisms as an essential driver of organizational performance (Weill and Ross 2004; Harguem et al. 2014). To ensure that organizations can act efficiently in the market, IT projects aiming to increase digitalization must be aligned with organizational goals. Harguem et al. (2014) argue that, therefore, the strategic consideration and the urgency for the alignment of IT security have been fueled. Grahn et al. (2021) state that the postponement or even the deliberate omission of IT security requirements may gear up digitalization projects. Thus, organizations need to establish adequate business strategies that balance digitalization's positive effects with IT security demands and efforts and provide an integrated view of how both design dimensions interplay (Bharadwaj et al. 2013). Following Bowen et al. (2007), IT-related decision-making can be an essential part of the IT governance mechanism to achieve strategic alignment (Wu et al. 2015).

However, organizations have various reasons to improve their IT security. On the one hand, Dor and Elovici (2016) note that various cyber and non-cyber events trigger discrete actions to improve IT security. Heidt et al. (2018) state that behavioral, cognitive, organizational, economic, and environmental aspects also influence organizational decisions on IT security. Furthermore, non-obligatory factors such as competitive advantage or end-user expectations shape the decision-making landscape and strategic options (van Niekerk and Naidoo 2014; Weishäupl et al. 2018).

I have illustrated that various drivers can encourage organizations to improve their IT security and that IT security governance is a key factor in this process. However, the question of how IT security is aligned with the organization's specific level of digitization and taken into account in individual IT projects is still unresolved.

3.2 Strategic Alignment of IT Security in IT Projects

Projects must consider IT security in an appropriate way to ensure top management support. However, the interplay between IT security and the progress in IT projects may include a trade-off. Zhang et al. (2019) pointed out that the employment of mature IT service providers may suffer from legal cybersecurity requirements on a state- and industry-level. In this regard, IT security measures may slow down digitalization (Paper 1). IT security projects consume time and money, which hinders the agility and speed that are required for digital transformation. Thereby, even in the same industry, organizations choose different approaches to meet these requirements and to design the digital transformation path concerning IT security (Paper 1). However, in the end, organizations must improve both aspects. In theory, there are three approaches to the strategic interplay of digitalization and IT security that create congruence between the business strategy and IT security. According to paper 1, I refer to these alignments in the following as ‘alignment paths’ and substantiate their existence.

Organizations can prioritize IT security in IT projects or even neglect it. According to paper 1, I refer to the strategic alignment by prioritizing IT security as ‘Security First’ (SF) and to the strategic alignment by mostly neglecting IT security requirements as ‘Security Pragmatism’ (SP). The two alignment paths SF and SP, describe a temporary postponement or prioritization of IT security based on the corporate strategy and context (Paper 1). The phenomenon of deferring software obligations to a later date by prioritizing is not new in literature. Cunningham (1993) introduced the ‘technical debt’ metaphor in software engineering. It characterizes ‘software maintenance obligations that need to be addressed in the future’ (Ramasubbu and Kemerer 2016, p. 1487).

First, the alignment path SF reflects a prioritization of IT security to meet high standards of IT security requirements. In the project context, SF sets security as a maxim for action to be addressed in the early phases of projects, as recommended by Dooly et al. (2015). Hovav and Gray (2014) confirm the importance of high IT security requirements by showing the large negative impact security breaches can have in certain industries, e.g., banking. Especially highly interconnected supply-chain networks are very vulnerable and suffer from the risk of disruption (Paper 1). Therefore, IT Security plays a significant role in these value-creation networks (Smith et al. 2007). In particular, increasing complexity in smart factory networks leads to increasing demand for IT security on an inter-organizational level (Häckel et al. 2019). For indus-

tries in which IT security possesses a strategic role, one organizations' investments in IT security may, following the observations of Jeong et al. (2019), positively affect the security of the whole industry. This leads to free-rider problems and hence reduces the incentive compatibility of a single organization to invest. Furthermore, we could observe standards and norms for IT Security becoming established, e.g., to prove trustworthiness to stakeholders. Nevertheless, Hsu et al. (2016) point out that security standards (e.g., ISO 27001) positively affect organizations' performance since the industry considers good IT security management obligatory instead of competitive advantage.

Second, the alignment path of SP represents the deferral of IT security measures to later project phases or the reduction of IT security requirements to a minimum. This strategy may lead to competitive advantages in the early stages of the innovation process (Jonker and Petković 2013) and, therefore, may be associated with innovation projects. Nevertheless, SP may also lead to an accumulation of technical debt (Paper 1). However, technical debt in the area of IT security can hinder reliability, which may lead to immense costs in case of an incident (Izurieta et al. 2018; Keller et al.). The resulting weaknesses represent security risks with an exceptionally high potential for damage.

Third, as organizations strive to progress in both areas simultaneously, and according to Payette et al. (2015), who suggested to 'design in' cybersecurity to the IT components, a synergetic development of IT projects and an adequate IT security standard creates the last alignment path. By following the 'Security-by-Design' (SbD) path, organizations focus on the harmonious development of both areas (Paper 1). SbD aims to address security continuously throughout all project phases (Paper 1). This approach can also be found in the scientific discourse (e.g., Payette et al. 2015) by developing strategies on how IT security can be integrated into IT project management. The overall objective of early-stage involvement and the endeavors is to develop a shared language and create a widespread understanding of security requirements in line with general IS strategic alignment (Preston and Karahanna 2009). In addition to that, some digital technologies provide security as an inherent feature. For instance, the Distributed Ledger Technology (DLT) respectively, the blockchain technology achieves security through the underlying technology and its properties (Eschweiler 2018; Kshetri 2017).

3.3 Security and Privacy by Design in IT Projects

After I focused on the consideration of IT security regarding exclusively technical components, in the following, I will briefly discuss how to align digitalization and the security of stored and processed data, from now on referred to as 'data privacy'.

IT projects are usually faced with the challenge that new or larger amounts of data must be processed. If this involves personal data in accordance with the GDPR or other regulations, these must be specially protected (Paper 2.1; Paper 2.2). For this thesis, I focus only on the GDPR and neglect other data regulations. Paper 1 identified SbD as the most economically appropriate approach to IT security. In addition, Papers 1.1 and 1.2 deal with blockchain technology, which is a prime example of SbD due to its inherent properties.

Blockchain is a transparent, transactional, distributed database structure that stores data decentrally in a peer-to-peer network (Glaser 2017). The blockchain groups this data into blocks and cryptographically "chains" them together in chronological, structured order (Schweizer et al. 2017). A so-called consensus mechanism determines the correct order of transactions (in the blocks) as well as the correct order of the blocks (in the "chain"). Cryptography and consensus mechanisms together ensure reliability, validity, and trust (Christidis and Devetsikiotis 2016; Porru et al. 2017). The resulting immutability of data enhances integrity and security (Fridgen et al. 2018b). For a detailed description of blockchain, I refer to Nakamoto (2008), Avital et al. (2016), and Schweizer et al. (2017).

While design and cryptography are the keys to IT security, the privacy of the data stored in the blockchain remains an unresolved issue (Paper 2.1; Paper 2.2). For example, the data in the Bitcoin blockchain, probably the best-known blockchain, is safe from modification or manipulation but can be read by any participant in the blockchain network. The Bitcoin blockchain, therefore, uses anonymization to ensure data privacy. However, if the anonymization is compromised, all data is freely available. This is in part contrary to the principle of confidentiality of the CIA-triad. In addition, the properties that support IT security, first and foremost immutability, are a clear contradiction to the requirements of the GDPR, which ensures, among others, the right to rectification (Article 16) and the right to erasure ("the right to be forgotten") (Article 17). In the following, I will focus on these two rights. For a detailed analysis of the challenges for blockchain projects due to the GDPR, I refer to paper 2.1 and paper 2.2. Both papers address this issue in the context of an IT project of Germany's Federal Office for Migration and Refugees (BAMF) which aimed to design a cross-organizational blockchain solution to support the German asylum procedure.

Due to the immutability of blockchain, data stored in it can only be changed or deleted by the consensus of all participants. However, this contradicts the fundamental blockchain principles and is challenging to realize in practice (Paper 2.2). To ensure data privacy while using blockchain technology, organizations do not only have to follow the SbD principle but also the Privacy-by-Design (PbD) principle. Analogous to SbD and according to article 25 of the GDPR, PbD aims to address data privacy continuously throughout all project phases by considering technical constraints (Paper 2.1).

The BAMF solved this issue by developing a three-staged architecture that connects the organizations' back-end systems to the cross-organizational blockchain, among other things using a so-called privacy service. For more details on the BAMF's blockchain architecture, I refer to paper 2.1 and paper 2.2. Paper 2.1 finally states the three following design principles for GDPR compliant blockchain solutions:

1. Avoid storing personal data on a blockchain.
2. A blockchain solution that needs to process personal data should use a private and permissioned pseudonymization approach.
3. A blockchain solution that needs to coordinate cross-organizational workflows should use a private and permissioned pseudonymization approach with identifier mapping.

Although these design principles refer to blockchain solutions, these design principles are also valid for other technologies and, in general, for SbD IT projects since they require thinking on elementary subjects of data privacy.

4 Systemic Risk in IT Projects and IT Project Portfolios

4.1 Dependencies of IT projects

Considering IT security and data privacy in IT projects results in many tasks, (sub) projects, or different projects that depend on each other. Therefore, organizations must manage simultaneous or successive projects as part of an IT project portfolio (Engwall and Jerbrant 2003). According to Reyck et al. (2005), IT project portfolio management considers all IT projects an organization is engaged in. In 1952, Markowitz coined the term 'portfolio management' by investigating the optimal mix of risk and return in financial investments (Markowitz 1952). In 1981, McFarlan (1981) addressed portfolio management in IT projects, probably for the first time. For a detailed overview of the history and deployment of IT project portfolio management, I refer to Reyck et al. (2005).

Research in IT project portfolio management mainly focuses on strategies for composing project portfolios (e.g., Conforto et al. 2014; Englund and Graham 1999) and resource allocation between simultaneous projects (e.g., Hendriks et al. 1999; Engwall and Jerbrant 2003; Gordon and Tulip 1997; Laslo and Goldberg 2008). In this thesis, I focus on assessing risks in IT project portfolios as an essential but so far less investigated aspect to prevent unexpected failure of projects and project portfolios, according to McFarlan (1981).

Project risk management essentially involves managing the uncertainties and risks of individual projects failing or not being completely successful (Ward and Chapman 2003). Effective risk management can prevent projects from exceeding budget, falling behind schedule, missing critical performance targets, or exhibiting any combination of these troubles (Carbone and Tippett 2004). However, besides project inherent risks due to individual failures, the project also induces risk due to interdependent tasks or IT projects within an IT project portfolio. On the one hand, IT projects of an organization compete for limited resources, such as specially skilled personnel, budget, or specific hardware (Laslo 2010; Laslo and Goldberg 2008; Lova et al. 2000). On the other hand, some projects base on the results of previously implemented projects. Therefore, IT projects depend on each other and should not be considered isolated but rather as elements of interconnected IT project portfolios (Beer et al. 2015; Neumeier et al. 2018; Radszuwill and Fridgen 2017; Wolf 2015). The same argumentation is also valid within a single project, where subtasks can depend on each other. This seems to be evident in traditionally managed projects. For example, in the waterfall model, phases are directly dependent on each other, and a delay in the current phase may lead to a delay of the following phase. Agile project management usually prevents such dependencies since it provides functional increments in each iteration. However, there is a risk that the parallel development of several user stories may lead to a shortage of limited resources, which in turn leads to dependencies. Therefore, the question arises of how tasks and projects depend on each other.

While some literature focused on certain types of dependencies (c.f. Lee and Kim 2001; Santhanam and Kyparisis 1996; Tillquist et al. 2002 Zuluaga et al. 2007), others presented a framework of different dependencies (c.f. Wehrmann et al. 2006; Zimmermann 2008). Literature often distinguishes between intra-temporal and inter-temporal dependencies (e.g., Beer et al. 2015; Wehrmann et al. 2006). Thus, in-

tra-temporal dependencies describe dependencies within one step of time (both projects run simultaneously). Inter-temporal dependencies describe dependencies between different time steps (one project ended before the other started). For instance, Beer et al. (2015) provided a more detailed subdivision of intra-temporal and inter-temporal dependencies (see figure 3).

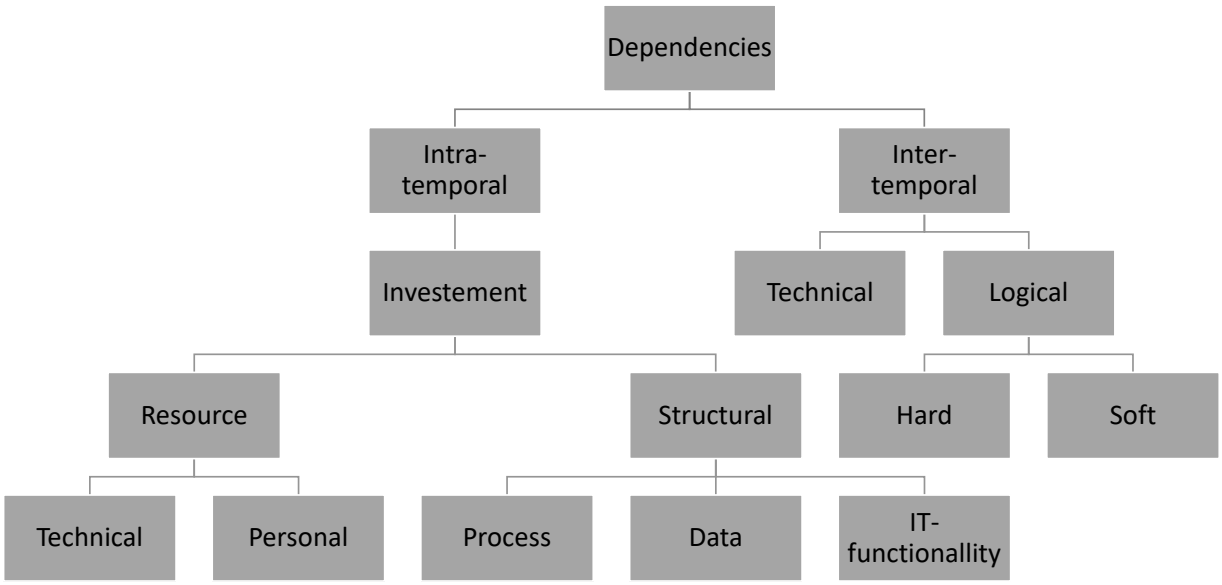

Figure 3 Types of dependencies in IT Portfolios (Beer et al. 2015)

According to Beer et al. (2015), technical and personal dependencies consider the competition of limited resources. For example, personal dependencies arise if only a few people in the organization have expert knowledge in a specific area. If two projects need this knowledge simultaneously, but only one expert is available, one or both projects may be delayed due to shared resources. Likewise, an unplanned absence of this person (e.g., due to illness) would cause a delay in both projects. In addition to the risk of personal dependencies, however, organizations may also gain an advantage by staffing the expert on both projects if the knowledge from one project leads to the fact that the work in the other project can be done more efficiently. Literature knows such positive effects as synergies (e.g., Radszuwill and Fridgen 2017). This thesis does not focus on synergies since negative effects are the primary driver of portfolio risk management (Häckel and Hänsch 2014). Therefore, in the further course of this thesis, I refer to the term 'dependencies' as the negative effects of dependencies and not to synergies. However, the question arises of how these dependencies induce project and project portfolio risk.

4.2 Dependencies induce Systemic Risk

For a long time, risk management in IT project portfolios focused on balancing the overall risk and return of the IT project portfolio, considering direct dependencies (Paper 4). According to Neumeier et al. (2018), literature knows multiple approaches, further called risk measures, for project and project portfolio planning (Hans et al. 2007) considering aspects of uncertainty, dealing with rare resources (Laslo 2010;

Lova et al. 2000), or both (Laslo and Goldberg 2008). Other risk measures apply scoring models (Lucas and Moore 1976; Walter and Spitta 2004) or established measures from other fields, like the balanced scorecard (van Grembergen and Haes 2005), to evaluate the risk of IT projects. For instance, Anbari (2003) applied the so-called earned value analysis to continuous control IT projects. In terms of project portfolios, Ghasemzadeh and Archer (2000) used linear programming, and Lee and Kim (2001) applied goal programming to provide decision support in finding an optimal project portfolio. However, these papers usually neglect the specifics of IT projects and IT project portfolios, such as transitive interdependencies.

For instance, Radszuwill and Fridgen (2017) and Neumeier et al. (2018) point out that it is essential not to limit risk management to the overall risk of a portfolio based on direct dependencies but also to consider individual project criticality and transitive dependencies. Radszuwill and Fridgen (2017) emphasize that a project, which has individually low risk but (transitively) depends on other projects can lead to a cascading failure of the entire IT project portfolio. Due to the direct and indirect dependency between IT projects, we can also observe the effects of systemic risks in IT project portfolios. In accordance with Paper 3, I want to illustrate a simplified example of inter-temporal transitive dependencies in IT project portfolios. In project 1, the organization implements a new database, which is the basis for project 2. Finally, projects 3 implements a customer application based on this web service. Therefore, the failure of project 1 will not only directly affect project 2 but also indirectly project 3.

Until today, literature has not fully investigated the impact of transitive dependencies, respectively, systemic risks in IT portfolio management. In recent years IS and project management literature transferred knowledge from other areas (e.g., critical infrastructure analysis, supply chain management, epidemiology, and social networks analysis), where systemic risks are well investigated. However, the transferred risk measures focus on different aspects of systemic risks. On the one hand, they focus on analyzing the overall risk of the IT portfolio (e.g., Beer et al. 2015) by considering direct and indirect dependencies. Organizations can use these risk measures to design IT project portfolios following the IT portfolio management objectives regarding project selection and project prioritization to minimize possible cascade effects. On the other hand, systemic risk measures in IT project portfolio management focus on analyzing the criticality of individual IT projects (e.g., Neumeier et al. 2018; Wolf 2015; Paper 4). These papers aim to identify critical projects with an exceptionally high impact on other projects or a high damage potential for the entire IT project portfolio. IT project portfolio management should aim to manage these projects with special care.

4.3 Management of Systemic risk in IT Projects and IT Project Portfolios

4.3.1 Modeling IT Projects and IT Project Portfolios as Graphs

To analyze the effects of systemic risk in projects and project portfolios, we must abstract and model projects and project portfolios in a first step. Literature knows several approaches to do this. Thus, the question arises of which approach should be

used to manage systemic risk. According to Geraldi and Lechter (2012), Tereso et al. (2019), and White and Fortune (2002), Gantt charts, for example, are a widely used model in practice. However, Gantt charts primarily consider temporal aspects and neglect others. Project management uses Gantt charts to organize different tasks within a project (e.g., milestone planning) rather than to manage systemic risks since they do not provide sufficient information, at least on direct and indirect dependencies (Paper 4). To solve this issue and due to the better visualization of the direct and indirect dependency of individual tasks or projects, literature suggests using graph theory to model projects and project portfolios (Beer et al. 2015; Radszuwill and Fridgen 2017; Ellinas 2019; Neumeier et al. 2018; Paper 3; Paper 4).

Graphs consist of nodes and edges. In terms of projects and project portfolios, literature models tasks, subprojects, or projects as nodes and dependencies as edges. Paper 4 illustrates that for simple cases, Gantt charts can be transformed into graphs (Figure 4).

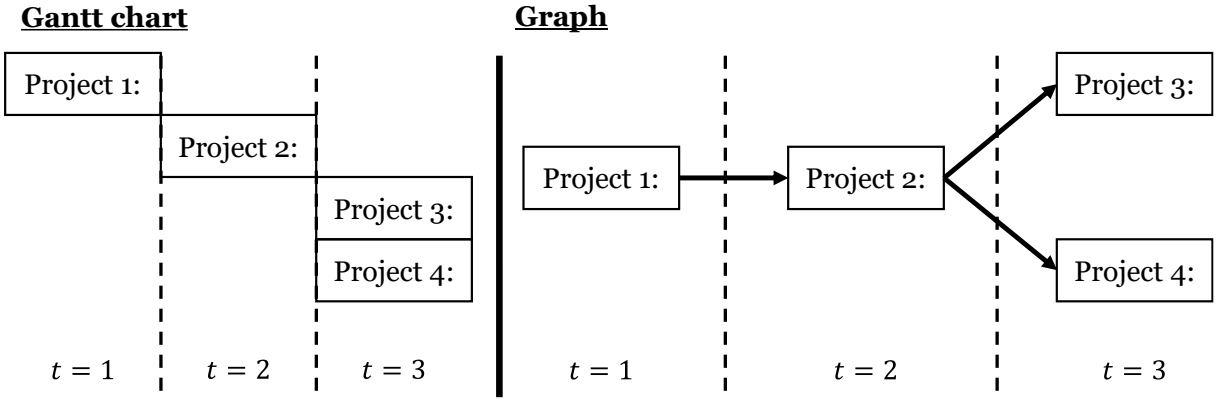

Figure 4 Schematic illustration of a project portfolio modeled as Gantt chart and graph (Paper 3)

Graphs can consider different types of nodes and edges. Due to its greater relevance, in the following, I briefly focus on modeling different types of dependencies using different types of edges. For example, Beer et al. (2015) distinguish between intra-temporal and inter-temporal dependencies. While inter-temporal dependencies are directed, since you cannot change the past, intra-temporal dependencies can be directed or undirected representing non-directional dependencies (Beer et al. 2015; Paper 3). By modeling dependent tasks and projects using graphs, literature mainly models non-directional dependencies as undirected edges or double-sided arcs and unidirectional dependencies as directed edges, respectively arcs. However, different risk measures interpret the direction of dependencies differently. In figure 4, the directed edge from project 1 to project 2 indicates that project 2 depends on project 1. Further, since tasks and projects depend on each other with varying degrees of intensity (Neumeier et al. 2018; Ellinas 2019; Paper 3; Paper 4), literature assigns weights to the edges. The portfolio theory of Markowitz (1952) models the intensity of the dependency between two financial products using a regression coefficient, e.g., Bravais Pearson. However, due to the uniqueness of tasks and projects, organizations cannot perform regression analysis and have to estimate the intensity of dependencies (Paper 4).

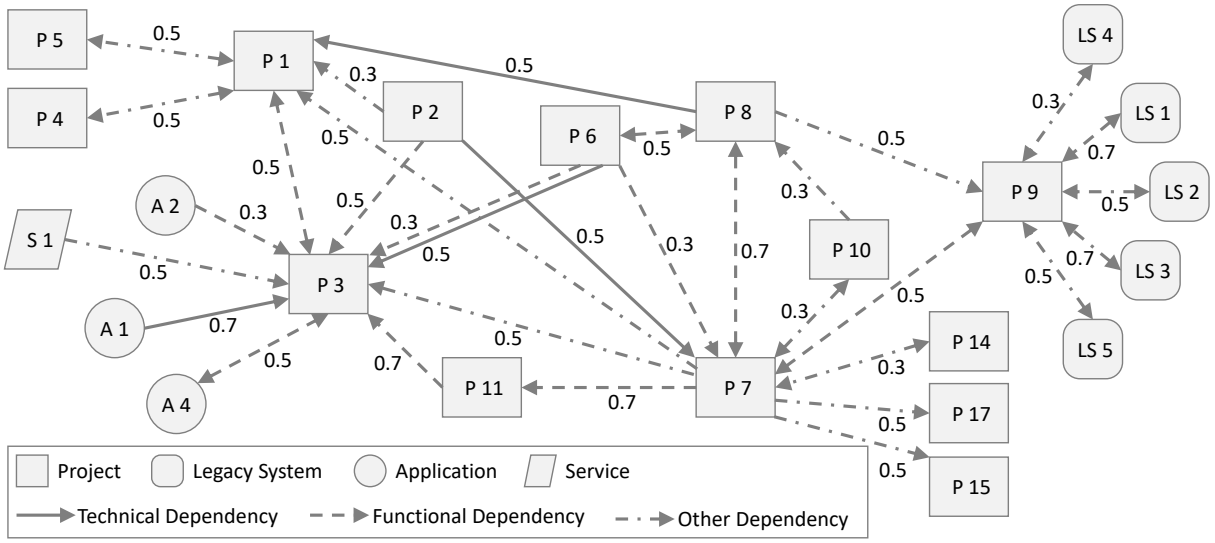

Figure 5 Real-world IT project portfolio modeled as a graph (Paper 3)

Figure 5 illustrates a real-world IT project portfolio modeled as a graph (Paper 3). First, the authors used different shapes to model projects and other elements of the organization's landscape, like legacy systems, applications, and services. Further, they used three different types of edges to model technical, functional, and other dependencies since the underlying dataset only distinguishes them. The edges' weights represent the individual dependencies' intensity. Thereby the authors modeled a 'low' dependency as 0.3, a medium dependency as 0.5, and a high dependency as 0.7. Therefore they used a very abstract definition of the weights. However, the modeling of the weights always depends on the underlying dataset and the designated problem to solve. For instance, Ellinas (2019), who builds on another real-world dataset and focuses on time, models the weights as day representing the float between two tasks indicating the response time available to deploy mitigation.

So far, we can conclude that to manage systemic risks in projects and project portfolios, organizations should model them as a graph to account for the existence of direct and directed edges, as well as their weights. However, there are still some additional aspects organizations must take care of.

4.3.2 Properties of systemic risk in IT Projects and IT Project Portfolios

Properties and effects of systemic risks differ in different application contexts. Therefore, organizations cannot quickly adapt systemic risk measures from other domains. Even systemic risk measures developed for IT portfolio management usually focus on specific aspects of systemic risk (Paper 3). Literature has already investigated the essential characteristics of systemic risks in projects and project portfolios (e.g., Beer et al. 2015; Ellinas 2018, 2019; Neumeier et al. 2018; Wolf 2015; Paper 3; Paper 4). I will point out the main properties of systemic risk in projects and project portfolios in the following.

First, tasks and projects depend on each other through direct, indirect, directional, non-directional, weighted, and non-weighted dependencies (Paper 3; Paper 4; Neumeier et al. 2018; Ellinas 2019; Wolf 2015). As already mentioned, inter-temporal dependencies can only be directed. Intra-temporal dependencies can either be

directed or undirected. Directed intra-temporal dependencies often represent resource dependencies (Neumeier et al. 2018). For example, a project depends on the availability of a specific technical component like a database or a web service. If this component is not (entirely) available, this has negative effects on the project. However, the project result may not influence the technical component.

Second, dependencies between tasks and projects can have positive and negative effects (Paper 3; Wolf 2015; Radszuwill and Fridgen 2017). Research and practice mainly regard dependencies to have negative effects (Häckel and Hänsch 2014). Therefore, a systemic risk must increase with the number of dependent tasks or projects indicating a high network density (Paper3; Paper 4). However, Paper 3 states that organizations should simultaneously consider the negative and positive effects (synergies) of dependencies to ensure holistic management of opportunities and risk. Radszuwill and Fridgen (2017) already addressed this issue by investigating the effects of resource dependencies and synergies in IT project portfolios.

Third, for instance, Paper 4 and Ellinas (2019) argue that the systemic risk in projects and project portfolios do not only base on dependencies. Tasks and projects also induce individual risk due to inherent parameters, like duration, probability of failure, risk measures (e.g., value at risk), or flags, e.g., indicating 'must have' projects, due to regulatory (Paper 3).

Fourth, based on the real-world dataset (Figure 5), Paper 3 states that tasks and projects can depend on each other via several separate dependencies with different intensities. Depending on how the entities are modeled, separate dependencies like 'low', 'medium', and 'high' can not be aggregated in a mathematically correct way.

Finally, Paper 3 and Wolf (2015) require systemic risk measures to consider the criticality of dependent tasks or projects within the calculation. Thereby, the criticality of a single task or project represents its influence on the project portfolio success (Neumeier et al. 2018). In concrete terms, this means that the systemic risk measure, for example, for project *i* depends on the individual criticality of all other dependent projects of the project portfolio.

For a detailed description of the properties of systemic risk in projects and project portfolios, I refer to Paper 3.

4.3.3 Systemic Risk Measures for IT Projects and IT Project Portfolios

Research already introduced different risk measures to manage systemic risk in projects and project portfolios during the past few years. In the following, I refer to these risk measures as systemic risk measures. Paper 3 provides a literature review of systemic risk measures for projects and project portfolios. According to this review, there exist six promising systemic risk measures. For instance, Beer et al. (2015) introduced a systemic risk measure to quantify project benefits and risks considering transitive dependencies. Neumeier et al. (2018) used Bayesian networks to model IT project portfolios and measuring single projects' criticality within an IT project portfolio. Further, Wolf (2015) provided an overview of different centrality measures. He investigated their suitability in the context of IT portfolio management. Finally, he concluded that the Alpha centrality, introduced by Bonacich and Lloyd (2001), is the most suitable one. Ellinas et al. (2015; 2016; 2018, 2019) investigated general aspects of systemic risk in projects focusing on durations and delays due to dependent tasks.

Further, Guo et al. (2019) introduced a cascade failure model to simulate the spread of failures between different tasks within a single project. This cascade failure model bases on load distribution in scale-free networks. Paper 4 introduced the so-called TD method to simulate the spread of failures and analyze project criticality in IT project portfolios based on the SI model of Kermack and McKendrick (1927). Besides others, this systemic risk measure also considers the speed of propagation, a significant factor of cascade effects in the context of epidemiology (Brockmann and Helbing 2013).

Since Paper 3 also investigated whether and which of these existing systemic risk measures regard the stated properties of systemic risk in the context of project and project portfolios. The authors ranked the risk measures according to their suitability to manage systemic risk in theory and practice. Finally, Paper 3 concludes that the systemic risk measure of Ellinas (2019) fits best to the stated properties. However, it lacks in the simultaneous consideration of the positive and negative effects of dependencies. Further, it ranked the systemic risk measures of Paper 4, Beer et al. (2015), Neumeier et al. (2018), and Guo et al. (2019) as second best. Due to the static definitions of the systemic risk measures of Beer et al. (2015) and Neumeier et al. (2018), Paper 3 argues that the risk measures of Paper 4 and Guo et al. (2019) are more promising than these.

In the following, I will briefly illustrate the results of Paper 3, introduce systemic risk measures of Ellinas (2019), Paper 4, and Guo et al. (2019), state their advantages and disadvantages, and discuss their suitability in practice. Even though not all systemic risk measures were explicitly developed for IT projects, we can still apply them in this context.

First, Ellinas (2019) proposes an analytical model based on Ellinas et al. (2015) and Ellinas et al. (2016) to identify the number of affected tasks, namely nodes, within a project. The systemic risk measure bases on a cascade failure model and results in two risk measures for each task i. On the one hand, it ranks each task's criticality according to its spreading power C_i^{SP} (equation 1) indicating the task-specific potential to cause cascade effects in later tasks. On the other hand, it ranks all tasks according to their sensitivity C_i^{S} (equation 2) indicating their susceptibility to failures of previous tasks.

$$C_i^{SP} = C_i^{SP(topo)} * C_i^{SP(temp)} \tag{1}$$

$$C_i^{S} = C_i^{S(topo)} * C_i^{S(temp)} * C_i^{S(float)} \tag{2}$$

Equations 1 and 2 consider both topological (topo) effects representing the task's position in the network, Activity-on-the-node network (AON) indicated by a directed graph, and temporal (temp) effects representing the task's specific duration (Ellinas 2019). The task's sensitivity further considers the float between two consecutive tasks representing the viable time to deploy mitigations. Thereby, the AON represents the float by the Euclidean space of the network (length of the edges). For a detailed description of all parameters and the underlying cascade model, I refer to Ellinas (2019).

This systemic risk measure has the great advantage that, apart from the simultaneous consideration of positive and negative effects, it considers all relevant properties of systemic risks in projects and project portfolios (Paper 3). Besides, organizations can

economically interpret the results like a potential delay of the entire project. However, it requires much data to realize this advantage. The high demand for data on individual tasks and projects (including dependencies, duration, buffer time between two tasks) is therefore also the most significant disadvantage of this systemic risk measure since such data is generally not fully available in organizations or can only be collected at significant additional expense. Therefore I conclude, that this systemic risk measure is suitable in theory but may lack in practice.

Second, Paper 4 introduced the TD method, based on the SI model from epidemiology, to simulate cascading failures in IT portfolios and analyze project criticality.

The SI model, introduced by Kermack and McKendrick (1927), considers two states: susceptible (state S) and infected (state I), which can only be reached in sequence (S → I). This describes a person who is currently healthy but is susceptible (state S) to illness. However, this person can become infected (state I) due to a spontaneous mutation (initial infect) or external influences (infected by another person) (Kermack and McKendrick 1927). Due to the transition S → I, an infected person cannot become susceptible again. This means that a person who reached state I cannot be cured. The 'infection rate' (β) indicates the possibility of transitioning from state S to state I. Kermack and McKendrick (1927) defines the infection rate as constant over time and for all people and depending on the specific disease. The cascading process of the SI model only ends when there are no more susceptible people left, which implies that everyone is infected.

In terms of project and project portfolios, the TD method distinguishes two states: 'on track' (T) and 'in difficulty' (D). According to Paper 4, a project which is in state T is on track, which means that it is in time, in scope, and in budget. However, it can become in difficult (state D) (Paper 3). If a project reaches state D it can affect other projects depending on it (Paper 3, Paper 4). Analogous to the SI model, the TD method assumes that that projects in state D can affect other projects which are currently in state T. Further, the TD method does also not consider the transition from state D back to state T, which would imply that a project gets back on track again. Unlike the SI model, in the TD method, the transition from state T to state D is based on the dependency's intensity between these two projects. Non-existing dependencies rely on the possibility of zero. Finally, the TD method results in a criticality measure (equation 3), which considers the total number of projects in state D and propagation speed.

$$CM_i = 1 + \sum_{t=1}^{n} \frac{\Delta elements_{i,t}^{D}}{t^{\gamma}} \qquad (3)$$

In equation 3, $\Delta elements_{i,t}^{D}$ indicates how many projects transferred to state D in time step t based on an initial failure in project i. The TD method considers the speed of propagation by weighting $\Delta elements_{i,t}^{D}$ with t^{γ}. Therefore cascade effects in former time steps are more critical than cascade effects in later time steps (Paper 4). Further, they used the parameter γ to control how strong the criticality measure considers the speed of propagation. Therefore the TD method's results depend on the subjective choice of the parameter γ (Paper 4).

Compared to the risk measure of Ellinas (2019), the calculation of the TD method is significantly less complex, which is an essential advantage since organizations can use it more quickly due to the fewer input data required. Nevertheless, it fulfills

almost all essential properties of systemic risks in projects and project portfolios. (Paper 3). However, the consideration of fewer systemic risk properties is a disadvantage of the TD method. Analogous to the Ellinas risk measure, the TD method also does not consider the positive and negative effects of dependencies. Moreover, the TD method does not consider specific parameters of individual tasks or projects. In addition, the informative value of the TD method is lower than of the systemic risk measure of Ellinas (2019). The TD method is limited exclusively to a ranking of the individual tasks' and projects' criticality. Organizations can therefore not interpret the result in economic terms. Besides, the defined transition T → D assumes that a project, which is in trouble could never be on track again. Besides the SI model, Kermack and McKendrick (1927) also introduced other models like the SIS model (allowed transition: S → I → S). Therefore an extension of the TD method would make the TD method more applicable in practice.

Third, Guo et al. (2019) investigated cascading failures in projects. The systemic risk measure explicitly considers each project task's duration as an indicator of its influence on other projects. The cascading model base on a flow redistribution model adapted from transport networks. This systemic risk measure considers the failure capacity of projects, which is limited by costs. Guo et al. (2019) define the capacity of each project as following:

$$C_n = (1 + \beta) * L_n(0) \; with \; L_n(0) = (k_n)^{\alpha} \qquad (4)$$

In equation 4, the capacity of project n (C_n) indicates the maximum load a project can handle. Thereby, the parameter $L_n(0)$ represents the initial load ($t = 0$) of project n estimated using centrality measures like the betweenness centrality, degree centrality, or the out-degree centrality depending on the application context (Paper 3). In doing so, Guo et al. (2019) focused on the degree centrality as k_n indicates the sum of the edges' weights. The parameter α adjusts the strength of the initial load. Further, analogous to Crucitti et al. (2004), who investigated flow redistribution models in transport networks, Guo et al. (2019) assume a linear correlation between the capacity and the initial load. Thereby, the parameter β adjusts the tolerance of projects against failures. For $\beta > 1$ implies that a project can handle a greater load than the initial load and can resist failures up to a certain degree. Therefore, this indicates a projects' self-protection mechanism. This means that a project may restore itself without affected dependent projects (Guo et al. 2019). A cascade effect only occurs if at any time step t at least one project load is bigger than its capacity. Finally, they provide two metrics representing the normalized avalanche size (CF_1) and the normalized avalanche size considering the weight of failed projects (CF_2). For a detailed description of the cascade model based on load redistribution and the calculation of CF_1 and CF_2 I refer to Guo et al. (2019)

Organizations can interpret the results of the systemic risk measure of Guo et al. (2019) economically, which is a significant advantage. However, the calculation of this systemic risk measure is similarly complex to Ellinas (2019) and requires a comprehensive data basis. Moreover, this systemic risk measure also does not satisfy all essential properties of systemic risk in projects and project portfolios. Besides not considering the positive and negative effects of dependencies simultaneously, it cannot regard for multiple separate dependencies between two tasks or projects, which do occur in real projects and project portfolios (Paper 3). Therefore, this risk measure might be of limited use in practice.

Overall, I conclude that all three systemic risk measures help to identify and manage systemic risk in projects and project portfolios. However, all three are very specifically designed and only support organizations in specific use cases. For example, organizations focusing on the risk of delays in projects or project portfolios should rely on the systemic risk measure of Ellinas (2019) or Guo et al. (2019). However, organizations that want to know which tasks or projects are particularly critical in terms of cascading effects should rely on the less complex TD method (Paper 4). All three systemic risk measures have their specific strengths and do not differ significantly in their drawbacks. In addition, they are not easy to implement and use and require a certain amount of know-how.

At this point, in line with Paper 3, I would therefore like to refer to the alpha centrality of Bonacich and Lloyd (2001), which performs significantly worse than the three systemic risk measures just described in terms of the main characteristics of systemic risks in projects and project portfolios (Paper 3). However, it is straightforward to implement and a suitable systemic risk measure for projects and project portfolios (Wolf 2015). Moreover, Paper 4 evaluated the TD method during an expert study using a real-world data set. The authors finally concluded that the TD method delivers comparable results to the alpha centrality since both criticality rankings are significantly correlated to each other and to the expert ranking, which indicates the benchmark. They further point out that both systemic risk measures are suitable in project and project portfolios. Still, the TD method may outperform the alpha centrality since a simulation approach is more flexible for adaptation than the alpha centrality (Paper 4). However, I want to note that the alpha centrality might be a suitable first guess for organizations to manage project criticality under consideration of the effects of systemic risk.

With the presented selection of systemic risk measures, I illustrated that besides cascade failure algorithms, centrality measures also play an essential role. They allow organizations to draw initial conclusions about the risk in the IT portfolio with comparatively little computing effort. I demonstrated that each systemic risk measure only focuses on specific aspects of systemic risk in projects and project portfolios, and therefore none ‘right’ systemic risk measure exists. Each has its advantages, and organizations have to choose a suitable one according to their specific application context and available data.

5 The interplay of IT security and systemic risk

After demonstrating in detail that IT security plays a significant role in aligning security needs to the organization’s level of digitalization while implementing IT projects and illustrating how organizations can manage IT projects in the context of IT security while regarding systemic risk, I will discuss the interplay between these two topics in more detail.

IT security projects strongly relate to systemic risk. The strategic alignment of digitalization and IT security significantly impacts the composition and complexity of IT projects and IT project portfolios since IT security projects are predominantly not independent from other IT projects. IT security projects (e.g., the implementation of new, more secure hardware) usually do not affect a single organizational area since organizations have to adapt not only the infrastructure but also further applications and business processes based on it. Further, the implementation of new infrastructure can also enable new innovative business models. Therefore, many

other IT projects in an organization depend on the successful implementation of IT security projects. This creates many different types of dependencies in the IT project portfolio, which in turn increases systemic risk.

The presented alignment paths underline the existence and relevance of these dependencies. Organizations that focus on security pragmatism in the short or medium-term should have a market advantage over their competitors (Paper 1). Nevertheless, a strong focus on digitization will always result in the necessity to implement IT security later to counteract the risk of failure or external attack that has arisen through digitization. I will illustrate this need with an example.

In the course of the digitization in manufacturing organizations known as the fourth industrial revolution (Industry 4.0), many organizations digitize single production steps or network production machines with different IT components creating smart factories. Organizations increasingly integrate IT services like control systems into their production environments. This increases the flexibility of production and allows them to offer new data-based services like predictive maintenance (Bürger et al. 2019; Sadeghi et al. 2015). However, organizations do not only connect their production facilities to the internet, but they also interconnect their value creation processes with external market players and customers to optimize production and business processes and create innovative solutions or even new business models (Bürger et al. 2019). This interconnection leads to new risks that must be managed through IT security (projects).

Digital production processes initially depend on the availability of IT, which is one aspect of the CIA triad. The unavailability of IT or individual components can significantly affect production (Häckel et al. 2019; Miehle et al. 2019). For instance, Bürger et al. (2019) investigated the impact of availability incidents by simulating cyber-attacks in smart factories. Further, Miehle et al. (2019) introduced a graph-based approach to model IT availability risks and their cascading effects using Petri nets. Furthermore, the link to external market players and customers increases the risk of external attacks to steal confidential data or destroy data integrity. In the era of industry 4.0, IT security management must prepare organizations for a wide variety of cyber-attacks. For a detailed overview of cyber-attacks and their characteristics, I refer to Berger et al. (2020), who developed a taxonomy for cyber-attacks focusing on IoT.

Besides, attempted or successful cyber-attacks or other IT security incidents mean that organizations must improve their IT security management. This need, in turn, leads to an increasing number of (interdependent) IT security projects and thus increasing the complexity of IT project portfolios and increasing systemic risk.

6 Conclusion

6.1 Summary and Outlook

In my thesis, I illustrated that the constantly increasing digitalization always accompanies an adjustment of IT security. Regardless of the strategic alignment of organizations regarding IT security, the interplay of both domains leads to increasingly complex IT project portfolios. This complexity increases the danger of systemic risk, which must be managed due to their high damage potential.

The investigation of systemic risks in the context of IT portfolios is still in its infancy. However, research already took the first successful steps. Research has broadly investigated different types of synergies and dependencies and their effects in theory and derived requirements for comprehensive risk management. Existing systemic risk measures for IT projects and IT project portfolios transfer established knowledge from other areas and contribute to a theoretical improvement of IT portfolio management. Their effectiveness in practice, however, is hardly proven. Although, among other things, Ellinas (2019), Paper 4, and Guo et al. (2019) used data from real IT projects, respectively IT project portfolios, to evaluate their systemic risk measures. However, in practice, organizations usually cannot provide such a database.

The lack of sufficient data about project parameters and especially dependencies (or synergies) is a significant problem in managing IT projects and IT project portfolios. In other domains, like supply networks or critical infrastructures, we know or can at least derive the network's structure. Nevertheless, organizations usually do not know the actual structure of their IT projects or IT project portfolios. However, quantitative systemic risk measures require knowledge of the entire IT portfolio. Thus, research essentially bases its contribution on the assumption that it is not applicable in practice.

Organizations have a good overview of which projects are currently running or are planned in the (near) future. However, identifying dependencies is much more complex, among other things, due to shared responsibilities within the management (Paper 3; Paper 4). For instance, project managers can usually make reliable statements about which other projects, people, or technical resources their project depends on. Statements about the importance of their project for other projects or the entire organization are more challenging to make. Combining the insights of many project managers could solve this problem. However, in practice, this problem might usually be too complex to be solved. It becomes even more complex when, in addition to the dependencies themselves, project managers also have to determine their intensities. In the financial sector, the correlation between two financial products (e.g., stocks) base on historical data. This correlation allows at least an approximate estimation of the intensity. However, historical data do not allow us to predict the future. Due to the uniqueness of IT projects, organizations cannot use historical data to calculate a correlation. Therefore, organizations estimate the intensities of the dependencies based on expert knowledge (Beer et al. 2015; Paper 3; Paper 4). However, the estimation leads to high uncertainty and low reliability. However, disruptive technologies can help solve this problem. Gartner (2019) notes that modern technologies, especially artificial intelligence, will take over 80% of today's project management tasks until 2030. Artificial intelligence can help to analyze IT projects (including all project documentation) and the organization infrastructure (e.g., personnel, software, and hardware), identify dependencies, and determine their intensity.

Despite the currently limited applicability in practice, the systemic risk measures developed so far still represent a great added value for knowledge management. On the one hand, future research will have to investigate the specific characteristics of systemic risks in IT portfolios even more precisely. On the other hand, future research should continue optimizing existing systemic risk measures or develop entirely new procedures by focusing on disruptive technologies like artificial intelligence. Moreover, due to the apparent accuracy of current systemic risk

measures, future research also must strengthen the understanding of how to interpret the results of systemic risk measures. Even with artificial intelligence or other IT support, the data is always subject to a certain degree of uncertainty. Therefore, future systemic risk measures should focus on using minimal input data to guarantee a sufficient quality of the results. However, it is better to estimate fewer data under uncertainty and know that the result will only be an indicator than to estimate many data 'wrong' and provoke an erroneous, false precision.

In the coming years, organizations will carry out an increasing number of digitization projects to strengthen their market position and thus face new security risks. This doctoral thesis will help them to understand the interplay of these two domains and support them in managing the resulting systemic risks.

6.2 Acknowledgment of Previous and Related Work

On all research projects and papers, I worked with colleagues at the University of Bayreuth, the University of Augsburg, the Project Group Business and Information Systems Engineering of the Fraunhofer Institute for Applied Information Technology (FIT), and the Research Center Finance and Information Management (FIM). Therefore, I indicate how my work builds on previous and related work conducted within these organizations.

Research Paper 1 was inspirend by Bürger et al. (2019), Berger et al. (2020), and Bitomsky et al. (2020), who investigated the impact of IT security incidents and cyber attacks in digitized production environments. Research Paper 2.1 und Research Paper 2.2 relate to the work of Schweizer et al. (2017) and Fridgen et al. (2018a) and were inspired by Fridgen et al. (2019) who already discussed opportunities and challenges of different blockchain solutions with regard to data privacy on other application fields. Further, Wolf (2015) inspired Research Paper 3, since he already derived criteria for systemic risk measures in context of project portfolios and evaluated different centrality measures according to their suitabillity. Research Paper 3 and Research Paper 4 rely on the work of Wehrmann et al. (2006), Zimmermann (2008), Beer et al. (2015), and Radszuwill and Fridgen (2017) who investigated the impact of different types of dependencies on the management of IT project portfolios. Finally, the papers of Radszuwill and Fridgen (2017) and Neumeier et al. (2018) provided a good starting point for Research Paper 4.

7 References

Acharya VV, Pedersen LH, Philippon T, Richardson M (2017) Measuring systemic risk. The Review of Financial Studies 30(1):2–47.

Agarwal A, Agarwal A (2011) The security risks associated with cloud computing. International Journal of Computer Applications in Engineering Sciences 1:257–259.

Alshamrani A, Bahattab A (2015) A comparison between three SDLC models waterfall model, spiral model, and Incremental/Iterative model. International Journal of Computer Science Issues (IJCSI) 12(1):106.

Anbari FT (2003) Earned value project management method and extensions. Project Management Journal 34(4):12–23.

Ash J, Newth D (2007) Optimizing complex networks for resilience against cascading failure. Physica A: Statistical Mechanics and its Applications 380:673–683.

Ashenden D (2008) Information Security Management: A Human Challenge? Information security technical report 13(4):195–201. doi:10.1016/j.istr.2008.10.006.

Avital M, Beck R, King JL, Rossi M, Teigland R (2016) Jumping on the Blockchain Bandwagon: Lessons of the Past and Outlook to the Future. In: Proceedings of the 37th International Conference on Information Systems (ICIS).

Bakker K de, Boonstra A, Wortmann H (2010) Does risk management contribute to IT project success? A meta-analysis of empirical evidence. International Journal of Project Management 28(5):493–503.

Barabási A-L, Albert R (1999) Emergence of Scaling in Random Networks. Science 286(5439):509–512.

Barabási A-L, Bonabeau E (2003) Scale-free networks. Scientific american 288(5):60–69.

Barnes SJ (2020) Information management research and practice in the post-COVID-19 world. International Journal of Information Management 55:102175.

Baskerville R, Myers MD (2004) Special issue on action research in information systems: Making IS research relevant to practice: Foreword. MIS Quarterly:329–335.

Beer M, Wolf T, Zare Garizy T (2015) Systemic Risk in IT Portfolios – An Integrated Quantification Approach. In: Proceedings of the 36th International Conference on Information Systems (ICIS).

Berg A, Haldenwang T (2018) Wirtschaftsschutz in der Industrie. https://www.bitkom.org/sites/default/files/file/import/Bitkom-PK-Wirtschaftsschutz-Industrie-13-09-2018-2.pdf. Accessed 2020-04-30.

Berger S, Bürger O, Röglinger M (2020) Attacks on the Industrial Internet of Things - Development of a Multi-Layer Taxonomy. Computers & Security:101790.

Berghaus S, Back A (2016) Stages in Digital Business Transformation: Results of an Empirical Maturity Study. In: Proceedings of the 10th Mediterranean Conference on Information Systems (MCIS).

Bharadwaj A, El Sawy OA, Pavlou PA, Venkatraman N (2013) Digital business strategy: toward a next generation of insights. MIS Quarterly:471–482.

Bitomsky L, Bürger O, Häckel B, Töppel J (2020) Value of data meets IT security–assessing IT security risks in data-driven value chains. Electronic Markets:1–17.

Bonacich P, Lloyd P (2001) Eigenvector-like measures of centrality for asymmetric relations. Social networks 23(3):191–201.

Bowen PL, Cheung M-YD, Rohde FH (2007) Enhancing IT governance practices: A model and case study of an organization's efforts. International Journal of Accounting information Systems 8(3):191–221.

Brockmann D, Helbing D (2013) The hidden geometry of complex, network-driven contagion phenomena. Science 342(6164):1337–1342.

Buhl HU, Fridgen G, König W, Röglinger M, Wagner C (2012a) Where's the competitive advantage in strategic information systems research? Making the case for boundary-spanning research based on the German business and information systems engineering tradition. The Journal of Strategic Information Systems 21(2):172–178.

Buhl HU, Müller G, Fridgen G, Röglinger M (2012b) Business and information systems engineering: a complementary approach to information systems–what we can learn from the past and may conclude from present reflection on the future. Journal of the Association for Information Systems 13(4):3.

Buldyrev SV, Parshani R, Paul G, Stanley HE, Havlin S (2010) Catastrophic cascade of failures in interdependent networks. Nature 464(7291):1025.

Bürger O, Häckel B, Karnebogen P, Töppel J (2019) Estimating the impact of IT security incidents in digitized production environments. Decision Support Systems 127:113144.

Cao L, Ramesh B (2008) Agile requirements engineering practices: An empirical study. IEEE software 25(1):60–67.

Carbone TA, Tippett DD (2004) Project risk management using the project risk FMEA. Engineering management journal 16(4):28–35.

Cardholm L (2016) Demonstrating Business Value of Security Investments in the Age of Digitalization. International Journal of Innovation in the Digital Economy (IJIDE) 7(3):1–25.

Chan YE, Reich BH (2007) IT alignment: what have we learned? Journal of Information technology 22(4):297–315.

Cherdantseva Y, Hilton J (2013) A reference model of information assurance & security. In: Proceedings of the International Conference on Availability, Reliability and Security, pp 546–555.

Christidis K, Devetsikiotis M (2016) Blockchains and Smart Contracts for the Internet of Things. IEEE Access 4:2292–2303. doi:10.1109/ACCESS.2016.2566339.

Conboy K (2009) Agility from first principles: Reconstructing the concept of agility in information systems development. Information Systems Research 20(3):329–354.

Conforto EC, Salum F, Amaral DC, Da Silva SL, De Almeida, Luís Fernando Magnanini (2014) Can agile project management be adopted by industries other than software development? Project Management Journal 45(3):21–34.

Cunningham W (1993) The WyCash portfolio management system. ACM SIGPLAN OOPS Messenger 4(2):29–30. doi:10.1145/157710.157715.

Davison RM, Martinsons MG, Ou CXJ (2012) The roles of theory in canonical action research. MIS Quarterly:763–786.

Devaraj S, Kohli R (2003) Performance Impacts of Information Technology: Is Actual Usage the Missing Link? Management Science 49(3):273–289. doi:10.1287/mnsc.49.3.273.12736.

Dooly Z, Doyle K, Power J (2015) Uncovering Innovation Practices and Requirements in Privacy and Cyber Security Organisations: Insights from IPACSO. In: Proceedings of the Cyber Security and Privacy Forum. Springer, Cham, Heidelberg, New York, Dordrecht, London, pp 140–150.

Dor D, Elovici Y (2016) A model of the information security investment decision-making process. Computers & Security 63:1–13.

Drugescu C, Etges R (2006) Maximizing the return on investment on information security programs: Program governance and metrics. Information systems security 15(6):30–40.

Eisenberg L, Noe TH (2001) Systemic risk in financial systems. Management Science 47(2):236–249.

Ellinas C (2018) Modelling indirect interactions during failure spreading in a project activity network. Scientific reports 8(1):1–12.

Ellinas C (2019) The domino effect: An empirical exposition of systemic risk across project networks. Production and Operations Management 28(1):63–81.

Ellinas C, Allan N, Durugbo C, Johansson A (2015) How Robust Is Your Project? From Local Failures to Global Catastrophes: A Complex Networks Approach to Project Systemic Risk. PloS one 10(11):e0142469. doi:10.1371/journal.pone.0142469.

Ellinas C, Allan N, Johansson A (2016) Project systemic risk: Application examples of a network model. International Journal of Production Economics 182:50–62.

Englund RL, Graham RJ (1999) From experience: linking projects to strategy. Journal of Product Innovation Management 16(1):52–64.

Engwall M, Jerbrant A (2003) The resource allocation syndrome: the prime challenge of multi-project management? International Journal of Project Management 21(6):403–409.

Erdős P, Rényi A (1960) On the evolution of random graphs. Publ. Math. Inst. Hung. Acad. Sci 5(1):17–60.

Eschweiler J (2018) Progressing Towards a Prescriptive Approach on Cyber Security–Adopting Best Practices and Leverage Technical Innovation. In: Cybersecurity Best Practices. Springer, pp 339–347.

Flyvbjerg B, Budzier A (2011) Why Your IT Project May Be Riskier Than You Think. Harvard Business Review 89:23–25.

Freixas X, Parigi BM, Rochet J-C (2000) Systemic risk, interbank relations, and liquidity provision by the central bank. Journal of money, credit and banking:611–638.

Fridgen G, Guggenberger N, Hoeren T, Prinz W, Urbach N, Baur J, Brockmeyer H, Gräther W, Rabovskaja E, Schlatt V (2019) Chancen und Herausforderungen von DLT (Blockchain) in Mobilität und Logistik.

Fridgen G, Lockl J, Radszuwill S, Rieger A, Schweizer A, Urbach N (2018a) A Solution in Search of a Problem: A Method for the Development of Blockchain Use Cases. In: Proceedings of the 24th Americas Conference on Information Systems (AMCIS), p 11.

Fridgen G, Radszuwill S, Urbach N, Utz L (2018b) Cross-Organizational Workflow Management Using Blockchain Technology - Towards Applicability, Auditability, and Automation. In: Proceedings of the 51th Hawaii International Conference on System Sciences (HICSS).

Gao J, Buldyrev SV, Havlin S, Stanley HE (2011) Robustness of a network of networks. Physical review letters 107(19):195701.

Gartner (2019) Gartner Says 80 Percent of Today's Project Management Tasks Will Be Eliminated by 2030 as Artificial Intelligence Takes Over, Stamford.

Gartner (2021a) Gartner Forecasts Worldwide IT Spending to Reach $4 Trillion in 2021. https://www.gartner.com/en/newsroom/press-releases/2021-04-07-gartner-forecasts-worldwide-it-spending-to-reach-4-trillion-in-2021. Accessed 2021-05-29.

Gartner (2021b) Gartner Forecasts Worldwide Security and Risk Management Spending to Exceed $150 Billion in 2021. https://www.gartner.com/en/newsroom/press-releases/2021-05-17-gartner-forecasts-worldwide-security-and-risk-managem. Accessed 2021-05-29.

Geraldi J, Lechter T (2012) Gantt charts revisited: A critical analysis of its roots and implications to the management of projects today. International Journal of Managing Projects in Business.

German Institute for Standardization (2009) Project management - Project management systems(DIN 69901).

Ghasemzadeh F, Archer NP (2000) Project portfolio selection through decision support. Decision Support Systems 29(1):73–88.

Glaser F (2017) Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis. In: Proceedings of the 50th Hawaii International Conference on System Sciences.

Goldfarb A, Tucker C (2019) Digital Economics. Journal of Economic Literature 57(1):3–43. doi:10.1257/jel.20171452.

Gordon J, Tulip A (1997) Resource scheduling. International Journal of Project Management 15(6):359–370.

Gordon LA, Loeb MP (2002) The Economics of Information Security Investment. ACM Transactions on Information and System Security (TISSEC) 5(4):438–457. doi:10.1145/581271.581274.

Grahn S, Granlund A, Lindhult E (2021) Barriers to Value Specification when Carrying out Digitalization Projects. Technology Innovation Management Review 11(5). https://timreview.ca/article/1442.

Guo N, Guo P, Dong H, Zhao J, Han Q (2019) Modeling and analysis of cascading failures in projects: A complex network approach. Computers & Industrial Engineering 127:1–7.

Häckel B, Hänsch F (2014) Managing an IT portfolio on a synchronised level, or: The costs of partly synchronised investment valuation. Journal of Decision Systems 23(4):388–412.

Häckel B, Hänsch F, Hertel M, Übelhör J (2019) Assessing IT availability risks in smart factory networks. Business Research 12(2):523–558.

Hans EW, Herroelen W, Leus R, Wullink G (2007) A hierarchical approach to multi-project planning under uncertainty. Omega 35(5):563–577.

Harguem S, Karuranga E, Mellouli S (2014) Impact of IT governance on organizational performance: Proposing an explanatory model. In: European Conference on Management, Leadership & Governance. Academic Conferences International Limited, p 436.

Heidt M, Gerlach J, Buxmann P (2018) A Holistic View on Organizational IT Security: The Influence of Contextual Aspects During IT Security Decisions. In: Proceedings of the 51th Hawaii International Conference on System Sciences (HICSS).

Hendriks MH, Voeten B, Kroep L (1999) Human resource allocation in a multi-project R&D environment: resource capacity allocation and project portfolio planning in practice. International Journal of Project Management 17(3):181–188.

Hevner AR (2007) A three cycle view of design science research. Scandinavian journal of information systems 19(2):4.

Hevner AR, March ST, Park J, Ram S (2004) Design science in information systems research. MIS Quarterly:75–105.

Hovav A, Gray P (2014) The ripple effect of an information security breach event: A stakeholder analysis. Communications of the Association for Information Systems 34(1):50.

Hsu C, Wang T, Lu A (2016) The Impact of ISO 27001 certification on firm performance. In: Proceedings of the 49th Hawaii International Conference on System Sciences (HICSS). IEEE, pp 4842–4848.

Huang X, Gao J, Buldyrev SV, Havlin S, Stanley HE (2011) Robustness of interdependent networks under targeted attack. Physical Review E 83(6).

IBM (2019) IBM: Cost of a Data Breach Report 2019. Computer Fraud & Security 2019(8):4. doi:10.1016/S1361-3723(19)30081-8.

Iivari J, Venable JR (2009) Action research and design science research-Seemingly similar but decisively dissimilar.

International Project Management Association (2015) Individual Competence Baseline for project, programme & portfolio management.

Izurieta C, Kimball K, Rice D, Valentien T (2018) A position study to investigate technical debt associated with security weaknesses. In: Proceedings of the 2018 International Conference on Technical Debt. IEEE, pp 138–142.

Järvinen P (2007) Action research is similar to design science. Quality & Quantity 41(1):37–54.

Jeong CY, Lee S-YT, Lim J-H (2019) Information security breaches and IT security investments: Impacts on competitors. Information & Management 56(5):681–695.

Johnston AC, Hale R (2009) Improved security through information security governance. Communications of the ACM 52(1):126–129.

Jonker W, Petković M (2013) Security, privacy and trust: from innovation blocker to innovation enabler. In: Workshop on Secure Data Management. Springer, Cham, pp 54–58.

Kane GC, Palmer D, Phillips AN, Kiron D, Buckley N (2015) Strategy, not technology, drives digital transformation. MIT Sloan Management Review and Deloitte University Press 14(1-25).

Kankanhalli A, Charalabidis Y, Mellouli S (2019) IoT and AI for smart government: A research agenda. Government Information Quarterly 36(2):304–309.

Kaufman GG, Scott KE (2003) What is systemic risk, and do bank regulators retard or contribute to it? The Independent Review 7(3):371–391.

Keller R, Ollig P, Fridgen G Decoupling, Information Technology, and the Tradeoff between Organizational Reliability and Organizational Agility. In:

Kermack WO, McKendrick AG (1927) A Contribution to the Mathematical Theory of Epidemics. Proceedings of the Royal Society A: Mathematical, Physical and Engineering Sciences 115(772):700–721. doi:10.1098/rspa.1927.0118.

Kshetri N (2017) Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecommunications policy 41(10):1027–1038.

Laslo Z (2010) Project portfolio management: An integrated method for resource planning and scheduling to minimize planning/scheduling-dependent expenses. International Journal of Project Management 28(6):609–618.

Laslo Z, Goldberg AI (2008) Resource allocation under uncertainty in a multi-project matrix environment: Is organizational conflict inevitable? International Journal of Project Management 26(8):773–788.

Lee JW, Kim SH (2001) An integrated approach for interdependent information system project selection. International Journal of Project Management 19(2):111–118.

Legner C, Eymann T, Hess T, Matt C, Böhmann T, Drews P, Mädche A, Urbach N, Ahlemann F (2017) Digitalization: Opportunity and Challenge for the Business and Information Systems Engineering Community. Business & Information Systems Engineering 59(4):301–308. doi:10.1007/s12599-017-0484-2.

Lova A, Maroto C, Tormos P (2000) A multicriteria heuristic method to improve resource allocation in multiproject scheduling. European journal of operational research 127(2):408–424.

Lucas H, Moore J (1976) A multiple-criterion scoring approach to information system project selection. INFOR: Information Systems and Operational Research 14(1):1–12.

March JG, Shapira Z (1987) Managerial perspectives on risk and risk taking. Management Science 33(11):1404–1418.

Markowitz H (1952) Portfolio Selection. The Journal of Finance 7(1):77–91.

McFarlan FW (1981) Portfolio approach to information systems. Harvard Business Review 59(5):142–151.

Miehle D, Häckel B, Pfosser S, Übelhör J (2019) Modeling IT Availability Risks in Smart Factories. Business & Information Systems Engineering:1–23.

Mosenia A, Jha NK (2016) A comprehensive study of security of internet-of-things. IEEE Transactions on Emerging Topics in Computing 5(4):586–602.

Munns AK, Bjeirmi BF (1996) The role of project management in achieving project success. International Journal of Project Management 14(2):81–87.

Nakamoto S (2008) Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review:21260.

Neumeier A, Radszuwill S, Garizy TZ (2018) Modeling project criticality in IT project portfolios. International Journal of Project Management 36(6):833–844.

Payette J, Anegbe E, Caceres E, Muegge S (2015) Secure by design: Cybersecurity extensions to project management maturity models for critical infrastructure projects. Technology Innovation Management Review 5(6).

Porru S, Pinna A, Marchesi M, Tonelli R (2017) Blockchain-Oriented Software Engineering: Challenges and New Directions. In: 2017 IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C). IEEE, pp 169–171.

Preston DS, Karahanna E (2009) Antecedents of IS strategic alignment: a nomological network. Information Systems Research 20(2):159–179.

Project Management Institute (2017) A Guide to the Project Management Body of Knowledge: (Pmbok Guide), Newtown Square, PA.

Radar Group (2012) The Impact of Data Silos in IT Planning (White Paper).

Radszuwill S, Fridgen G (2017) Forging a Double-Edged Sword: Resource Synergies and Dependencies in Complex IT Project Portfolios. 38th International Conference on Information Systems (ICIS), Seoul, South Korea.

Ramasubbu N, Kemerer CF (2016) Technical Debt and the Reliability of Enterprise Software Systems: A Competing Risks Analysis. Management Science 62(5):1487–1510. doi:10.1287/mnsc.2015.2196.

Rastogi R, Solms R von (2004) Information Security Governance - A Re-Definition. In: Security management, integrity, and internal control in information systems (IICIS 2004). Springer, Boston, pp 223–236.

Reyck B de, Grushka-Cockayne Y, Lockett M, Calderini SR, Moura M, Sloper A (2005) The impact of project portfolio management on information technology projects. International Journal of Project Management 23(7):524–537.

Röglinger M, Schwindenhammer L, Stelzl K (2018) How to Put Organizational Ambidexterity into Practice : Towards a Maturity Model. In: 16th International Conference on Business Process Management (BPM).

Royce WW (1987) Managing the development of large software systems. proceedings of IEEE WESCON. In: Proceedings of the 9th International Conference on Software Engineering, pp 328–388.

Sadeghi A-R, Wachsmann C, Waidner M (2015) Security and privacy challenges in industrial internet of things. In: Proceedings of the 52nd ACM/EDAC/IEEE Design Automation Conference (DAC). IEEE, pp 1–6.

Saltzer JH, Schroeder MD (1975) The protection of information in computer systems. Proceedings of the IEEE 63(9):1278–1308.

Santhanam R, Kyparisis GJ (1996) A decision model for interdependent information system project selection. European journal of operational research 89(2):380–399.

Schwaber K, Beedle M (2002) Agile software development with Scrum. Prentice Hall Upper Saddle River.

Schweizer A, Knoll P, Urbach N, Gracht HA von der, Hardjono T (2020) To what extent will blockchain drive the machine economy? Perspectives from a prospective study. IEEE Transactions on Engineering Management 67(4):1169–1183.

Schweizer A, Schlatt V, Urbach N, Fridgen G (2017) Unchaining Social Businesses - Blockchain as the Basic Technology of a Crowdlending Platform. In: Proceedings of the 38th International Conference on Information Systems (ICIS).

Smith GE, Watson KJ, Baker WH, Pokorski Ii JA (2007) A critical balance: collaboration and security in the IT-enabled supply chain. International Journal of Production Research 45(11):2595–2613.

Solms B von, Solms R von (2005) From information security to...business security? Computers & Security 24(4):271–273. doi:10.1016/j.cose.2005.04.004.

Solms R von, Solms SB von (2006) Information Security Governance: a model based on the direct–control cycle. Computers & Security 25(6):408–412.

Strogatz SH (2001) Exploring complex networks. Nature 410(6825):268.

Tereso A, Ribeiro P, Fernandes G, Loureiro I, Ferreira M (2019) Project management practices in private organizations. Project Management Journal 50(1):6–22.

The Standish Group (2018) Decision latency theory: It is all about the interval.

Tillquist J, King JL, Woo C (2002) A representational scheme for analyzing information technology and organizational dependency. MIS Quarterly:91–118.

van Grembergen W, Haes S de (2005) Measuring and improving IT governance through the balanced scorecard. Information systems control Journal 2(1):35–42.

van Niekerk B, Naidoo V (2014) Strategic information security management as a key tool in enhancing competitive advantage in South Africa. Journal of Contemporary Management 11(1):33–46.

Vial G (2019) Understanding digital transformation: A review and a research agenda. The Journal of Strategic Information Systems 28(2):118–144.

Walter SG, Spitta T (2004) Approaches to the ex-ante evaluation of investments into information systems. Wirtschaftsinformatik 46(3):171–180.

Wang J-W, Rong L-L (2009) Cascade-based attack vulnerability on the US power grid. Safety science 47(10):1332–1336.

Wang Y, Han JH, Beynon-Davies P (2019) Understanding blockchain technology for future supply chains: a systematic literature review and research agenda. Supply Chain Management: An International Journal.

Ward S, Chapman C (2003) Transforming project risk management into project uncertainty management. International Journal of Project Management 21(2):97–105.

Watts DJ (2002) A simple model of global cascades on random networks. Physica A: Statistical Mechanics and its Applications 99(9):5766–5771. doi:10.1073/pnas.082090499.

Watts DJ, Strogatz SH (1998) Collective dynamics of 'small-world'networks. Nature 393(6684):440.

Wehrmann A, Heinrich B, Seifert F (2006) Quantitatives IT-Portfoliomanagement: Risiken von IT-Investitionen wertorientiert steuern. Wirtschaftsinformatik 48.

Weill P, Ross JW (2004) IT governance: How top performers manage IT decision rights for superior results. Harvard Business Press.

Weishäupl E, Yasasin E, Schryen G (2018) Information security investments: An exploratory multiple case study on decision-making, evaluation and learning. Computers & Security 77:807–823.

White D, Fortune J (2002) Current practice in project management—An empirical study. International Journal of Project Management 20(1):1–11.

Whitmore A, Agarwal A, Da Xu L (2015) The Internet of Things—A survey of topics and trends. Information Systems Frontiers 17(2):261–274. doi:10.1007/s10796-014-9489-2.

Wilde T, Hess T (2007) Forschungsmethoden der wirtschaftsinformatik. Wirtschaftsinformatik 49(4):280–287.

Williams P (2001) Information security governance. Information security technical report 6(3):60–70.

Wolf T (2015) Assessing the Criticality of IT Projects in a Portfolio Context using Centrality Measures. 12th International Conference on Wirtschaftsinformatik (WI). In: Proceedings of the 12th International Conference on Wirtschaftsinformatik (WI).

Wu SP-J, Straub DW, Liang T-P (2015) How information technology governance mechanisms and strategic alignment influence organizational performance: Insights from a matched survey of business and IT managers. MIS Quarterly 39(2):497–518.

Zhang T, Havakhor T, Biros D (2019) Does Cybersecurity Slow Down Digitization? A Quasi-experiment of Security Breach Notification Laws. In: Proceedings of the 40th International Conference on Information Systems (ICIS).

Zimmermann S (2008) IT-Portfoliomanagement–Ein Konzept zur Bewertung und Gestaltung von IT. Informatik-Spektrum 31(5):460–468.

Zowghi D, Nurmuliani N A study of the impact of requirements volatility on software project performance. In: Ninth Asia-Pacific Software Engineering Conference, 2002. IEEE, pp 3–11.

8 Appendix

8.1 Research Papers Relevant to this Thesis[1]

Paper 1

Guggenmos, F.; Hackel, B.; Ollig, P; Stahl, B.

Security First, Security by Design, or Security Pragmatism – Strategic Roles of IT Security in Digitalization Projects

Submitted

Paper 2.1

Rieger, A.; Lockl, J.; Urbach, N.; Guggenmos, F.; Fridgen, G. (2019)

Building a Blockchain Application that Complies with the EU General Data Protection Regulation

In: MIS Quarterly Executive, 18(4)

(VHB Jourqual 3: Category B, SCI Impact Factor 2020: 4.088)

Paper 2.2

Guggenmos, F., Lockl, J., Rieger, A., Wenninger, A., & Fridgen, G. (2020)

How to Develop a GDPR-Compliant Blockchain Solution for Cross-Organizational Workflow Management: Evidence from the German Asylum Procedure

In: Proceedings of the 53rd Hawaii International Conference on System Sciences

(VHB Jourqual 3: Category C)

Paper 3

Guggenmos, F.; Amend, J.; Fridgen, G

Systemic risk might endanger your Project Portfolio – A Critical Overview of Systemic Risk Measures

To be submitted

[1] All papers can be found in the supplement. Kindly note that the text formatting and the reference style may differ from published papers, to allow for a consistent layout. There is a separate reference section, as well as a separate numbering of figures, tables, and footnotes for each paper.

Paper 4

Guggenmos, F., Hofmann, P.; Fridgen, G. (2019)

How ill is your IT Portfolio?: Measuring Criticality in IT Portfolios Using Epidemiology

In: Proceedings of the 40th International Conference on Information Systems

(VHB Jourqual 3: Category A)

8.2 Declaration of Co-authorship and Individual Contribution

In this section, I outline the individual contribution of all co-authors to the research papers included in this thesis. Signed copies declaring the authors' contributions to each paper have been submitted with this thesis. For this section, their content has been partially translated from German originals into English.

Paper 1: Security First, Security by Design, or Security Pragmatism – Strategic Roles of IT Security in Digitalization Projects

I co-authored this research paper with Philipp Ollig, Bastian Stahl, and Björn Häckel. The co-authors have contributed to the paper in the following way.

Guggenmos, Florian (equal co-authorship): Literature work, Input of know-how in the context of Design Science Research, Textual elaboration, Development of the artifact, Execution of the evaluation (Interviews)

Häckel, Björn (subordinate co-authorship): Support and scientific mentorship

Ollig, Philipp (equal co-authorship): Literature work, Input of know-how in the context of IT security, Textual elaboration, Development of the artifact, Execution of the evaluation (Interviews)

Stahl, Bastian (equal co-authorship): Suggestion and idea, Literature work, Input of know-how in the context of IT security, Textual elaboration, Development of the artifact, Execution of the evaluation (Interviews)

Paper 2.1: Building a Blockchain Application that Complies with the EU General Data Protection Regulation

I co-authored this research paper with Alexander Rieger, Jannik Lockl, Gilbert Fridgen, and Nils Urbach. The co-authors have contributed to the paper in the following way.

Rieger, Alexander (lead co-authorship): Conceptualization, Formal analysis, Investigation, Project administration, Visualization, Writing – original draft.

Guggenmos, Florian (subordinate co-authorship): Investigation, Validation, Writing – original draft.

Lockl, Jannik (subordinate co-authorship): Investigation, Methodology, Writing – review & editing.

Fridgen, Gilbert (subordinate co-authorship): Supervision, Writing – review & editing.

Urbach, Nils (subordinate co-authorship): Supervision, Writing – review & editing.

Paper 2.2: How to Develop a GDPR-Compliant Blockchain Solution for Cross-Organizational Workflow Management: Evidence from the German Asylum Procedure

I co-authored this research paper with Jannik Lockl, Alexander Rieger, Annette Wenninger, and Gilbert Fridgen. The co-authors have contributed to the paper in the following way.

Guggenmos, Florian (equal co-authorship): Conceptualization, Formal analysis, Investigation, Visualization, Writing – original draft.

Lockl, Jannik (equal co-authorship): Conceptualization, Investigation, Methodology, Writing – review & editing.

Rieger, Alexander (equal co-authorship): Conceptualization, Project administration, Validation, Writing – review & editing.

Wenninger, Annette (equal co-authorship): Conceptualization, Formal analysis, Investigation, Methodology, Writing – original draft.

Fridgen, Gilbert (subordinate co-authorship): Supervision, Writing – review & editing.

Paper 3: Systemic risk might endanger your Project Portfolio – A Critical Overview of Systemic Risk Measures

I co-authored this research paper with Julia Amend and Gilbert Fridgen. The co-authors have contributed to the paper in the following way.

Amend, Julia (equal co-authorship): Literature work, Textual elaboration, Execution of the evaluation/analysis

Guggenmos, Florian (equal co-authorship): Suggestion and idea, Literature work, Textual elaboration, Input of know-how in the context of systemic risk, Execution of the evaluation/analysis

Fridgen, Gilbert (subordinate co-authorship): Support and scientific mentorship, Input of know-how and feedback

Paper 4: How ill is your IT Portfolio?: Measuring Criticality in IT Portfolios Using Epidemiology

I co-authored this research paper with Peter Hofmann and Gilbert Fridgen. The co-authors have contributed to the paper in the following way.

Florian Guggenmos (lead co-authorship): Florian Guggenmos initiated and co-developed the research project. He contributed by conducting the literature analysis and interviews and developing and evaluating the on track or in difficulty method (the TD method). Further, he engaged in most of the textual elaboration. Additionally, he participated in research discussions and provided feedback on the paper's content and structure. Thus, Florian Guggenmos's co-authorship is reflected in the entire research project.

Peter Hofmann (subordinate co-author): Peter Hofmann co-developed the research project. He contributed by developing, instantiating, and evaluating the on track or in difficulty method (the TD method). Further, he engaged in textual elaboration, especially in the introduction, research method, and conclusion section. Additionally, he participated in research discussions and provided feedback on the paper's content

and structure. Thus, Peter Hofmann's co-authorship is reflected in the entire research project.

Gilbert Fridgen (subordinate co-author): Gilbert Fridgen provided mentorship, participated in research discussions, provided feedback on the paper's content and structure, and engaged in textual elaboration. Thus, Gilbert Fridgen's co-authorship is reflected in the entire research project.

8.3 Paper 1 - Security First, Security by Design, or Security Pragmatism – Strategic Roles of IT Security in Digitalization Projects

Authors: Florian Guggenmos, Björn Hackel, Philipp Ollig, Bastian Stahl

Extended Abstract[1]:

Digitalization is commonly associated with beneficial effects on the overall organizational performance, competitive advantage, and organizational effectiveness and efficiency (Devaraj and Kohli 2003; Goldfarb and Tucker 2019). To capitalize on these benefits of digitalization, organizations strive to develop IT capabilities enhancing their digital maturity (Röglinger et al. 2018). Even organizations whose core competence was not previously in digital solutions, such as industry or manufacturing, adapt digital technologies to enhance production flexibility or provide digital service-supported products (Margherita und Braccini 2020).

Organizations enhance their digital maturity through digitalization projects (Barthel und Hess 2019; Gimpel et al. 2018; Barthel und Hess 2020). These projects drive digital progress. However, they entail a plethora of challenges. Especially IT security has become a significant challenge for IT managers (Kappelman et al. 2020) as incidents have consequences for the affected organization and its stakeholders (Li et al. 2021). IT security incidents can lead to imminent costs due to data loss or system failure and indirect costs like loss of reputation. Thus, in the German industry, the damage caused by IT attacks between 2016 and 2018 amounted to 43 billion € (Berg und Haldenwang 2018). To avoid such consequences, organizations invest in IT security measures induced by several drivers (Li et al. 2021).

However, taking IT security into account can make sense not only from the perspective of risk minimization. Research indicates, under certain circumstances, that positive business values can be created by investing in IT security (Bose und Man Leung 2019; Cardholm 2016). Thus, IT security has evolved from a purely technical domain to a holistic management task and should be given a strategic role in digitalization projects (Soomro et al. 2016; Rothrock et al. 2018).

In practice, however, the strategic consideration of IT security is underrepresented in many organizations. Especially in

[1] At the time of this thesis' publication, this research paper is under review for publication in a scientific journal. Therefore, an extended abstract covering the paper's content is provided.

digitalization projects, the strategic integration of IT security is a crucial challenge (Vial 2019; Abolhassan 2017; Wu et al. 2015). Digitalization projects usually do not consider IT security to be a value lever. In some cases, IT security even is regarded as a barrier (Grahn et al. 2021). In addition, IT security measures in digitalization projects consume scarce resources and time, increasing the iron triangle's trade-off between time, cost, and quality or function (Atkinson 1999; Lech 2013). For this reason, organizations must consider the central drivers and requirements for IT security and at the same time, constantly question whether the requirements for IT security are not actually impeding the progress of the project. In particular, project managers should consider IT security in the early stages of project planning and define the strategic role for the project (Payette et al. 2015; Pinto und Prescott 1988).

Existing research has already identified specific drivers for IT security, e.g., industry-specific requirements in the healthcare sector (Angst et al. 2017). However, there is a lack of knowledge about how to utilize this knowledge and enable practitioners like project managers to position IT security according to the project's specifications strategically.

Therefore, this paper aims to support project managers in a systematic and differentiated evaluation of digitalization projects to determine IT security's strategic role considering the organization's strategic orientation and the industry-specific context. Building on essential works of IT security drivers and the IT security decision-making process, this paper strives to develop an artifact that aggregates these drivers and assists in choosing a strategic role of IT security. Thus, this paper answers the call of existing works to consider IT security strategically in project management (e.g., Payette et al. 2015) and software development (e.g., Straub 2020).

This paper followed a DSR approach (Hevner et al. 2004) and developed a method that enables assessing the strategic alignment of IT security in the early stages of digitalization projects. In a first step, it derived design specifications for the artifact and investigated the strategic alignment paths of IT security through an interview study. Fourteen interviews confirmed the existence of three strategic alignment paths regarding IT security within digitalization projects. The alignment path of Security First (SF) describes the prioritization of IT security. Second, Security by Design (SD) refers to progress in both domains under the maxim of continuous alignment. Third, Security Pragmatism (SP) refers to postponement or deprioritization of IT security. In line with existing research on IT security decision processes (Heidt et al. 2019a; Heidt et al. 2019b), this paper identified several internal and external drivers that impact the choice of

strategic path.

As part of our DSR approach, this paper developed an artifact that reconciled the drivers with the alignment paths within four iterations. The artifact's application enables organizations to evaluate digitalization projects differently based on the relevant drivers to select a suitable alignment path. To rigor evaluate the artifact, this paper followed Sonnenberg und vom Brocke (2012) and conducted both an ex-ante and an ex-post evaluation of the artifact.

The findings mainly underpin previous research findings in strategic decision-making and enhance these with a coherent conceptual artifact of three strategic ways to address IT security in digitalization projects. In doing so, this paper used the existing body of knowledge on decision-making as a theoretical lens to ground the artifact in theory and solve a real-world problem in an organizational context. Besides that, the method may support practitioners to reflect on existing digitalization projects and put them into context. The artifact supports project managers in finding a common perspective on IT security requirements and balance different stakeholder's requirements to achieve strategic alignment of IT security. Especially in the early phases of the project management process, the artifact offers a common frame and indicates strategic options for action and underlying motivations and triggers. Hence, using the artifact, managerial awareness for the value of IT security may be stimulated. Finally, the artifact helps to integrate IT security in digitalization projects and to map strategic decisions conceptually.

References

Abolhassan, Ferri (2017): Security: The Real Challenge for Digitalization. In: Ferri Abolhassan (Hg.): Cyber Security. Simply. Make it Happen. Leveraging Digitization Through IT Security. Cham: Springer International Publishing (Management for Professionals), S. 1–11.

Angst, Corey M.; Block, Emily S.; D'Arcy, John; Kelley, Ken (2017): When Do IT Security Investments Matter? Accounting for the Influence of Institutional Factors in the Context of Healthcare Data Breaches. In: MIS Quarterly 41 (3), S. 893–916. DOI: 10.25300/MISQ/2017/41.3.10.

Atkinson, Roger (1999): Project management: cost, time and quality, two best guesses and a phenomenon, its time to accept other success criteria. In: International Journal of Project Management 17 (6), S. 337–342. DOI: 10.1016/S0263-7863(98)00069-6.

Barthel, Philipp; Hess, Thomas (2019): Are Digital Transformation Projects Special? In: Proceedings of the 23rd Pacific Asia Conference on Information Systems (PACIS). Xi'an (China).

Barthel, Philipp; Hess, Thomas (2020): Towards a Characterization of Digitalization Projects in the Context of Organizational Transformation. In: PAJAIS 12 (3), S. 31–56. DOI: 10.17705/1pais.12302.

Berg, Achim; Haldenwang, Thomas (2018): Wirtschaftsschutz in der Industrie. bitkom. Berlin. Online verfügbar unter https://www.bitkom.org/sites/default/files/file/import/Bitkom-PK-Wirtschaftsschutz-Industrie-13-09-2018-2.pdf, zuletzt aktualisiert am 2018, zuletzt geprüft am 30.04.2020.

Bose, Indranil; Man Leung, Alvin Chung (2019): Adoption of Identity Theft Countermeasures and its Short- and Long-Term Impact on Firm Value. In: MIS Quarterly 43 (1), S. 313–327. DOI: 10.25300/MISQ/2019/14192.

Cardholm, Lucas (2016): Demonstrating Business Value of Security Investments in the Age of Digitalization. In: International Journal of Innovation in the Digital Economy 7 (3), S. 1–25. DOI: 10.4018/IJIDE.2016070101.

Devaraj, Sarv; Kohli, Rajiv (2003): Performance Impacts of Information Technology: Is Actual Usage the Missing Link? In: Management Science 49 (3), S. 273–289. DOI: 10.1287/mnsc.49.3.273.12736.

Gimpel, Henner; Hosseini, Sabiölla; Huber, Rocco Xaver Richard; 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 (JITTA) 19 (1), S. 31–54.

Goldfarb, Avi; Tucker, Catherine (2019): Digital Economics. In: Journal of Economic Literature 57 (1), S. 3–43. DOI: 10.1257/jel.20171452.

Grahn, Sten; Granlund, Anna; Lindhult, Erik (2021): Barriers to Value Specification when Carrying out Digitalization Projects. In: Technology Innovation Management Review 11 (5). Online verfügbar unter https://timreview.ca/article/1442.

Heidt, Margareta; Gerlach, Jin; Buxmann, Peter (2019a): A Holistic View on Organizational IT Security: The Influence of Contextual Aspects During IT Security Decisions. In: Proceedings of the 52nd Hawaii International Conference on System Sciences (HICSS). 52nd Hawaii International Conference on System Sciences. Maui, Hawaii, USA, January 8-11, 2019.

Heidt, Margareta; Gerlach, Jin P.; Buxmann, Peter (2019b): Investigating the Security Divide between SME and Large Companies: How SME Characteristics Influence Organizational IT Security Investments. In: Inf Syst Front 21 (6), S. 1285–1305. DOI: 10.1007/s10796-019-09959-1.

Hevner, Alan R.; March, Salvatore T.; Park, Jinsoo; Ram, Sudha (2004): Design Science in Information Systems Research. In: MIS Quarterly, S. 75–105.

Kappelman, Leon; L. Johnson, Vess; Maurer, Chris; Guerra, Katie; McLean, Ephraim; Torres, Russell et al. (2020): The 2019 SIM IT Issues and Trends Study. In: MISQE 19 (1), S. 69–104. DOI: 10.17705/2msqe.00026.

Lech, Przemysław (2013): Time, Budget, And Functionality?—IT Project Success Criteria Revised. In: Information Systems Management 30 (3), S. 263–275. DOI: 10.1080/10580530.2013.794658.

Li, He; Yoo, Sungjin; Kettinger, William J. (2021): The Roles of IT Strategies and Security Investments in Reducing Organizational Security Breaches. In: Journal of

management information systems 38 (1), S. 222–245. DOI: 10.1080/07421222.2021.1870390.

Margherita, Emanuele Gabriel; Braccini, Alessio Maria (2020): Industry 4.0 Technologies in Flexible Manufacturing for Sustainable Organizational Value: Reflections from a Multiple Case Study of Italian Manufacturers. In: Inf Syst Front. DOI: 10.1007/s10796-020-10047-y.

Payette, Jay; Anegbe, Esther; Caceres, Erika; Muegge, Steven (2015): Secure by Design: Cybersecurity Extensions to Project Management Maturity Models for Critical Infrastructure Projects. In: Technology Innovation Management Review 5 (6), S. 26–34. DOI: 10.22215/timreview/904.

Pinto, Jeffrey K.; Prescott, John E. (1988): Variations in Critical Success Factors Over the Stages in the Project Life Cycle. In: Journal of Management 14 (1), S. 5–18. DOI: 10.1177/014920638801400102.

Röglinger, Maximilian; Schwindenhammer, Lisa; Stelzl, Katharina (2018): How to Put Organizational Ambidexterity into Practice : Towards a Maturity Model. In: 16th International Conference on Business Process Management (BPM). 16th International Conference on Business Process Management. Sydney, NSW, Australia, September 9–14, 2018. Online verfügbar unter https://eref.uni-bayreuth.de/44763/.

Rothrock, Ray; Kaplan, James; van der Oord, Friso (2018): The Board's Role in Managing Cybersecurity Risks. In: MIT Sloan Management Review 59 (2), S. 12–15. Online verfügbar unter https://search.proquest.com/scholarly-journals/boards-role-managing-cybersecurity-risks/docview/1986317468/se-2?accountid=8429.

Sonnenberg, Christian; vom Brocke, Jan (2012): Evaluations in the science of the artificial–reconsidering the build-evaluate pattern in design science research. In: International Conference on Design Science Research in Information Systems: Springer, S. 381–397.

Soomro, Zahoor Ahmed; Shah, Mahmood Hussain; Ahmed, Javed (2016): Information security management needs more holistic approach: A literature review. In: International Journal of Information Management 36 (2), S. 215–225. DOI: 10.1016/j.ijinfomgt.2015.11.009.

Straub, Jeremy (2020): Software Engineering: The First Line of Defense for Cybersecurity. In: Wenzheng Li (Hg.): ICSESS 2020. Proceedings of 2020 IEEE 11th International Conference on Software Engineering and Service Science : October 16-18, 2020, China Hall of Science and Technology, Beijing, China. 2020 IEEE 11th International Conference on Software Engineering and Service Science (ICSESS). Beijing, China, 10/16/2020 - 10/18/2020. Piscataway, NJ: IEEE Press, S. 1–5.

Vial, Gregory (2019): Understanding digital transformation: A review and a research agenda. In: The Journal of Strategic Information Systems 28 (2), S. 118–144. DOI: 10.1016/j.jsis.2019.01.003.

Wu, Shelly Ping-Ju; Straub, Detmar W.; Liang, Ting-Peng (2015): How Information Technology Governance Mechanisms and Strategic Alignment Influence Organizational Performance: Insights from a Matched Survey of Business and IT

Managers. In: MIS Quarterly 39 (2), S. 497–518. DOI: 10.25300/MISQ/2015/39.2.10.

8.4 Paper 2.1 - Building a Blockchain Application that Complies with the EU General Data Protection Regulation

Authors: Alexander Rieger, Florian Guggenmos, Jannik Lockl, Gilbert Fridgen, Nils Urbach

Published in: MIS Quarterly Executive

Abstract: Complying with the EU General Data Protection Regulation (GDPR) poses significant challenges for blockchain projects, including establishing clear responsibilities for compliance, securing lawful bases for processing personal data, and observing rights to rectification and erasure. We describe how Germany's Federal Office for Migration and Refugees addressed these challenges and created a GDPR-compliant blockchain solution for cross-organizational workflow coordination. Based on the lessons learned, we provide three recommendations for ensuring blockchain solutions are GDPR-compliant.

8.5 Paper 2.2 - How to Develop a GDPR-Compliant Blockchain Solution for Cross-Organizational Workflow Management: Evidence from the German Asylum Procedure

Authors: Alexander Rieger, Florian Guggenmos, Jannik Lockl, Gilbert Fridgen, Nils Urbach

Published in: Proceedings of the 53th Hawaii International Conference on System Sciences (HICSS), Wailea, USA, 2020

Abstract: Blockchain technology has the potential to resolve trust concerns in cross-organizational workflows and to reduce reliance on paper-based documents as trust anchors. Although these prospects are real, so is regulatory uncertainty. In particular, the reconciliation of blockchain with Europe's General Data Protection Regulation (GDPR) is proving to be a significant challenge. We tackled this challenge with the German Federal Office for Migration and Refugees. Here, we explain how we used Action Research to guide the Federal Office in creating a GDPR-compliant blockchain solution for the German asylum procedure. Moreover, we explain the architecture of the Federal Office's solution and present two design principles for developing GDPR-compliant blockchain solutions for cross-organizational workflow management

8.7 Paper 3 - Systemic risk might endanger your Project and Project Portfolio – A Critical Overview of Systemic Risk Measures

Authors: Florian Guggenmos, Julia Amend, Gilbert Fridgen

Extended Abstract[2]:

The "Chaos Report" by Standish Group (2018) emphasizes the prevalence of information technology (IT) project failures and the importance of project management. According to this study, 45% of all IT projects are challenged, and 19% even fail. Furthermore, Flyvbjerg and Budzier (2011) specify that approximately 16% of all IT projects exceed their budget by 200%. A Radar Group (2012) survey concludes that opaqueness arising from dependencies between IT projects is one reason for these budget overruns. However, the question arises of how organizations should deal with such dependencies.

Different tasks within a project and different projects within an organization's project portfolio depend on each other in various ways. Regardless of whether considered projects are specifically related to IT or not, they may use the same infrastructure, require the same limited resources, or rely on other preceding projects' output. Therefore, on project management does not consider projects isolated but rather interconnected as complex project networks (Beer et al., 2015; Ellinas, 2019; Neumeier et al., 2018; Radszuwill and Fridgen, 2017; Wolf, 2015).

In complex networks, dependencies induce a specific type of risk, called systemic risk. Centeno et al. (2015) defined systemic risk generally as the threat that individual failures spread across systems through the process of contagion, also known as ‘cascade effects’. A well-known example of cascade effects is the COVID-19 pandemic. During the disease, the virus spreads through the population. Thereby, the infection of one person by another represents a single stage of the cascade effect. However, we can also observe cascading effects in projects and project portfolios. Cascade effects caused by a single failure and spread by dependencies may lead to a collapse of the entire project portfolio and, finally, result in significant financial losses or even bankruptcy (Beer et al., 2015).

Recent research in this field aims to quantitatively describe the effects of systemic risk in projects and project portfolios and, thus, improve the organizations’ project and portfolio

[2] At the time of this thesis’ publication, this research paper is a working paper to be submitted for publication in a scientific journal. Therefore, an extended abstract covering the paper’s content is provided.

management. Literature already knows risk measures that also account for systemic risk, further referred to as systemic risk measures. These systemic risk measures mainly focus on identifying critical projects within the project portfolio. For instance, Wolf (2015) investigated the suitability of commonly used centrality measures representing famous approaches in social networks research in the context of IT project portfolios. Other researchers transferred so-called 'network diffusion models' from the context of supply chain management (Guo et al., 2019) and epidemiology (Guggenmos et al., 2019). Further, Elinas et al. (2016; 2019) transferred ideas from load distribution models to investigate systemic risk, not in project portfolios but single projects due to dependent tasks. While these examples illustrate that research adopted systemic risk measures from other domains to projects and project portfolios, the characteristics of systemic risks in these domains differ significantly from projects and project portfolios. Consequently, the questions arise whether these risk measures consider the specific characteristics of projects and project portfolios and whether they are suitable for practical use against the backdrop of the available data.

This paper analyzes the specific characteristics of systemic risk in projects and project portfolios to support organizations choosing appropriate risk measures according to their available data to address these issues. This paper used a literature-based research approach to identify relevant risk measures that correspondingly enable us to determine the most critical projects in a project portfolio or determine the overall portfolio risk considering systemic risk. It conducted a structured literature search considering four project management journals and five scientific databases to identify promising systemic risk measures. The literature search resulted in seven systemic risk measures. Namely the alpha centrality (Bonacich and Lloyd, 2001), an integrated systemic risk quantification approach (Beer et al., 2015), a Bayesian network approach (Neumeier et al., 2018), the TD method (Paper 4), a general network approach (Ellinas, 2019), a flow redistribution model (Guo et al., 2019), and a vulnerability assessment model (Guo et al., 2020). This paper used a set of eight evaluation criteria derived from the literature and observation of a real-world project portfolio data set to analyze these systemic risk measures.

Finally, the analysis demonstrated that none of the systemic risk measures fits all criteria. However, the risk measure of Ellinas (2019) fulfills at least seven out of eight criteria followed by the TD method, the flow redistribution model, and the systemic risk measures of Beer et al. (2015) and Neumeier et al. (2018), which fulfill six out of eight criteria.

However, none of the analyzed systemic risk measures fit criterion 8, indicating a simultaneous consideration of dependencies' positive and negative effects. This paper concludes that previous research focused on analyzing risk and neglected an integrated view of opportunities and risk. However, research must not consider opportunities and risks isolated but integrated.

Generally, this paper provides two theoretical contributions. First, it provides a structured overview of existing systemic risk measures in the context of projects and project portfolios, which was yet missing in such a form. Second, it offers a set of criteria to analyze systemic risk measures in the context of projects and project portfolios. Such an updated set of criteria was also missing, as the one proposed by Wolf (2015) is rather outdated, and a re-assessment with a potential extension is reasonable. Besides that, this paper also provides one significant managerial contribution. The overview of analyzed systemic risk measures provides organizations suggestions on which risk measures might be suitable for their project and project portfolio management according to their available data.

Overall, the topic of measuring systemic risk still provides much room for further research, in general, and in the particular case of projects and project portfolios. For instance, it is challenging to model project portfolios as graphs because of missing information about dependencies in practice. In doing so, research in other fields like secure multi-party computation (cf. Zare-Garizy et al., 2018) provides promising solutions. Nevertheless, this paper's overview of systemic risk measures can serve as a first step to face high exposure to systemic risk due to the increasing number of interlaced IT projects. Based on the presented results, research and practice should consequently conduct continuing, detailed investigations of systemic risk in project portfolios and, thus, decrease the rate of project failures.

References:

Beer, M., Wolf, T., Zare Garizy, T., 2015. Systemic Risk in IT Portfolios – An Integrated Quantification Approach. to be presented at: 36th International Conference on Information Systems (ICIS), 2015, Fort Worth, USA.

Bonacich, P., Lloyd, P., 2001. Eigenvector-like measures of centrality for asymmetric relations. Social Networks 23 (3), 191–201.

Centeno, M.A., Nag, M., Patterson, T.S., Shaver, A., Windawi, A.J., 2015. The emergence of global systemic risk. Annual Review of Sociology 41, 65–85.

Ellinas, C., 2019. The domino effect: an empirical exposition of systemic risk across project networks. Production and Operations Management 28 (1), 63–81.

Ellinas, C., Allan, N., Johansson, A., 2016. Project systemic risk: Application examples of a network model. International Journal of Production Economics 182, 50–62.

Flyvbjerg, B., Budzier, A., 2011. Why Your IT Project May Be Riskier Than You Think. Harvard Business Review 89, 23–25.

Guggenmos, F., Hofmann, P., Fridgen, G., 2019. How ill is your IT Portfolio?– Measuring Criticality in IT Portfolios Using Epidemiology to be presented at: 40th International Conference on Information Systems (ICIS).

Guo, N., Guo, P., Dong, H., Zhao, J., Han, Q., 2019. Modeling and analysis of cascading failures in projects: A complex network approach. Computers & Industrial Engineering 127, 1–7.

Guo, N., Guo, P., Madhavan, R., Zhao, J., Liu, Y., 2020. Assessing the Vulnerability of Megaprojects Using Complex Network Theory. Project Management Journal 51 (4), 429–439.

Neumeier, A., Radszuwill, S., Garizy, T.Z., 2018. Modeling project criticality in IT project portfolios. International Journal of Project Management 36 (6), 833–844.

Radar Group, 2012. The Impact of Data Silos in IT Planning (White Paper).

Radszuwill, S., Fridgen, G., 2017. Forging a Double-Edged Sword: Resource Synergies and Dependencies in Complex IT Project Portfolios.

Standish Group, 2013. ChaosManifesto.

The Standish Group, 2018. Decision latency theory: It is all about the interval. Chaos Report. The Standish Group.

Wolf, T., 2015. Assessing the Criticality of IT Projects in a Portfolio Context using Centrality Measures. 12th International Conference on Wirtschaftsinformatik (WI), März 2015, Osnabrück, Germany.

Zare-Garizy, T., Fridgen, G., Wederhake, L., 2018. A privacy preserving approach to collaborative systemic risk identification: the use-case of supply chain networks. Security and Communication Networks 2018.

8.8 Paper 4 - How ill is your IT Portfolio?: Measuring Criticality in IT Portfolios Using Epidemiology

Authors: Florian Guggenmos, Peter Hofmann, Gilbert Fridgen

Published in: Proceedings of the 40th International Conference on Information Systems (ICIS), Munich, Germany, 2019

Abstract: IT project portfolios, consisting of IT projects, also interact with the entire IT landscape. In case of a failure of only one element, existing dependencies can lead to a cascade failure, which can cause high losses. Despite the present effects of systemic risk, research into IT portfolio management lacks suitable methods to quantitatively assess systemic risk. We follow the design science research paradigm to develop and evaluate our 'on track' or 'in difficulty' (TD) method by applying the SI model, representing a recognized network diffusion model in epidemiology, in an IT portfolio context. We evaluate our method using a real-world dataset. We introduce a criticality measure for diffusion models in IT portfolios and compare the TD method's results and the alpha centrality to human judgment as a benchmark. From our evaluation, we conclude that the TD method outperforms alpha centrality and is a suitable risk measure in IT portfolio management.