Universität
Augsburg
University

Systemic Risk Assessment in Complex Network Structures

Information Technology as a Challenge and a Chance

Kumulative Dissertation

Der Wirtschaftswissenschaftlichen Fakultät

der Universität Augsburg

zur Erlangung des Grades eines

Doktors der Wirtschaftswissenschaften

(Dr. rer. pol.)

Vorgelegt von

Tirazheh Zare Garizy

(Master of Engineering)

Erstgutachter: Prof. Dr. Hans Ulrich Buhl

Zweitgutachter: Prof. Dr. Michael Krapp

Vorsitzender der mündlichen Prüfung: Prof. Dr. Yarema Okhrin

Tag der mündlichen Prüfung: 03.04.2017

Table of Contents

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

Index of Research Papers

This doctoral thesis contains the following research papers.

Research Paper 1

Zare Garizy T (2016) Bayesian Network Modelling for Assessing the Criticality of IT Projects in a Portfolio Context. Working paper.

VHB-JOURQUAL 3: --

Research Paper 2

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), Fort Worth, Texas, USA, December 2015

VHB-JOURQUAL 3: category A

Research Paper 3

Zare Garizy T, Fridgen G, Wederhake L (2016) Systemic Risk in Supply Chain Networks – A Privacy Preserving Approach for Collaborative Analysis. Working paper[1].

VHB-JOURQUAL 3: --

[1] Research Paper 3 is an extended version of Fridgen and Zare Garizy (2015) accepted and presented at ECIS 2015 (VHB-JOURQUAL 3: B). Research Paper 3 includes detailed information on the developed artifact, pseudocode of the artifact, and a detailed description of the artifact's code. This leads to a difference of more than 30% between the current journal version and the previously published ECIS 2015 paper.

I Introduction

Digitalization and globalization are the two main drivers of the increment in the level of connectedness in today's global systems (Helbing 2013; Gimpel and Röglinger 2015). Despite the promising socio-economic benefits and opportunities of high connectivity between systems, these global systems are vulnerable to failure (Helbing 2013). In March 2011, an earthquake in Tohoku, Japan affected Toyota's production system for more than three months, while some of its production lines were affected for up to six months (Matsuo 2015). This disruption happened to Toyota because Denso - a supplier of Toyota - could not comply with Toyota's demand for automotive microcontroller units manufactured by Renesas Electronics which was located at Tohoku (Matsuo 2015). The disruption therefore was due to a tier two supplier of Toyota having lost their facilities in the area affected by the earthquake.

The earthquake in Tohoku in 2011, the flood crisis in Thailand in 2011, the cloud computing strike outage in Dublin in 2011, the global financial crisis of 2007-2009, and the electrical blackout in Italy in 2003 are only a few examples of recent disruptive events that created systemic risk and caused costly system disruptions (Hall 2004; Chopra and Sodhi 2014; Matsuo 2015; Acharya et al. 2010; Buldyrev et al. 2010; Keller and König 2014; Miller 2011). There are many types of disruptive events (e.g. natural disasters, financial crashes, food shortages, organized crime, or cyberwar), that can bring along systemic risk on a global scale (Helbing 2013). While systemic risk is a fundamental concept in the analysis of financial systems (Bandt and Hartmann 2000) it is becoming increasingly important in analyzing other systems as well. For instance, the concept of systemic risk can be applied to analyze today's supply chain networks which consist of inter-tier connections, cycles and feedback loops with rather *network structures* than *chains* (Ledwoch et al. 2016). Analyzing health systems, financial systems, supply chain networks, or information systems reveals that most of these systems are subject to systemic risk due to their complex network structures (Helbing 2013; Acemoglu et al. 2015). Complex network structures "are graphs with non-trivial topological features; they display patterns of connectivity between their elements that are neither purely regular nor purely random" (Vrabič et al. 2012).

Systemic risk is "the threat that individual failures, accidents, or disruptions present to a system through the process of contagion." (Centeno et al. 2015). Systemic risk is not only the risk of isolated, independent failure, but the emerging risk due to the cascading effect of a failure within the interconnected systems (Helbing 2013). Such cascading effects (also called domino effects) have an impact on the system's performance and can lead to a system crisis (Ellinas et al. 2016; Acemoglu et al. 2015). The potential severity of such system crises emphasizes the importance of the assessment of systemic risk (Cetina et al. 2016; Helbing 2013).

Considering the assessment of systemic risk in complex network structures, information technology (IT) is, in metaphorical terms, a *man wearing two hats* (cf. Figure 1). On the one hand, today's large and complex IT project portfolios (ITPP) are subject to systemic risk (Zhang 2016; Wolf 2015; Ellinas et al. 2016), which turns IT (projects) into a challenge for organizations. On the other hand, organizations that handle the challenges of IT can profit from IT solutions in the assessment of systemic risk of their underlying systems (in Research Paper 3, their supply chain network). It should be noted that Fridgen (2010) introduced a similar approach and regarded two different roles of IT in his work. The work of Fridgen (2010) accounts for IT as an enabler of risk/return management and also assesses the associated risk of IT outsourcing projects (see also Buhl et al. (2009), Fridgen (2009), Fridgen and Müller (2009), and Buhl and Fridgen (2011)). However, he did not account for systemic risk and did not provide solutions for the assessment of systemic risk. This doctoral thesis especially regards the *assessment of systemic risk* in complex network structures and accounts for the role of IT, alongside.

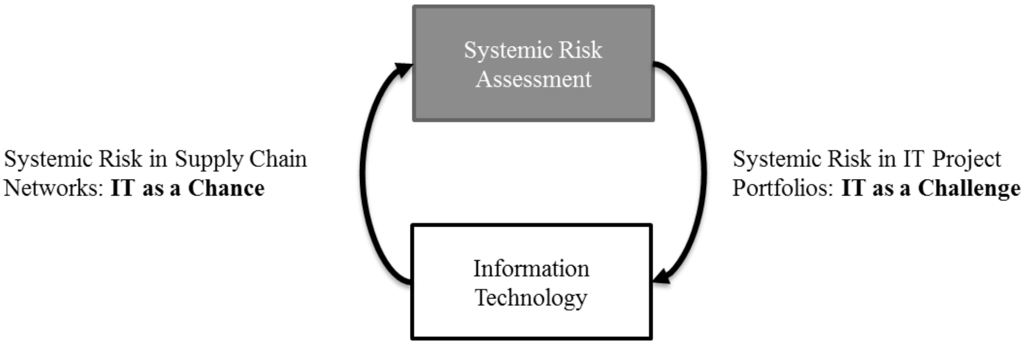

Systemic Risk Assessment
Systemic Risk in Supply Chain Networks: **IT as a Chance**
Systemic Risk in IT Project Portfolios: **IT as a Challenge**
Information Technology

Figure 1. IT as a challenge and a chance for organizations[1]

Many system disruptions in the digital world result from the lack of comprehensive understanding of the network structure of these systems (Helbing 2013). To avoid costly system disruptions, it is important to invest in systemic risk assessment solutions which enable better understanding of individual components of these systems, as well as the dependencies between these systems (Ackermann et al. 2007; Helbing 2013; Zhang 2016).

[1] Inspired by Fridgen (2010)

A network interpretation of the complex structure of systems allows for the development of solutions to gain a deeper understanding of individual components and the dependence structures of the systems. These solutions can utilize as established methods either centrality measures (Wasserman and Faust 2009; Newman 2013) or probabilistic graphical models (Killen and Kjaer 2012). On the one hand, centrality measures are suitable approaches for quantitatively analyzing the patterns of dependencies in networks and capturing specific features of its nodes (Newman 2013; Freeman 1977; Wasserman and Faust 2009). Examples of commonly used centrality measures in the assessment of systemic risk are betweenness centrality and alpha centrality (Kim et al. 2011; Wolf 2015; Bonacich and Lloyd 2001). On the other hand, probabilistic graphical models are suitable for dealing with the uncertainty and complexity of systems (Jordan 1999). Considering various probabilistic graphical models, Bayesian network modeling is identified a well-established method for systemic risk analysis (Khakzad et al. 2013).

Application of centrality measures or Bayesian network modeling for systemic risk assessment presupposes knowing the network structure (adjacency matrix) of the systems beforehand. Considering individual components of the systems as nodes and the dependencies between the nodes as edges result in the adjacency matrix of a system. However, retrieving all the information that composes the network structure, especially in global systems such as supply chain networks, is not a trivial task (Kim et al. 2011). IT can enable both the retrievement of information on the network structure of these systems and the aggregation (Kerschbaum et al. 2011; Helbing 2013) for utilizing and applying the aforementioned methods in the assessment of systemic risk. The development of suitable IT solutions requires data-driven solutions and close collaboration between real-life techno-socio-economic-environmental systems (Helbing 2013). These IT solutions support decision makers in better assessment of systemic risk, e.g., in forecasting the dissemination and the effects of failures, or quantifying estimated overall damage (Mertens and Barbian 2015).

IT solutions can support organizations in collecting the required information and assessing systemic risk. However, in many systems - and especially in supply chain networks – a further challenge arises, since, due to the lack of trust and fear of losing their competitive advantages, many organizations are unwilling to disclose or share information of their underlying business network (Kerschbaum et al. 2011; Blackhurst et al. 2005). This results in a scarcity of real-time data on supply chain networks, which poses a major problem for adequate risk assessment in supply chain networks using on the aforementioned methods (Wolfgang et al. 2008; Kim et al. 2011; Blackhurst et al. 2005). The application of cryptography approaches (e.g. secure multiparty computation (Yao 1986)) in systemic risk assessment methods can improve the applicability of these methods. Solutions developed based on these approaches can enable the assessment of systemic risk with privacy preserving information sharing between organizations. These privacy preserving approaches reduce the risk of losing the competitive advantage by sharing information. In summary, IT provides a chance for organizations to proactively assess the systemic risk and to reduce privacy concerns coming along with its application (Helbing 2013).

The development of suitable IT solutions for the assessment of systemic risk in global networks is one of the grand challenges of IT in the next years (Mertens and Barbian 2015; GI 2014). Digitalization intensifies the challenge and forces organizations to develop innovative IT solutions to sustain their competitiveness (Nguyen and Mutum 2012; Urbach and Ahlemann 2016). In 2017, the worldwide IT spending is expected to reach $3.5 trillion, which includes 7.2 percent growth in software spending to a total of $357 billion (van der Meulen 2016). Such growth implies an increasing number of IT projects within organizations and a growing proportion of their budget being allocated to those IT projects (Cha et al. 2009; Dahlberg et al. 2015).

However, an average cost overrun of 200%, an average schedule overrun of 70% by one out of six IT projects (Flyvbjerg and Budzier 2011), and a failure rate of 19% (Hastie and Wojewoda 2015) emphasize the complexity of successfully managing IT (projects). Furthermore, organizations often execute IT projects in an IT project portfolio (ITPP) (Bathallath et al. 2016a). In these ITPPs, the failure of a single IT project can cascade and cause severe value disruptions within the ITPP and its connected systems (Nelson 2007; Helbing 2013). Therefore, organizations need to invest in the assessment of systemic risk of IT projects and ITPPs to be able to proactively manage their associated risks (Zhang 2016; Bathallath et al. 2016b; Carlo et al. 2008).

To assess the systemic risk within ITPPs it is important to consider both its individual components (e.g. IT projects) and the dependencies between these components. Extensive information systems publications consider dependencies to be an important feature of many IT projects (Aaker and Tyebjee 1978; Santhanam and Kyparisis 1996; Lee and Kim 2001; Bardhan et al. 2004; Eilat et al. 2006; Kundisch and Meier 2011; Buhl 2012; Meier et al. 2016).

Dependency is the relationship between two IT projects, by which the state (e.g. success or failure) of one IT project is correlated or influenced by the state of another (Rinaldi et al. 2001; Cho 2010; Fridgen and Müller 2011). Dependencies between IT projects thus bear the risk that an IT project's success being affected by one or more of its dependent IT projects or by the availability of its required resources (Buhl 2012). For example, the delay of an IT project is often caused by the delay of its predecessor IT project (Buhl 2012). On the other hand, dependencies between IT projects may also lead to higher value creation. For example, an IT infrastructure project, which as a standalone project might not create high value, could enable another IT project, so that their completion leads to significant value creation for the organization (Bardhan et al. 2004). Resource dependencies and technical dependencies are common categories of dependencies between IT projects (Aaker and Tyebjee 1978; Bardhan et al. 2004; Lee and Kim 2001; Wehrmann et al. 2006; Lee 2008; Fridgen et al. 2015). When considering time as a component in analyzing dependencies, IT projects can be classified as inter- or intratemporally dependent (Zimmermann 2008; Embrechts et al. 2009; Meier and Zimmermann 2015). Dependencies between IT projects can be hard (negative), when an IT project is prerequisite to another, soft (positive), when an IT project enhances another, or soft (negative), when two IT projects cannibalize each other (Bardhan et al. 2004; Angelou and Economides 2008).

The challenge in the assessment of systemic risk in ITPPs is to develop a comprehensive network modelling approach that allows for the integration of the different categories of dependencies. There are first approaches towards the modelling of ITPPs as networks (Wolf 2015; Bathallath et al. 2016a); however, these approaches have some shortcomings, especially in quantifying and integrating the aforementioned dependencies. Therefore, it is necessary to invest in approaches to integrate and quantify dependencies to utilize the aforementioned methods (e.g. centrality measure, Bayesian network modelling) for the assessment of systemic risk (Dwivedi et al. 2015; Müller et al. 2015; Helbing 2013). These approaches should empower decision makers in the assessment of systemic risk and serve as the first step towards the management of the challenges of systemic risk in ITPPs (Khan and Burnes 2007; Hallikas et al. 2004). Furthermore, these methods should serve for a better alignment of IT projects with the organization's strategy (Bathallath et al. 2016b).

Altogether, the assessment of systemic risk in complex network structures and the role of IT, respectively, reveal great potential for research to address the current challenges practitioner and researchers face. This doctoral thesis elaborates on the assessment of systemic risk of IT projects and ITPPs as the first step in proactive management of their associated risks, in order to attain a higher success rate of IT projects. Organizations which handle the challenges of IT can profit from IT solutions in the assessment of systemic risk. Furthermore, this doctoral thesis introduces a privacy preserving IT solution for the assessment of systemic risk in supply chain networks. The following section (Section I.1) illustrates the objectives and structure of this doctoral thesis. Section I.2 describes the research context and embeds included research papers into the context of this doctoral thesis.

I.1 Objectives and Structure

The objective of this doctoral thesis is to provide solutions for the assessment of systemic risk in complex network structures, and the role of IT, respectively. In this context, the thesis studies the two roles of IT as a challenge and as a chance for organizations. Table 1 provides an overview of the objectives of this doctoral thesis.

Table 1. Objectives and Structure of this Doctoral Thesis

I Introduction	
Objective I.1:	Outlining the objectives and the structure of the doctoral thesis
Objective I.2:	Motivating the research context and embedding included research papers into the context of the doctoral thesis
II Systemic Risk in IT Project Portfolios: IT as a Challenge (Research Papers 1 and 2)	
Objective II.1:	Assessing systemic risk of single IT projects within an IT project portfolio
Objective II.2:	Integrating systemic risk assessment in the IT project portfolio evaluation
III Systemic Risk in Supply Chain Networks: IT as Chance (Research Paper 3)	
Objective III.1:	Developing an IT solution to assess the systemic risk within supply chain networks preserving the privacy of organizations
IV Conclusion	
Objective IV.1:	Presenting the findings of this doctoral thesis
Objective IV.2:	Addressing the direction of future research

I.2 Research Context and Research Questions

The following sections motivate the research questions of chapters II & III and the included research papers (Research Papers 1-3), respectively. Each section addresses one of the aforementioned roles of IT in organizations.

I.2.1 Chapter II: Systemic Risk in IT Project Portfolios: IT as a Challenge

Research Paper 1: *"Bayesian Network Modelling for Assessing the Criticality of IT Projects in a Portfolio Context"*

Due to the dependence structures of ITPPs, the failure of an IT project may cascade into the ITPP and may cause disruptions to other projects. To proactively identify and manage the systemic risk and avoid its consequences for the organization, it is important to invest in the assessment of the criticality of IT projects within ITPPs. The criticality assessment includes not only the analysis of independent failures, but also the associated risk due to the cascading effect of failure within the interconnected systems, and the economic impact of the failure (Theoharidou et al. 2009). Research Paper 1 provides a holistic method for the criticality assessment of IT projects in an ITPP context. For this purpose, the paper identifies the requirements for the criticality assessment of IT projects in the context of ITPP. Further, the paper evaluates the application of Bayesian network modelling for IT project criticality assessment. Bayesian network modelling is an accurate method which is widely used for criticality assessment in, for example, financial portfolios (Shenoy and Shenoy 1999), the railway industry (Marsh and Bearfield 2004), off-shore installation in the oil and gas industry (Ren et al. 2009), chemical process plants (Khakzad et al. 2013), and maritime transportation (Trucco et al. 2008). Accordingly, Research Paper 1 addresses the following research question:

> RQ 1. Can Bayesian network modelling serve to assess the criticality of IT projects within an ITPP, considering the associated effects of failure based on the economic impact and dependencies between IT projects?

Research Paper 2: *"Systemic Risk in IT Portfolios – An Integrated Quantification Approach"*

Besides the assessment of the criticality of IT projects, it is necessary to develop rigorous methods to consider the assessment of systemic risk in a value-based evaluation of ITPPs. These valuation methods should serve for a better alignment of IT projects in organizations' strategies. Research Paper 2 provides a solution inspired by the portfolio theory of Markowitz

(1952), which enhances existing IT project evaluation methods (Beer et al. 2013; Fridgen et al. 2015) by considering systemic risk for a holistic ITPP evaluation method. Thus, Research Paper 2 addresses the following research question:

> RQ 2. How can costs, benefits, risks, and different types of dependencies be integrated into a value-based ITPP evaluation method?

I.2.2 Chapter III: Systemic Risk in Supply Chain Networks: IT as a Chance

Research Paper 3: *"*Systemic Risk in Supply Chain Networks – A Privacy Preserving Approach for Collaborative Analysis*"*

Considering organizations in the supply chain network as nodes and the economic dependencies (e.g. material or financial flow) between them as edges, a supply chain network can be considered as a network structure (Kim et al. 2011). This structure of a supply chain network and the positioning of organizations within the network plays an important role in its vulnerability or robustness (Kim et al. 2011; Serdarasan 2013). A number of scholars have evaluated the applicability of centrality measures in order to analyze supply chain networks (Mizgier et al. 2013; Kim et al. 2011). Considering different centrality measures, the betweenness centrality can serve as a suitable measure for identifying organizations that have high impact on the supply chain network's performance. A fault in an organization with high impact can cause severe value disruptions. On the one hand, application of centrality measures requires availability of the information on each organization (node) and it connections (edges) within the supply chain network. On the other hand, organizations are concerned about their competitiveness and about risking their strategic connections by exchanging this information (Kerschbaum et al. 2011; Blackhurst et al. 2005). Therefore, the development of IT solutions which apply well-established methods of cryptography like secure multiparty computation (Yao 1986; Cramer et al. 2010) can provide a solution in the assessment of criticality in a supply chain network without risking organizations' competitiveness. To summarize, Research Paper 3 addresses the following research question:

> RQ 3. How can methods of network studies and cryptography serve to assess systemic risk in supply chain networks while preserving the privacy of organizations?

I.2.3 Chapter IV: Conclusion and Future Research

Chapter IV contains the conclusion and key findings of this doctoral thesis. Further, it outlines the areas of future research in the assessment of systemic risk in ITPPs and addresses further potential of IT in the assessment of systemic risk in today’s complex network structures.

I.3 References

Aaker DA, Tyebjee TT (1978) A model for the selection of interdependent R&D projects. IEEE Trans. Eng. Manage. EM-25(2):30–36. doi: 10.1109/TEM.1978.6447279

Acemoglu D, Ozdaglar A, Tahbaz-Salehi A (2015) Networks, Shocks, and Systemic Risk. National Bureau of Economic Research, Cambridge, MA

Acharya VV, Brownlees C, Engle R, Farazmand F, Richardson M, Cooley TF, Walter I (2010) Measuring Systemic Risk. In: Regulating Wall Street. John Wiley & Sons, Inc, pp 85–119

Ackermann F, Eden C, Williams T, Howick S (2007) Systemic risk assessment: A case study. J Oper Res Soc 58(1):39–51. doi: 10.1057/palgrave.jors.2602105

Angelou GN, Economides AA (2008) A Decision Analysis Framework for Prioritizing a Portfolio of ICT Infrastructure Projects. IEEE Trans. Eng. Manage. 55(3):479–495. doi: 10.1109/TEM.2008.922649

Bandt O de, Hartmann P (2000) Systemic risk: a survey. http://sdw.zentral-bank.eu/pub/pdf/scpwps/ecbwp035.pdf. Accessed 16 December 2016

Bardhan I, Bagchi S, Sougstad R (2004) Prioritizing a Portfolio of Information Technology Investment Projects. Journal of Management Information Systems 21(2):33–60. doi: 10.1080/07421222.2004.11045803

Bathallath S, Smedberg Å, Kjellin H (2016a) Managing project interdependencies in IT/IS project portfolios: a review of managerial issues. Developing and enforcing internal information systems standards: InduMaker's 4(1):67–82

Bathallath S, Smedberg Å, Kjellin H (2016b) Project Interdependency Management in IT/IS Project Portfolios: From a Systems Perspective. Procedia Computer Science 100:928–934. doi: 10.1016/j.procs.2016.09.250

Beer M, Fridgen G, Müller H, Wolf T (2013) Benefits Quantification in IT Projects. In: 11th International Conference on Wirtschaftsinformatik, pp 707–720

Blackhurst J, Craighead CW, Elkins D, Handfield RB (2005) An empirically derived agenda of critical research issues for managing supply-chain disruptions. International Journal of Production Research 43(19):4067–4081. doi: 10.1080/00207540500151549

Bonacich P, Lloyd P (2001) Eigenvector-like measures of centrality for asymmetric relations. Social Networks 23(3):191–201. doi: 10.1016/S0378-8733(01)00038-7

Buhl HU (2012) The Contribution of Business and Information Systems Engineering to the Early Recognition and Avoidance of "Black Swans" in IT Projects. Bus Inf Syst Eng 4(2):55–59. doi: 10.1007/s12599-012-0206-8

Buhl HU, Fridgen G (2011) IT-Enabled Risk/Return Management: Service-Oriented Infrastructures vs. Dedicated Systems. In: 19th European Conference on Information Systems

Buhl HU, Fridgen G, Hackenbroch W (2009) An Economic Analysis of Service-Oriented Infrastructures for Risk/Return Management. In: 17th European Conference on Information Systems, p 2.060

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

Carlo J, Lyytinen K, Boland R (2008) Systemic risk, information technology artifacts, and high reliability organizations: A case of constructing a radical architecture. All Sprouts Content 4(4)

Centeno MA, Nag M, Patterson TS, Shaver A, Windawi AJ (2015) The Emergence of Global Systemic Risk. Annu. Rev. Sociol. 41(1):65–85. doi: 10.1146/annurev-soc-073014-112317

Cetina J, Rajan S, Paddrik ME (2016) Stressed to the Core: Counterparty Concentrations and Systemic Losses in CDS Markets. OFR WP 16:1

Cha HS, Pingry DE, Thatcher ME (2009) What determines IT spending priorities? Commun. ACM 52(8):105. doi: 10.1145/1536616.1536644

Cho WJ (2010) IT portfolio selection and IT synergy, University of Illinois at Urbana-Champaign

Chopra S, Sodhi MS (2014) Reducing the risk of supply chain disruptions. MIT Sloan Management Review 55(3):73

Cramer R, Damgard I, Nielsen JB (2010) Secure multiparty computation and secret sharing-an information theoretic approach. Citeseer

Dahlberg T, Kivijarvi H, Saarinen T (2015) The Role of IT Investment Consistency among the Enablers behind the Success of IT Deployment. In: 48th Hawaii International Conference on System Sciences (HICSS), pp 5462–5471

Dwivedi YK, Wastell D, Laumer S, Henriksen HZ, Myers MD, Bunker D, Elbanna A, Ravishankar MN, Srivastava SC (2015) Research on information systems failures and successes: Status update and future directions. Inf Syst Front 17(1):143–157. doi: 10.1007/s10796-014-9500-y

Eilat H, Golany B, Shtub A (2006) Constructing and evaluating balanced portfolios of R&D projects with interactions: A DEA based methodology. European Journal of Operational Research 172(3):1018–1039. doi: 10.1016/j.ejor.2004.12.001

Ellinas C, Allan N, Johansson A (2016) Project systemic risk: Application examples of a network model. International Journal of Production Economics 182:50–62. doi: 10.1016/j.ijpe.2016.08.011

Embrechts P, Nešlehová J, Wüthrich MV (2009) Additivity properties for Value-at-Risk under Archimedean dependence and heavy-tailedness. Insurance: Mathematics and Economics 44(2):164–169

Flyvbjerg B, Budzier A (2011) Why Your IT Project May Be Riskier than You Think. SSRN Electronic Journal. doi: 10.2139/ssrn.2229735

Freeman LC (1977) A Set of Measures of Centrality Based on Betweenness. Sociometry 40(1):35. doi: 10.2307/3033543

Fridgen G (2009) Using a Grid for Risk Management: Communication Complexity of Covariance Calculations. In: 15th Americas Conference on Information Systems

Fridgen G (2010) Information Technology: Instrument and Object of Risk/Return Management. Dissertation, University of Augsburg

Fridgen G, Klier J, Beer M, Wolf T (2015) Improving Business Value Assurance in Large-Scale IT Projects? A Quantitative Method Based on Founded Requirements Assessment. ACM Transactions on Management Information Systems 5(3):11/1

Fridgen G, Müller H (2009) Risk/Cost Valuation of Fixed Price IT Outsourcing in a Portfolio Context. In: 30th International Conference on Information Systems

Fridgen G, Müller H (2011) An Approach for Portfolio Selection in Multi-Vendor IT Outsourcing. In: 32nd International Conference on Information Systems

Fridgen G, Zare Garizy T (2015) Supply Chain Network Risk Analysis: A Privacy Preserving Approach. In: 23rd European Conference on Information Systems (ECIS)

GI (2014) The Grand Challenges der Informatik. https://www.gi.de/themen/grand-challenges/systemische-risiken.html. Accessed 12 October 2016

Gimpel H, Röglinger M (2015) Digital Transformation: Changes and Chances: Insights based on an Empirical Study. http://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/542/wi-542.pdf

Hall PV (2004) "We'd Have to Sink the Ships": Impact Studies and the 2002 West Coast Port Lockout. Economic Development Quarterly 18(4):354–367. doi: 10.1177/0891242404269500

Hallikas J, Karvonen I, Pulkkinen U, Virolainen V, Tuominen M (2004) Risk management processes in supplier networks. International Journal of Production Economics 90(1):47–58. doi: 10.1016/j.ijpe.2004.02.007

Hastie S, Wojewoda S (2015) Standish Group 2015 Chaos Report - Q&A with Jennifer Lynch. https://www.infoq.com/articles/standish-chaos-2015

Helbing D (2013) Globally networked risks and how to respond. Nature 497(7447):51–59. doi: 10.1038/nature12047

Jordan MI (ed) (1999) Learning in graphical models, 1. MIT Press ed. Adaptive computation and machine learning. MIT Press, Cambridge, Mass.

Keller R, König C (2014) A Reference Model to Support Risk Identification in Cloud Networks. In: 35th International Conference on Information Systems

Kerschbaum F, Schroepfer A, Zilli A, Pibernik R, Catrina O, Hoogh S de, Schoenmakers B, Cimato S, Damiani E (2011) Secure Collaborative Supply-Chain Management. Computer 44(9):38–43. doi: 10.1109/MC.2011.224

Khakzad N, Khan F, Amyotte P, Cozzani V (2013) Domino effect analysis using Bayesian networks. Risk Anal 33(2):292–306. doi: 10.1111/j.1539-6924.2012.01854.x

Khan O, Burnes B (2007) Risk and supply chain management: Creating a research agenda. Int Jrnl Logistics Management 18(2):197–216. doi: 10.1108/09574090710816931

Killen CP, Kjaer C (2012) Understanding project interdependencies: The role of visual representation, culture and process. International Journal of Project Management 30(5):554–566. doi: 10.1016/j.ijproman.2012.01.018

Kim Y, Choi TY, Yan T, Dooley K (2011) Structural investigation of supply networks: A social network analysis approach. Journal of Operations Management 29(3):194–211. doi: 10.1016/j.jom.2010.11.001

Kundisch D, Meier C (2011) IT/IS project portfolio selection in the presence of project interactions-review and synthesis of the literature. In: Wirtschaftsinformatik Proceedings, Paper 64

Ledwoch A, Brintrup A, Mehnen J, Tiwari A (2016) Systemic Risk Assessment in Complex Supply Networks. IEEE Systems Journal:1–12. doi: 10.1109/JSYST.2016.2596999

Lee EA (2008) Cyber Physical Systems: Design Challenges. http://www2.eecs.berkeley.edu/Pubs/TechRpts/2008/EECS-2008-8.html

Lee JW, Kim SH (2001) An integrated approach for interdependent information system project selection. International Journal of Project Management 19(2):111–118. doi: 10.1016/S0263-7863(99)00053-8

Markowitz H (1952) Portfolio Selection. The Journal of Finance 7(1):77–91. doi: 10.1111/j.1540-6261.1952.tb01525.x

Marsh W, Bearfield G (2004) Using Bayesian Networks to Model Accident Causation in the UK Railway Industry. In: Spitzer C, Schmocker U, Dang VN (eds) Probabilistic Safety Assessment and Management. Springer London, London, pp 3597–3602

Matsuo H (2015) Implications of the Tohoku earthquake for Toyota′s coordination mechanism: Supply chain disruption of automotive semiconductors. International Journal of Production Economics 161:217–227. doi: 10.1016/j.ijpe.2014.07.010

Meier C, Kundisch D, Willeke J (2016) Is it Worth the Effort? Bus Inf Syst Eng. doi: 10.1007/s12599-016-0450-4

Meier C, Zimmermann S (2015) The Impact of Human Resource Sharing on IT Project Risk. In: Proceedings of the 36th International Conference on Information Systems (ICIS)

Mertens P, Barbian D (2015) Researching “Grand Challenges”. Bus Inf Syst Eng 57(6):391–403. doi: 10.1007/s12599-015-0405-1

Miller R (2011) Outage in Dublin Knocks Amazon, Microsoft Data Centers Offline. http://www.datacenterknowledge.com/archives/2011/08/07/lightning-in-dublin-knocks-amazon-microsoft-data-centers-offline/. Accessed 16 December 2016

Mizgier KJ, Jüttner MP, Wagner SM (2013) Bottleneck identification in supply chain networks. International Journal of Production Research 51(5):1477–1490. doi: 10.1080/00207543.2012.695878

Müller MP, Meier C, Kundisch D, Zimmermann S (2015) Interactions in IS Project Portfolio Selection - Status Quo and Perspectives. In: Wirtschaftsinformatik Proceedings, Paper 50

Nelson RR (2007) T Project Management: Infamous Failures, Classic Mistakes, and Best Practices. MIS Quarterly Executive 6(2):67–78

Newman MEJ (2013) Networks: An introduction, Reprint. with corr. Oxford Univ. Press, Oxford

Nguyen B, Mutum DS (2012) A review of customer relationship management: successes, advances, pitfalls and futures. Business Process Management Journal 18(3):400–419

Ren J, Jenkinson I, Wang J, Xu DL, Yang JB (2009) An Offshore Risk Analysis Method Using Fuzzy Bayesian Network. J. Offshore Mech. Arct. Eng. 131(4):41101. doi: 10.1115/1.3124123

Rinaldi SM, Peerenboom JP, Kelly TK (2001) Identifying, understanding, and analyzing critical infrastructure interdependencies. IEEE Control Syst. Mag. 21(6):11–25. doi: 10.1109/37.969131

Santhanam R, Kyparisis GJ (1996) A decision model for interdependent information system project selection. European Journal of Operational Research 89(2):380–399. doi: 10.1016/0377-2217(94)00257-6

Serdarasan S (2013) A review of supply chain complexity drivers. Computers & Industrial Engineering 66(3):533–540. doi: 10.1016/j.cie.2012.12.008

Shenoy C, Shenoy P (1999) Bayesian network models of portfolio risk and return. Computational Finance:87–106

Theoharidou M, Kotzanikolaou P, Gritzalis D (2009) Risk-Based Criticality Analysis. In: Palmer C, Shenoi S (eds) Critical Infrastructure Protection III: Third Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, Hanover, New Hampshire, USA, March 23-25, 2009, Revised Selected Papers. Springer Berlin Heidelberg, Berlin, Heidelberg, pp 35–49

Trucco P, Cagno E, Ruggeri F, Grande O (2008) A Bayesian Belief Network modelling of organisational factors in risk analysis: A case study in maritime transportation. Reliability Engineering & System Safety 93(6):845–856. doi: 10.1016/j.ress.2007.03.035

Urbach N, Ahlemann F (eds) (2016) IT-Management im Zeitalter der Digitalisierung. Springer Berlin Heidelberg, Berlin, Heidelberg

van der Meulen R (2016) Gartner Says Global IT Spending to Reach $3.5 Trillion in 2017. http://www.gartner.com/newsroom/id/3482917

Vrabič R, Husejnagić D, Butala P (2012) Discovering autonomous structures within co.mplex networks of work systems. CIRP Annals - Manufacturing Technology 61(1):423–426. doi: 10.1016/j.cirp.2012.03.083

Wasserman S, Faust K (2009) Social network analysis: Methods and applications, 19. printing. Structural analysis in the social sciences, vol 8. Cambridge Univ. Press, Cambridge

Wehrmann A, Heinrich B, Seifert F (2006) Quantitatives IT-Portfoliomanagement. Wirtsch. Inform. 48(4):234–245. doi: 10.1007/s11576-006-0055-5

Wolf T (2015) Assessing the Criticality of IT Projects in a Portfolio Context using Centrality Measures. In: Wirtschaftsinformatik Proceedings, p Paper 48

Wolfgang K, Hohrath P, Winter M (2008) Risikomanagement in Wertschöpfungsnetzwerken-Status quo und aktuelle Herausforderungen. Supply Chain Risk Management 7(8):7–21

Yao AC (1986) How to generate and exchange secrets. In: 27th Annual Symposium on Foundations of Computer Science (sfcs 1986), pp 162–167

Zhang Y (2016) Selecting risk response strategies considering project risk interdependence. International Journal of Project Management 34(5):819–830. doi: 10.1016/j.ijproman.2016.03.001

Zimmermann S (2008) IT-Portfoliomanagement – Ein Konzept zur Bewertung und Gestaltung von IT. Informatik Spektrum 31(5):460–468. doi: 10.1007/s00287-007-0224-y

II Systemic Risk in IT Project Portfolios: IT as a Challenge

This chapter includes the papers ”*Bayesian Network Modelling for Assessing the Criticality of IT Projects in a Portfolio Context*” and ”*Systemic Risk in IT Portfolios – An Integrated Quantification Approach*”.

II.1 Bayesian Network Modelling for Assessing the Criticality of IT Projects in a Portfolio Context[1]

Author:	Tirazheh Zare Garizy

Abstract

Digitalization and globalization are the two main factors leading to large and complex IT project portfolios. IT project portfolios’ dependence structures are often vulnerable to a cascading effect of failure and irrecoverable consequences for organizations. To avoid such failure scenarios proactively, the ability to assess the criticality of IT projects in an IT project portfolio context is crucial for organizations. This paper applies Bayesian network modelling and provides concrete guidance on how to evaluate the criticality of IT projects in a portfolio context. Our novel method considers different types of dependencies in an integrated cost-risk approach and provides the risk exposure of IT projects as a measure of criticality. The method is able to consider information on IT projects’ success and failure during a portfolio’s execution for ex-nunc and ex-post assessments. The method enables decision-makers to assess the criticality of IT projects, which is the first step towards the management of systemic risk and can increase the success rate of IT projects.

Keywords: IT Project Portfolio, Bayesian Network, Dependencies, Criticality Assessment.

[1] Grateful acknowledgment is due to the DFG (German Research Foundation) for their support of the project “ITPM (FR 2987/2-1, BU 809/13-1)” making this paper possible.

II.1.1 Introduction

Digitalization, globalization, and rapid technological changes increase the importance of IT projects for sustainable competitiveness (Kutsch et al., 2014; Wolf, 2015; Beer et al., 2015). However, despite the importance of the success of IT projects, they are facing a high failure rate (Saynisch, 2010). A study of Flyvbjerg and Budzier (2011) states that one out of six IT projects exhibits an average cost overrun of 200% and an average schedule overrun of almost 70%. Recent technological, social, and economic changes have increased the complexity of managing IT projects, which has led to a higher impact of occurring risks (Saynisch, 2010). Additionally, IT projects are often accomplished in a portfolio of several dependent IT projects, which further raises the impact of occurring risks (Graves et al., 2003; Buhl, 2012; Centeno et al., 2015; Martínez and Fernandez-Rodriguez, 2015). Although organizations seek to manage the risk associated with IT projects, recent studies indicate IT project risk management is regularly under-performed in practice (Bannerman, 2008; Kutsch et al., 2014). Also, literature emphasizes the insufficiency of existing IT project portfolio (ITPP) risk assessment methods and the need for an adequate consideration of dependencies within ITPPs (Flyvbjerg and Budzier, 2011; Müller et al., 2015).

Criticality assessment is defined as analyzing the probability and severity of a failure (traditional risk analysis), and the associated effects of failure based on its economic impact and dependencies (Theoharidou et al., 2009). The majority of common risk assessment approaches focus on stand-alone IT project risk assessment and do not consider the dependencies between IT projects (Bardhan et al., 2004; Jonen and Lingnau, 2007; Bakker et al., 2010). Dependencies between IT projects often arise when multiple IT projects require the output of a predecessor IT project (technical dependencies), or they share resources (resource dependencies) (Bardhan et al., 2004; Müller et al., 2015). A predecessor IT project, which fails to deliver the planned output, may cause serious problems for other IT projects. Additionally, shared resources are often overused by one of the IT projects of a portfolio, which may cause failure of multiple other IT projects (Heinrich et al., 2014). The dependencies between IT projects often cause cascading failure in ITPPs and irrecoverable consequences for organizations.

Mapping ITPPs as networks offers insights into the dependencies between different IT projects and also supports decision makers with the ITPP management process (Killen and Kjaer, 2012). Taking up the network interpretation of ITPPs several network measures (Wasserman and

Faust, 2009; Newman, 2013) or probabilistic graphical models (Koller and Friedman, 2009) can provide deeper insight and better understanding of ITPP's dependencies.

Network measures are suitable to analyze the interactions, and the patterns of dependencies in networks quantitatively (Newman, 2013). Betweenness, closeness, and alpha centrality are some of the network analysis measures widely used in social network analysis (Freeman, 1977; Wasserman and Faust, 2009; Bonacich and Lloyd, 2001). Recent methods in supply chain network analysis apply these measures to capture characteristics of supply chain networks, or identify risky organizations within supply chain networks (Kim et al., 2011; Mizgier et al., 2013; Fridgen and Zare Garizy, 2015). Wolf (2015) interprets the corresponding network of ITPP as a graph and identifies alpha centrality as a suitable network measure for criticality assessment in ITPPs. Despite being novel in how it considers dependencies, this method has some limitations and does not provide a measure which takes the economic impact of failures into account. Beer et al. (2015) extend that method and apply alpha centrality to integrate the effect of transitive dependencies into a measure of risk for ITPP evaluation. However, they do not provide a criticality value for each IT project. Therefore, and despite of these first approaches in criticality assessment, more advanced approaches which model dependency structures of ITPPs and monetarily assess the criticality of IT projects are required.

Probabilistic graphical models are suitable tools to deal with uncertainty and complexity in networks (Jordan, 1999). Among probabilistic graphical models, Bayesian network modelling is a promising method for risk analysis (Khakzad et al., 2013). It is widely used in other fields for criticality assessment and analysis of domino effects in networks (Shenoy and Shenoy, 1999; Marsh and Bearfield, 2004; Trucco et al., 2008; Ren et al., 2009; Khakzad et al., 2013; Garvey et al., 2015). Therefore, we identify Bayesian network modelling as an alternative approach which might also be applicable to the IT projects' criticality assessment. Hence, we set the following research question:

"Can Bayesian network modelling serve to assess the criticality of IT projects within an ITPP considering the associated effects of failure based on the economic impact and dependencies between IT projects?"

To answer this question, we study the dependence structures of ITPPs and evaluate to which extent Bayesian network modelling can cover the criticality assessment of IT projects within ITPPs. As our research method, we use the recurring research cycle of Meredith et al. (Meredith et al., 1989). Meredith et al. (Meredith et al., 1989) propose a three-stage research cycle paradigm in the field of operations research. The cycle starts with the description phase, proceeds to the explanation phase, and the testing phase (Meredith et al., 1989). Accordingly, the remainder of this paper is structured as follows: the problem formulation section characterizes the elements of the problem and therefore, covers the description phase of the research paradigm. The solution approach section elaborates on the procedure of assessing the criticality using Bayesian network and infers causal relations within ITPPs, which covers the explanation phase of the research paradigm. In the evaluation section, we examine if the method meets our requirements on criticality assessment. Furthermore, we evaluate the functionalities and usability of our model with a demonstration example. To study the behaviour of the model and to evaluate its robustness to the deviation of input parameters, we conduct a sensitivity analysis, and use simulation as a dominant mode of testing (Meredith et al., 1989; Pannell, 1997). In the discussion section, we critically discuss limitations of this method. In the conclusion, we summarize results and provide an outlook for further research.

II.1.2 Problem Formulation

II.1.2.1 Different Types of Dependencies in ITPPs

Academia has come up with several classifications for dependencies between IT projects. The most common frameworks distinguish between three categories: resource dependencies, technical dependencies, and benefits (Aaker and Tyebjee, 1978; Lee and Kim, 2001; Wehrmann et al., 2006; Beer et al., 2015). Resource dependencies arise from shared personal or shared infrastructure between projects which are taking place at one point in time. Originally designed to realize cost synergies, resource dependencies can also lead to risk accumulation effects (Heinrich et al., 2014). Technical dependencies arise when an IT project requires the output of its predecessor IT project (Diepold et al., 2009; Beer et al., 2015). Benefits dependencies (or synergies) arise when the simultaneous realization of multiple projects increases the value of at least one of the projects (Buchholz et al., 1987). An alternative way to differentiate between dependencies is to classify them as intertemporal and intratemporal (Santhanam and Kyparisis, 1996; Bardhan et al., 2004; Zimmermann, 2008; Kundisch and Meier, 2011; Meier and Zimmermann, 2015). Intertemporal dependencies are commonly interpreted as technical dependencies, and intratemporal dependencies are commonly interpreted as resource dependencies between IT projects (Santhanam and Kyparisis, 1996; Diepold et al., 2009).

Corresponding to the common interpretation of criticality, we consider each IT project or shared resource to have two states: success or failure. Failure of an IT project occurs when it is unable to deliver the desired output. Failure of shared resources occurs when a resource is overused by a particular project and does not have the capacity to fulfill its tasks for other projects. Failure of projects or resources, which have dependencies with risk accumulation effect lead to a cascading failure through the entire ITPP and provoke a network failure. For the purpose of criticality assessment, we focus on dependencies with risk accumulation effects. Our assessment revealed that both technical and resource dependencies show risk accumulation effects. Technical dependencies have risk accumulation effects when a project failure cascades through the network and cause failure of its successor projects as well as other indirectly dependent projects. Resource dependencies can cause risk accumulation effects when a shared resource which is overused by one IT project, provokes the failures of multiple IT projects.

Several papers have already brought forward useful approaches to model the corresponding network of ITPPs as graphs (Beer et al., 2015; Wolf, 2015). We model ITPPs graphs as follows: IT projects and shared resources are depicted by nodes. Technical dependencies and resource dependencies are depicted as directed edges between projects and their shared resources. We use circles to denote nodes which represent projects and arrows to denote edges which represent technical dependencies between projects. Figure 1 illustrates a technical dependency of P_j on P_i. It reads “Project P_j depends on project P_i”.

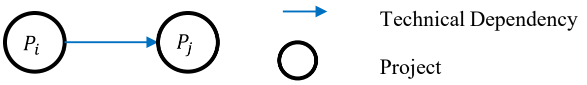


Figure 1. Two IT projects with technical dependency

We use squares to denote nodes which represent *shared* resources and dashed arrows to denote edges which represent resource dependencies between projects. We consider shared resources between projects as nodes with two or more resource dependencies originating from them. The edges point to the projects which are sharing the particular resource.

Resources that are only assigned to a single IT project do not constitute a resource dependency between IT projects. Therefore, we do not consider them as nodes in our model. Nevertheless, we consider the dependencies of a project on its exclusive resources as part of its inherent risk. Figure 2 illustrates resource dependencies between IT projects P_i and P_j due to the shared resource R_I. It reads “Project P_i depends on resource R_I”.

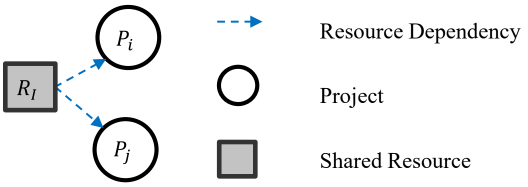


Figure 2. Two IT projects with resource dependency

Interpreting the corresponding network of ITPP as a graph, we can model how the failure of a single IT project cascades through the entire ITPP.

II.1.2.2 Requirements to Assess Criticality in ITPPs

A method that aims to assess the criticality of IT projects within ITPPs should meet the following requirements, according to Wolf (2015), Müller et al. (2015), and Theoharidou et al. (2009):

Requirement 1: *The method accounts for both direct and indirect dependencies.*

Direct dependencies arise between projects with technical or resource dependencies. Due to the transitive characteristic of networks, the effect of a failure cascades through the network and indirectly impacts further projects. Therefore, when considering dependencies, it is important to account for direct and indirect dependencies.

Requirement 2: *The method accounts for the impact of different strengths of dependencies.*

The dependencies between projects can have different impacts on the success or failure of their directly dependent projects. The impact determines the strength of their dependencies. It is important to integrate the strength of dependencies into the determination of the criticality of projects.

Requirement 3: *The method accounts for project-specific influence factors to quantitatively consider the importance of directly and indirectly dependent IT projects.*

Besides the importance of the dependencies in criticality assessment, the economic impact of the failure plays an important role. This economic impact can be the cost of failure or other project-specific influence factors. The impact of dependencies between projects varies depending on the economic impact of a project’s failure. The higher the cost of failure of a project, the more its contribution to the criticality value of itself and its directly and indirectly depended projects.

Requirement 4: *The method integrates different dependencies, their strengths, and project-specific influence factors of criticality into one measure of criticality.*

To provide an accountable criticality value for IT projects it is important to consider the network-specific factors (different dependencies, and their strength), and project-specific influence factors (Theoharidou et al., 2009). Accordingly, the method should integrate all these factors into a single measure of criticality of each IT project.

The criticality assessment method which meets the above-mentioned requirements provides a holistic insight into the risks and dependencies between IT projects and their impacts on the ITPPs. It empowers decision makers to successfully implement ITPPs (Bathallath et al., 2016). In Section II.1.4, we examine how and to what extent our proposed method accounts for requirements 1-4.

II.1.2.3 Need for a New Method for Criticality Assessment in ITPPs

Whilst accounting for the dependencies between IT projects is important for ITPPs' success, there are only few approaches which take multiple categories of dependencies into account (Meier et al., 2016; Bathallath et al., 2016; Keil et al., 2013; Killen and Kjaer, 2012; Wolf, 2015; Beer et al., 2015). Many of these approaches (Meier et al., 2016; Bathallath et al., 2016; Keil et al., 2013; Killen and Kjaer, 2012) focus on the identification and visualization of dependencies, rather than on criticality assessment in the context of ITPP. Wolf (2015) and Beer et al. (2015) provided the first approaches based on alpha centrality to assess the criticality in ITPPs. Despite the advantages of these approaches, they do not meet all four of the previously stated requirements (cf. Table 1).

Table 1. Fulfillment of the stated requirements by existing approaches

	Wolf (2015)	Beer et al. (2015)
Requirement 1	✓ The method accounts for both direct and indirect dependencies.	✓ The method accounts for both direct and indirect dependencies.
Requirement 2	(✓) The method has the possibility to account for the impact of dependencies, but the author does not provide a solution to quantify this impact.	✓ The method accounts for the impact of dependencies by distinguishing between two types of dependencies (intra- and intertemporal) and by using the relative time lag to quantify dependencies.

Table 1. Fulfillment of the stated requirements by existing approaches

	Wolf (2015)	Beer et al. (2015)
Requirement 3	(✓) The method has the possibility to account for project-specific influence factors, but does not introduce a suitable factor which accounts for the economic impact of failures.	(✓) The method considers a pseudo-covariance matrix as a project-specific influence factor. However, the method does not consider the economic impact of failures.
Requirement 4	(✓) The method integrates different dependencies, their strengths, and project-specific influence factors of criticality. The method delivers a criticality score, but does not consider associated effects of failure based on its economic impact and dependencies.	✗ The method integrates different dependencies, their strengths, and project-specific influence factors of criticality. However, since the method considers a pseudo-covariance matrix as project-specific influence factor, the result of alpha centrality is a matrix. This matrix determines corresponding ITPP risk and does not provide the criticality value of each IT project.

Furthermore, approaches of Wolf (2015) and Beer et al. (2015) have two main drawbacks due to the application of alpha centrality in their calculations. In the alpha centrality, α determines the arbitrary ratio between the importance of ITPP structure (network structure) and the IT projects (nodes) in the calculation (Bonacich and Lloyd, 2001). This results in the first drawback: the result of alpha centrality depends significantly on the choice of α and there is no specific guidance on how to choose α (Bonacich and Lloyd, 2001). The second drawback is: difficulties in interpretation of the criticality scores. Since, the interpretation is not intuitive, it makes the method's usability in practice quite challenging.

Based on the mentioned drawbacks and limitation of existing methods, it is necessary to develop approaches which cover all four of the stated requirements and reduce these drawbacks.

II.1.3 Solution Approach through Bayesian Network Modelling

We aim to develop a model which is scalable and is explicitly applicable for large and complex ITPPs, where criticality can no longer be assessed intuitively. In the following, we elaborate our procedure to calculate the risk exposure of each IT project as a measure of criticality. We therefore, model ITPPs and their dependence structure as a Bayesian network.

II.1.3.1 ITPPs as Bayesian Network

"Bayesian networks are graphical structures for representing the probabilistic relationships among a large number of variables and for doing probabilistic inference with those variables" (Neapolitan, 2004). Bayesian networks combine expert judgments with the traditional quantitative analysis in an intuitive manner (Shenoy and Shenoy, 1999). For example, a Bayesian network of a disease and its symptoms could reveal the probability of the presence of a disease, given its symptoms.

A Bayesian network is a directed acyclic graph (DAG) with nodes representing a set of random variables and edges representing conditional dependencies between nodes (Jensen, 2002; Russell and Norvig, 2010). Node X with direct edge to Y is called a *parent* of Y, and Y is called its *child*. Nodes without direct edges pointing to them are called *roots*. If a node X influences node Z directly (through an edge) or indirectly (through edges of neighboring nodes), then Z is a *reachable* node for X (Neapolitan, 2004). A conditional probability table (CPT) contains the strength of edges (conditional dependencies) between directly connected nodes (Neapolitan, 2004; Jensen et al., 2007). Bayesian networks enable calculating probabilities of the occurrence of an event, given particular observations of the state of the network's nodes (Neapolitan, 2004). For example, in a DAG of Figure 2 with three nodes P_i, P_j, and R_I, we can obtain the probability of occurrence of an event (e.g. success of P_i, $P_i = T$), given an observation (e.g. failure of R_I, $R_I = F$) in the network as in equation (1).

$$P(P_i = T|R_I = F) = \frac{P(P_i = T, R_I = F)}{P(R_I = F)} = \frac{\sum_{P_j \in \{T,F\}} P(P_i = T, R_I = F, P_j)}{\sum_{P_i, P_j \in \{T,F\}} P(P_i, R_I = F, P_j)} \quad (1)$$

Bayesian networks have been widely used as an accurate method to project management and risk assessment (Shenoy and Shenoy, 1999; Shenoy and Shenoy, 2002; Marsh and Bearfield, 2004; Trucco et al., 2008; Ren et al., 2009; Martínez and Fernandez-Rodriguez, 2015). Recently, the idea of adopting Bayesian networks in IT project management is emerging. Gingnell et al. (2014) quantified IT projects' success factors using Bayesian networks. Hu et al. (2012) used Bayesian networks to analyse outsourced software project risks. However, to the best of our knowledge, Bayesian networks have not been used in ITPPs criticality assessment yet.

To model ITPPs as Bayesian networks the corresponding graph must be a DAG. Therefore, we state the assumption that the graph of the ITPP is acyclic.

This assumption is in line with real-world scenarios of IT projects without dual relations between projects (cf. (Wiest, 1981)). Furthermore, if we consider IT projects as fine granular subprojects which only deliver one output, technical dependencies do not cause a cyclical dependency. Moreover, resource dependencies, since in our modelling resource dependencies are originating from a resource which is always a root (cf. Section II.1.2.1), by definition cannot cause cyclical graph. Hence, when excluding unlikely scenarios which may lead to cyclical dependencies in ITPPs, our assumption is in line with real-world scenarios.

The next step of our modelling procedure is to estimate the CPT of each IT project and shared resource. We already mentioned each IT project or shared resource (node) in our model has two states: success (T) and failure (F). The CPT of a root node contains the estimated values of probabilities of the node's failure and success. The CPT of a non-root node, contains the estimated values of probabilities of the node's failure and success, given all possible combinations of the success and failure of its parents. Subsequently, CPT entries express the strength of the node's technical and resource dependencies in an integrated manner. Consequently, henceforth we do not distinguish between types of dependencies in the calculations but refer to the entries of CPT instead.

Common methods to estimate CPTs use existing data and/or expert estimations (Neapolitan, 2004). Since using Bayesian Networks in ITPPs assessment is not yet common, existing data is scarce. Therefore, we focus on expert estimations. Due to the various perceptions of failure, it is important to implement mechanisms to have a clear definition of the probability of failure for our value estimations. Moreover, the cognitive bias of the managers can influence the estimation and results, and it is necessary to implement mechanisms, which moderate this effect (Etzioni, 2014). These mechanisms support the homogeneity of the estimated values and enable uniform interpretation of the result in the organization. To estimate CPTs based on expert estimations, the expert should estimate probabilities of the failure and success of each project and shared resource, given all possible combinations of the success and failure of their parents. The following questions are two example questions for the expert estimations: *What is the probability that your project cannot deliver the planned output if predecessor project A does not deliver the desired output while all other parent projects deliver the desired output and all* *shared resources fulfil their tasks? What is the probability that your project cannot deliver the planned output if all predecessor projects do not deliver the desired output and all shared resources fail to fulfil their tasks?*

In large and complex ITPPs, it is not possible that a single person estimates the CPTs for all IT projects. In these cases, each IT project manager should provide the CPT of their IT project and its shared resources. This decentral data estimation approach benefits from the local information of all IT project managers. However, the close collaboration with the ITPP manager in the estimation process is crucial to ensure data consistency across the inputs of various IT project managers.

II.1.3.2 Assessing Criticality of the IT Projects Using Bayesian Network Modelling

So far, we developed the Bayesian network of an ITPP, which can facilitate decision-making. A Bayesian network enables the estimation of the probabilities of success or failure of certain nodes (e.g., IT projects or shared resources), based on an observation (e.g., success or failure of an IT project) (Jensen, 2002). Using this method, we can model how the failure of a single IT project cascades through the entire ITPP. Besides, the method can consider information on IT projects' success and failure during portfolios execution for ex-nunc (continual) and ex-post assessments.

In the assessment of IT projects' criticality, we strongly focus on the key influence factors of criticality. First, we calculate the joint probabilities of the failures of one or more IT projects, given that project P_i fails. We assess the criticality of P_i based on the changes, which the observation of the failure of P_i causes to the states of other IT projects. To consider the economic impact, increase the tangibility of the results, and provide managerial insight we incorporate the cost of failure of IT projects into our assessment. With this approach, we take an integrated cost-risk perspective on the criticality of each IT project. Methodologically, we use the so-called "with-without" principle from risk management (Howe and Cochrane, 1993; Tasche, 2008). This principle calculates the marginal risk contribution of an asset by calculating the difference of the portfolio risk with and without the asset (Howe and Cochrane, 1993; Tasche, 2008). Transferred to our model, we use the difference between the costs of failure within the entire ITPP if P_i fails and if it does not fail as our measure of risk. In the following, we elaborate on this method in detail. First, we determine how the failure of an IT project affects the states of its directly and indirectly dependent (reachable) IT projects. Therefore, we refer to the conditional probabilities of failure for the cases in which P_i fails ($P(P_j = F|P_i = F)$) and in which it does not fail ($P(P_j = F|P_i = T)$). Second, we integrate the cost of failure of IT projects into our assessment. To do so, we define the expected cost of failure (ECF) of an IT project P_j as the product of the probability of its failure and its cost of failure using the "*with-without*" principle. We calculate the ECF as depicted in equation (2).

$$ECF(P_j = F|P_i) = P(P_j = F|P_i = \mathrm{F}) \times CF(P_j) - P(P_j = F|P_i = T) \times CF(P_j) \tag{2}$$

The result of equation (2) is the effect of P_i on the failure of its reachable project P_j. To calculate the total expected loss which may occur due to the failure of P_i, we sum up the expected cost of failure of P_i and all its reachable IT projects, as shown in equation (3).

$$\Delta CF(P_i) = \ CF(P_i) + \sum_j ECF(P_j = F|P_i) \tag{3}$$

The result of equation (3) is the extent of loss which P_i can cause in the network. As a final step, we need to consider the probability of failure for P_i to incorporate the likelihood of this loss and provide the *risk exposure* (RE) or also called the risk impact of each IT project (Boehm, 1989). Equation (4) provides the RE of P_i as an integrated cost-risk measure of criticality for IT project P_i.

$$RE(P_i) = \ \Delta CF(P_i) \times P(P_i = F) \tag{4}$$

II.1.4 Evaluation

Modelling ITPPs as Bayesian networks enables us to address the following requirements on criticality assessment. Regarding requirement 1: we refer to the conditional probabilities of success and failure of projects in equation (2), which enables us to consider both direct and indirect dependencies. Regarding requirement 2: we use the entries of CPTs for our calculations, which enables us to consider the impact of different strengths of dependencies. Regarding requirement 3: we refer to the cost of failure as a project specific influence factor in equation (2) and equation (3), which integrates the importance of dependent IT projects quantitatively. Regarding requirement 4: we derive RE of each IT project in equation (4), which serves as the measure of criticality, and considers dependencies and their strength, as well as project-specific characteristics for the criticality assessment. The RE of an IT project is higher if its failure has more consequences for the network and if more IT projects might be affected by its failure. The RE of an IT project decreases if the probability of the success of IT projects increase and therefore the impact of dependencies decreases. The RE of an IT project is more influenced by the cost of failure if the effect of dependencies decreases. The assessment reveals the expected relation between input parameters and RE. This monetary assessment of criticality by calculating the RE of each IT project enables considering both economic impacts of failure of single IT projects as well as the dependence structure of ITPP in a holistic approach.

Our Bayesian network modelling approach enables us to overcome two main drawbacks of alpha centrality based approaches (cf. Section II.1.2.3): Firstly, our method does not have any α-like factor which significantly impacts the result. Our method only requires the estimation of CPD and the cost of failure which can be estimated more intuitively by decision makers than estimating α. Secondly, our approach is based on common patterns of human reasoning. Therefore it is easier for decision makers to interpret its results compared to the results of alpha centrality.

In the remainder of this section, we evaluate the functionalities and usability of our model within a demonstration example. In general, our model is scalable and explicitly designed for large and complex ITPPs, where criticality can no longer be assessed intuitively and where it can deliver most valuable support for decision makers. However, we have deliberately chosen a relatively small ITPP as a demonstration example. Although the small portfolio size leads to findings that might seem straightforward, it transparently demonstrates its functionality and enables a comprehensible evaluation. Using a large and complex settings would be too exhaustive for the purpose of a demonstration. To study the behaviour of the model and to evaluate its robustness to the inaccuracy of input parameters, we conduct a sensitivity analysis with respect to the deviation of the input parameters (Pannell, 1997; Fridgen and Müller, 2011). For our demonstration and robustness validation, we use the RE of IT projects (equation (4)). We used expert estimations and simulation as a dominant method of testing (Fridgen and Müller, 2009), which is in line with Meredith et al. (1989).

II.1.4.1 Demonstration Example

For the demonstration example, we interviewed the IT manager of a medium-sized applied research organization with two branches in Germany. Most of the IT infrastructure of this organization is in the cloud, which makes their IT infrastructure scalable. Therefore, projects' resource dependencies are mainly due to personnel resource sharing. The IT manager identified the sharing of personnel as the main challenge of their ITPPs. Table 2 illustrates one of their current ITPPs that consists of eight IT projects and one shared resource.

Table 2. The ITPP of the organization

Variable	*Description*
P_1	System images (Windows 7) for the first branch's laptops
P_2	System images (Windows 7) for the first branch's workstations
P_3	System images (Windows 7) for the second branch's laptops (this branch has no workstations)
P_4	System images (Windows 10) for laptops (integrated solution for both branches)
P_5	System images (Windows 10) for the first branch's workstations
P_6	System images (Windows-ToGo) for laptops, workstations, and other devices, which enables the bring-your-own-device concept and aims to release a portable Windows 10
P_7	Connection tool for an improved usability of SharePoint on laptops and workstations
P_8	Connecting tool for an improved usability of SharePoint on all systems
R_1	Personnel resource shared between projects

The projects P_1 and P_2 are sharing the resource R_1. The IT project manager emphasized the importance of the successful implementation of P_1 and P_2 to reuse the gained functional and technical know-how for the successful implementation ofP_3. Therefore, P_3 technically depends on P_1 and P_2. P_4 and P_5 are sharing R_1 which causes a resource dependency. P_4 and P_5 require the functionality of P_3, which causes its technical dependency to P_3. The project P_6 depends on the projects P_4 and P_5, since the availability of the sub modules of the system image creation and the establishment of user acceptance for Windows 10 are necessary to start P_6. P_6 also depends on P_8 for its connectivity to SharePoint. The personnel resource R_1 is an expert with an in-depth know-how of the project and the organization. This is the only shared resource of this ITPP. As previously mentioned (cf. II.1.2.1) resources which are not shared are not part of the model. Therefore, R_1 is the only resource which we use in the modelling of this ITPP. Figure 3 illustrates the graph of this ITPP.

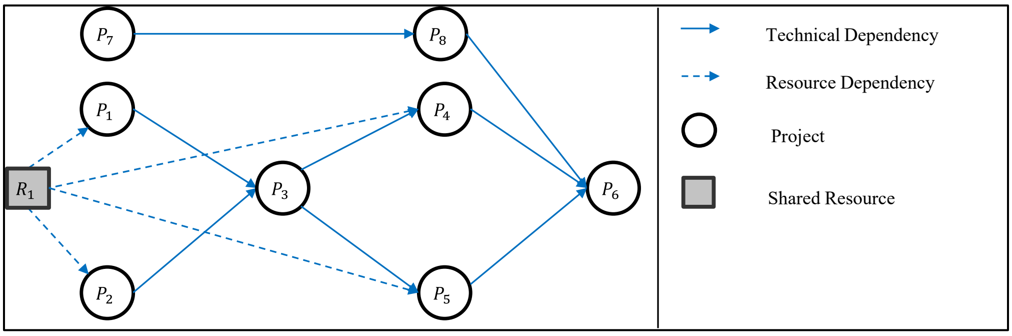


Figure3. ITPP of a medium-sized organization

The IT manager also estimated the entries of the CPT of each IT project and each shared resource as well as the cost of failure of each IT project. For demonstration purposes, we provide the CPT of project P_3 in Table 3.

Table 3. The CPT for Project 3

	$P_1 = F$		$P_1 = T$	
	$P_2 = F$	$P_2 = T$	$P_2 = F$	$P_2 = T$
$P(P_3 = F\|P_1, \mathrm{P}_2)$	100%	95%	50%	10%
$P(P_3 = \mathrm{T}\|P_1, \mathrm{P}_2)$	0%	5%	50%	90%

Forming the DAG of the ITPP and determining the CPTs, we build the Bayesian network and calculate the RE of each project using equation (4). For demonstration purposes, we elaborate on the computation path for RE of P_3 in the following. Table 4 provides the cost of failure and the conditional probabilities of P_4, P_5, and P_6 (reachable from P_3). On this basis, we can substantiate equations (2), (3) and (4) by $\Delta CF(P_3) =$ 6,197 €, $P(P_3 = F) =$ 66%, and ultimately the RE of 4,099 € for P_3.

Table 4. Conditional probability of the failures of reachable IT projects from P_3

IT Project	*CF (€)*	$P(P_j = F\|P_3 = F)$	$P(P_j = F\|P_3 = T)$
P_4	625	73%	8%
P_5	1,875	80%	0.4%
P_6	10,000	73%	55%

Table 5 provides the results of RE for all IT projects of the ITPP.

Table 5. IT projects sorted based on their RE

Project	P_1	P_8	P_2	P_3	P_6	P_7	P_5	P_4
RE	6,707	6,611	6,032	4,099	3,984	3,823	2,454	717

With this information, we are able to assess the criticality of IT projects in the ITPP using our method. By defining priority groups, we minimize the effect of possible estimation errors in decision making, since estimation errors cause changes in the position of adjacent projects in the priority list (section II.1.4.2). We group projects with similar RE and assign them to priority groups as follows. System images (Windows 7) for the first branch's laptops and workstations (P_1 and P_2), and connection tool for an improved usability of SharePoint on all systems (P_8) belong to the category of most critical IT projects for ITPP. Since their RE are very close to each other, all three require high management attention to prevent the ITPP's failure. Subsequently, system images (Windows 7) for the second branch's laptops (P_3), Windows-ToGo project (P_6), and connection tool for an improved usability of SharePoint on laptops and workstations (P_7) have lower RE and can be assigned to the category of medium risk projects for management attention.

II.1.4.2 Sensitivity Analysis

Since our method uses estimated parameters, it is important to study how the model reacts to estimation inaccuracies. Moreover, the understanding of the relation between input parameters and criticality prioritization is important for a sound evaluation of the model. Therefore, we conduct a sensitivity analysis with respect to the input data from the demonstration example to investigate the robustness of our model and its behaviour. As variation steps, "ceteris paribus", we increase the success probabilities and the cost of failure of one IT project as reported by the IT manager by 1%, 10%, 25%, and 50%.

Table 6 provides the sensitivities on the variation of the entries of CPT of P_3, and highlights those IT projects, which changed their positions on the priority list. Despite the estimation error, P_1 and P_8 stay the most critical projects. Moreover, the projects' position-changes only take place between adjacent projects of the original priority list, with similar RE. Therefore, the estimation error of one project ceteris paribus, does not have a high impact on the respective criticality of the IT projects. Additionally, we could observe that increasing the probability of the success for P_3 decreases the cost of failure of the entire ITPP. This observation illustrates the desired, proportional relation between success probability and the portfolio criticality.

Table 6 Sensitivity analysis results of varying values of CPT for P_3

Estimation error	*IT projects sorted based on their RE (€)*							
0%	P_1	P_8	P_2	P_3	P_6	P_7	P_5	P_4
	6,707	6,611	6,032	4,099	3,984	3,823	2,454	717
1%	P_1	P_8	P_2	P_3	P_6	P_7	P_5	P_4
	6,677	6,610	6,007	4,061	3,984	3,823	2,452	719
10%	P_8	P_1	P_2	P_6	P_7	P_3	P_5	P_4
	6,602	6,415	5,792	3,980	3,817	3,706	2,434	738
25%	P_8	P_1	P_2	P_6	P_7	P_3	P_5	P_4
	6,589	5,995	5,431	3,975	3,806	3,086	2,401	774
50%	P_8	P_1	P_2	P_6	P_7	P_5	P_3	P_4
	6,562	5,302	4,790	3,963	3,786	2,337	1,994	839

We also examined the changes in priorities by simultaneously varying the values of CPTs of all IT projects. This multiple variation caused more position changes with mostly similar pattern as compared to the variation of the values of CPT of P_3. Only increasing success probabilities by 25% led to a dramatic change and made P_6 the most critical IT project. However, it should be noted that 25% estimation error in all input parameters is quite unlikely in the real-world. Therefore, we assign a high robustness to our model. As a second finding, we observed that simultaneously increasing the probabilities of success (which implies a decrease of the importance of direct and indirect dependencies) decreases the influence of network structure on criticality values. Consequently, the importance of the project-specific influence factors (cost of failure) increased. In the final step, we examine the result of varying cost of failure for all IT projects simultaneously as well as for one IT project ceteris paribus. Whereas varying all values at the same rate did not lead to any changes in the prioritization, the variation for a single project (e.g. P_3) evokes few positional changes. The result of the analysis gives us no indication that the estimation errors may cause an unexpectedly extreme response of the model which leads to errors in decision making. We also observed the expected relation between input parameters and criticality prioritization (e.g. incrementing probability failure increases RE).

II.1.5 Discussion

In our method, we stated the assumption that IT projects are fine granular subprojects which only deliver one output and therefore, technical dependencies may not cause a cyclical dependency. Accounting for dependencies between these fine granular subprojects is necessary for the criticality assessment, though, in large ITPPs this will be a challenging and time-consuming task. Moreover, increasing the number of IT projects (nodes) impacts the time complexity of the algorithms used for Bayesian network modelling. In the worst case, this time complexity can be exponential as function of the number of nodes without any observation of their state in the network (Cooper, 1990). Yet, the risk identification has a significant positive impact on risk transparency and consequently ITPP's success (Teller and Kock, 2013). This brings the decision makers to the trade-off between effort or the "cost" of gathering data for modelling and the potential benefits of the assessment of systemic risk in the management of systemic risk. The development of the techniques to support decision makers to evaluate if the application of the method is worth the effort is subject to further research.

Our proposed approach relies on the ex-ante estimation of the failure probability of an IT project under the circumstance that another project has failed. This might sound unfeasible in the real-world and especially in large and complex ITPPs. However, we proposed gathering CPTs of each IT project from their respective IT project managers, in collaboration with the ITPP manager. Consequently, each IT project manager requires to estimate the CPTs of their IT project only considering the dependencies to the neighboring IT projects and not to the whole ITPP. This increases the applicability and the feasibility of the method by profiting from the decentral knowledge of all involved IT project managers.

II.1.6 Conclusion, and Outlook

In this paper, we developed an approach based on a Bayesian network modelling, and we used the research paradigm of Meredith et al. (1989) as our research method. Our method integrated various types of dependencies, their strengths and project-specific influence factors in the criticality assessment of IT projects. Subsequently, the method presented the RE of IT projects as a measure of criticality. Our method not only supports decision makers in ex-ante assessments but it is also applicable for ex-nunc and ex-post assessments. We therefore, contribute to the formalization of the risk management process, which is positively related to the management quality of ITPPs and consequently to their success (Teller, 2013; Keil et al., 2013). This enables efficient risk response actions as well as better resource allocation (Teller and Kock, 2013). In our evaluation, we used a demonstration example, sensitivity analysis, and simulations. Nevertheless, further testing of our model in real-world scenarios is important.

Our model focused on the risks associated with IT projects and shared resources to evaluate the criticality of IT projects. Our long-term vision is to extend our method according to the following aspects. First, we want to extend our method by assessing benefits of different types of dependencies towards a holistic ITPP evaluation method. Second, we want to extend our method through the application of methods like fuzzy reasoning and by using real-world data in order to reduce the estimation error and to increase its usability.

II.1.7 References

Aaker, D. A. and T. T. Tyebjee (1978). “A model for the selection of interdependent R&D projects.” *IEEE Transactions on Engineering Management* EM-25 (2), 30–36.

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

Bannerman, P. L. (2008). “Risk and risk management in software projects: A reassessment.” *Journal of Systems and Software* 81 (12), 2118–2133.

Bardhan, I., S. Bagchi and R. Sougstad (2004). “Prioritizing a Portfolio of Information Technology Investment Projects.” *Journal of Management Information Systems* 21 (2), 33–60.

Bathallath, S., Å. Smedberg and H. Kjellin (2016). “Managing project interdependencies in IT/IS project portfolios: a review of managerial issues.” *Developing and enforcing internal information systems standards: InduMaker’s* 4 (1), 67–82.

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

Boehm, B. (1989). “Software risk management.” In: *ESEC ’89: 2nd European Software Engineering Conference University of Warwick, Coventry, UK September 11-15, 1989 Proceedings*. Ed. by C. Ghezzi and J. A. McDermid. Berlin, Heidelberg: Springer Berlin Heidelberg, p. 1–19.

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

Buchholz, S., T. Roth and K. M. Hess (1987). *Creating the high performance team*. John Wiley & Sons Inc.

Buhl, H. U. (2012). “The Contribution of Business and Information Systems Engineering to the Early Recognition and Avoidance of “Black Swans” in IT Projects.” *Business & Information Systems Engineering* 4 (2), 55–59.

Centeno, M. A., M. Nag, T. S. Patterson, A. Shaver and A. J. Windawi (2015). “The Emergence of Global Systemic Risk.” *Annual Review of Sociology* 41 (1), 65–85.

Cooper, G. F. (1990). “The computational complexity of probabilistic inference using bayesian belief networks.” *Artificial Intelligence* 42 (2-3), 393–405.

Diepold, D., C. Ullrich, A. Wehrmann and S. Zimmermann (2009). “A real options approach for valuating intertemporal interdependencies within a value-based IT portfolio management-A risk-return perspective.” In: *ECIS 2009 Proceedings*, Paper 10.

Etzioni, A. (2014). “Humble Decision-Making Theory.” *Public Management Review* 16 (5), 611–619.

Flyvbjerg, B. and A. Budzier (2011). “Why Your IT Project May Be Riskier than You Think.” *SSRN Electronic Journal.*

Freeman, L. C. (1977). “A Set of Measures of Centrality Based on Betweenness.” *Sociometry* 40 (1), 35.

Fridgen, G. and H. V. Müller (2009). “Risk/Cost Valuation of Fixed Price IT Outsourcing in a Portfolio Context.” In: *30th International Conference on Information Systems (ICIS 2009).*

Fridgen, G. and H. V. Müller (2011). “An Approach for Portfolio Selection in Multi-Vendor IT Outsourcing.” In: *32nd International Conference on Information Systems (ICIS).*

Fridgen, G. and T. Zare Garizy (2015). “Supply Chain Network Risk Analysis: A Privacy Preserving Approach.” In: *23rd European Conference on Information Systems (ECIS).*

Garvey, M. D., S. Carnovale and S. Yeniyurt (2015). “An analytical framework for supply network risk propagation: A Bayesian network approach.” *European Journal of Operational Research* 243 (2), 618–627.

Gingnell, L., U. Franke, R. Lagerström, E. Ericsson and J. Lilliesköld (2014). “Quantifying Success Factors for IT Projects—An Expert-Based Bayesian Model.” *Information Systems Management* 31 (1), 21–36.

Graves, S. B., J. L. Ringuest and A. L. Medaglia (2003). *Models & Methods for Project Selection:* Concepts from Management Science, Finance and Information Technology. New York: Springer Science.

Heinrich, B., D. Kundisch and S. Zimmermann (2014). “Analyzing Cost and Risk Interaction Effects in IT Project Portfolios.” *BIT: Banking and Information Technology* 15 (2/2014), 8–20.

Howe, C. W. and H. C. Cochrane (1993). "Guidelines for the uniform definition, identification, and measurement of economic damages from natural hazard events: With comments on historical assets, human capital, and natural capital." *FMHI Publications*, Paper 64.

Hu, Y., X. Mo, X. Zhang, Y. Zeng, J. Du and K. Xie (2012). "Intelligent Analysis Model for Outsourced Software Project Risk Using Constraint-based Bayesian Network." *Journal of Software* 7 (2).

Jensen, F. V. (2002). *An introduction to Bayesian networks.* Reprint. London: Taylor & Francis.

Jensen, F. V., M. Jordan, J. Kleinberg, T. D. Nielsen and B. Schölkopf, Eds. (2007). *Bayesian Networks and Decision Graphs:* February 8, 2007. Second Edition. New York, NY: Springer New York.

Jonen, A. and V. Lingnau (2007). "Bewertung von IT-Investitionen — Einbezug von Werttreibern und Risiken." *Controlling & Management* 51 (4), 246–250.

Jordan, M. I., Ed. (1999). *Learning in graphical models.* 1. MIT Press ed. Cambridge, Mass.: MIT Press.

Keil, M., A. Rai and S. Liu (2013). "How user risk and requirements risk moderate the effects of formal and informal control on the process performance of IT projects." *European Journal of Information Systems* 22 (6), 650–672.

Khakzad, N., F. Khan, P. Amyotte and V. Cozzani (2013). "Domino effect analysis using Bayesian networks." *Risk analysis an official publication of the Society for Risk Analysis* 33 (2), 292–306.

Killen, C. P. and C. Kjaer (2012). "Understanding project interdependencies: The role of visual representation, culture and process." *International Journal of Project Management* 30 (5), 554–566.

Kim, Y., T. Y. Choi, T. Yan and K. Dooley (2011). "Structural investigation of supply networks: A social network analysis approach." *Journal of Operations Management* 29 (3), 194–211.

Koller, D. and N. Friedman (2009). *Probabilistic graphical models:* Principles and techniques. Cambridge, Mass.: MIT Press.

Kundisch, D. and C. Meier (2011). "IT/IS project portfolio selection in the presence of project interactions-review and synthesis of the literature." In: *Wirtschaftsinformatik Proceedings*, Paper 64.

Kutsch, E., T. R. Browning and M. Hall (2014). "Bridging the Risk Gap." *Research Technology Management* 57 (2), 26–32.

Lee, J. W. and S. H. Kim (2001). "An integrated approach for interdependent information system project selection." *International Journal of Project Management* 19 (2), 111–118.

Marsh, W. and G. Bearfield (2004). "Using Bayesian Networks to Model Accident Causation in the UK Railway Industry." In: *Probabilistic Safety Assessment and Management*. Ed. by C. Spitzer, U. Schmocker and V. N. Dang. London: Springer London, p. 3597–3602.

Martínez, D. M. and J. C. Fernandez-Rodriguez (2015). "Artificial Intelligence Applied to Project Success: A Literature Review." *International Journal of Interactive Multimedia and Artificial Intelligence* 3 (5), 77.

Meier, C., D. Kundisch and J. Willeke (2016). "Is it Worth the Effort?" *Business & Information Systems Engineering*.

Meier, C. and S. Zimmermann (2015). "The Impact of Human Resource Sharing on IT Project Risk." In: *Proceedings of the 36th International Conference on Information Systems (ICIS).*

Meredith, J. R., A. Raturi, K. Amoako-Gyampah and B. Kaplan (1989). "Alternative research paradigms in operations." *Journal of Operations Management* 8 (4), 297–326.

Mizgier, K. J., M. P. Jüttner and S. M. Wagner (2013). "Bottleneck identification in supply chain networks." *International Journal of Production Research* 51 (5), 1477–1490.

Müller, M. P., C. Meier, D. Kundisch and S. Zimmermann (2015). "Interactions in IS Project Portfolio Selection - Status Quo and Perspectives." In: *Wirtschaftsinformatik Proceedings*, Paper 50.

Neapolitan, R. E. (2004). *Learning Bayesian networks*. Upper Saddle River, NJ: Pearson Prentice Hall.

Newman, M. E. J. (2013). *Networks:* An introduction. Reprint. with corr. Oxford: Oxford Univ. Press.

Pannell, D. (1997). "Sensitivity analysis of normative economic models: Theoretical framework and practical strategies." *Agricultural Economics* 16 (2), 139–152.

Ren, J., I. Jenkinson, J. Wang, D. L. Xu and J. B. Yang (2009). "An Offshore Risk Analysis Method Using Fuzzy Bayesian Network." *Journal of Offshore Mechanics and Arctic Engineering* 131 (4), 41101.

Russell, S. J. and P. Norvig (2010). *Artificial intelligence:* A modern approach. 3. ed. Upper Saddle River, NJ: Prentice-Hall.

Santhanam, R. and G. J. Kyparisis (1996). "A decision model for interdependent information system project selection." *European Journal of Operational Research* 89 (2), 380–399.

Saynisch, M. (2010). "Beyond frontiers of traditional project management: An approach to evolutionary, self-organizational principles and the complexity theory-results of the research program." *Project Management Journal* 41 (2), 21–37.

Shenoy, C. and P. Shenoy (1999). "Bayesian network models of portfolio risk and return." *Computational Finance*, 87–106.

Shenoy, C. and P. P. Shenoy (2002). "Modeling Financial Portfolios Using Belief Functions." In: *Belief Functions in Business Decisions*. Ed. by J. Kacprzyk, R. P. Srivastava and T. J. Mock. Heidelberg: Physica-Verlag HD, p. 316–332.

Tasche, D. (2008). "Capital Allocation to Business Units and Sub-Portfolios: the Euler Principle." In: *Pillar II in the new Basel accord: The challenge of economic capital*. Ed. by A. Resti. London: Risk Books, p. 423–453.

Teller, J. (2013). "Portfolio Risk Management and Its Contribution to Project Portfolio Success: An Investigation of Organization, Process, and Culture." *Project Management Journal* 44 (2), 36–51.

Teller, J. and A. Kock (2013). "An empirical investigation on how portfolio risk management influences project portfolio success." *International Journal of Project Management* 31 (6), 817–829.

Theoharidou, M., P. Kotzanikolaou and D. Gritzalis (2009). "Risk-Based Criticality Analysis." In: *Critical Infrastructure Protection III: Third Annual IFIP WG 11.10 International Conference on Critical Infrastructure Protection, Hanover, New Hampshire, USA, March 23-25, 2009, Revised Selected Papers*. Ed. by C. Palmer and S. Shenoi. Berlin, Heidelberg: Springer Berlin Heidelberg, p. 35–49.

Trucco, P., E. Cagno, F. Ruggeri and O. Grande (2008). "A Bayesian Belief Network modelling of organisational factors in risk analysis: A case study in maritime transportation." *Reliability Engineering & System Safety* 93 (6), 845–856.

Wasserman, S. and K. Faust (2009). *Social network analysis:* Methods and applications. 19. printing. Cambridge: Cambridge Univ. Press.

Wehrmann, A., B. Heinrich and F. Seifert (2006). "Quantitatives IT-Portfoliomanagement." *WIRTSCHAFTSINFORMATIK* 48 (4), 234–245.

Wiest, J. D. (1981). "Precedence diagramming method: Some unusual characteristics and their implications for project managers." *Journal of Operations Management* 1 (3), 121–130.

Wolf, T. (2015). "Assessing the Criticality of IT Projects in a Portfolio Context using Centrality Measures." In: *Wirtschaftsinformatik Proceedings*, Paper 48.

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

II.2 Systemic Risk in IT Portfolios – An Integrated Quantification Approach[1,2]

[1] This doctoral thesis appends the following comments and corrections to the published version of this paper:

- On page 7 and 8 of the paper, the variables σ_i and σ_j are referred as the variance of the expected value, but the correct notation is the standard deviation.
- The result of Equation (6), on page 13 of the paper is a matrix and not a vector as stated. Therefore the expression $x = (I - \alpha * A^T)^{-1} \circ E$ is not correct. The correct expression of the equation is: $X = (I - \alpha * A^T)^{-1} \circ E$.
- As mentioned on page 7 of the paper, for the purpose of quantitative assessment of an IT portfolio, we draw on an approach inspired by both portfolio theory of Markowitz (Markowitz 1952) and the approach of Beer et al. (2013), whereby the approach of Beer et al. (2013) is compatible with the Bernoulli principle (Bernoulli 1954). On page 8 and 13 of the paper we replace the parameters of the covariance ($\sigma_i\sigma_j$ and ρ_{ij}) of the Equation (1) ($\Phi(\mu,\sigma) = -C + \Sigma\,\mu_i - \gamma\,\Sigma\Sigma\,\sigma_i\sigma_j\rho_{ij}$) based on our own interpretation and for our modelling purposes. We interpret $\sigma_i\sigma_j$ as a (not normalized) covariance, and use it as an exogenous matrix in Equation (6). Further, we do not use the Bravais–Pearson correlation coefficient ρ_{ij} and use a pseudo correlation value $\tilde{\rho}_{ij}$ instead. In Equation (2), we replace $\sum_i \sum_{j \neq i} \sigma_i\sigma_j\rho_{ij}$ with $\sum_i \sum_{j \neq i} \sigma_i\sigma_j\tilde{\rho}_{ij}$. $\sum_i \sum_{j \neq i} \sigma_i\sigma_j\tilde{\rho}_{ij}$ is based on an element-wise multiplication of the elements of the matrices $(I - \alpha * A^T)^{-1}$ and E in Equation (6) and the sum of the rows of the resulted matrix. The inspiration and adoption of parameters give the impression that our method is a well-founded and statistically rigorous approach, which is not the case. It constitutes an ad-hoc approach inspired by the formulas mentioned up.

  Furthermore, on page 7 we state the assumption that the cash flows of an IT project are normally distributed random variables. The assumption, given that the utility function of the preference function is exponential, is necessary to be compatible with the Bernoulli principle (Bernoulli 1954). However, since our approach is ad-hoc this assumption is unnecessary for our method.

  Nevertheless, the adoption of the computational logic and respective assumption allows us to provide a pragmatic solution for the quantitative assessment of systemic risk in IT portfolios. Further, it enables us to evaluate and depict the plausibility of our method based on the comparison of its result with the result of the established method of Beer et al. (2013).
- On page 13, in Equation (5) we elaborate on the variables of α-centrality. It is necessary to extend the elaboration of the variable α by the fact that large values of α indicate that the status of nodes (IT projects) is endogenously (based on network structure) determined, while the small values mean that the dependencies between nodes (transitive dependencies) is relatively unimportant in determining the overall status of the nodes (Bonacich and Lloyd, 2001). Although the choice of α has a high impact on the results of this paper, we did not address how to choose α. An organization for instance can apply our method in real-world cases, and use ex-post historical data of these IT portfolios to estimate an appropriate α for its IT portfolios.
- In Equation (6) ($X = (I - \alpha * A^T)^{-1} \circ E$) the question which arise is: Is the matrix $(I - \alpha * A^T)$ invertible? The range of α is the answer to this question. The method limits α to the range of $0 < \alpha < \lambda_1^{-1}$ (the spectral radius of A). This bounds on α ensures that the matrix $(I - \alpha * A^T)$ is invertible (Benzi and Klymko 2015).

References

Beer M, Fridgen G, Müller H, Wolf T (2013) Benefits Quantification in IT Projects. In: 11th International Conference on Wirtschaftsinformatik, pp 707–720

Benzi M, Klymko C (2015) On the Limiting Behavior of Parameter-Dependent Network Centrality Measures. SIAM Journal on Matrix Analysis and Applications 36(2):686–706. doi: 10.1137/130950550

Bernoulli, D. 1954. “Exposition of a New Theory on the Measurement of Risk,” Econometrica (22:1), January, pp. 23-36.

Bonacich P, Lloyd P (2001) Eigenvector-like measures of centrality for asymmetric relations. Social Networks 23(3):191–201. doi: 10.1016/S0378-8733(01)00038-7

Markowitz, H. 1952. "Portfolio selection," The Journal of Finance (1:7), March, pp. 77-91.

Authors:	Martina Beer, Thomas Wolf, Tirazheh Zare Garizy
Published in:	Proceedings of the 36th International Conference on Information Systems (ICIS), Fort Worth, Texas, USA, December 2015

Abstract

Recent trends in digitalization, combined with continuous innovation pressure, have led to an increasing number of IT projects that are often accomplished within huge IT project portfolios. Although numerous IT project and portfolio evaluation and planning approaches have been developed and applied in companies all over the world, approximately 25% of IT projects still fail, which may result in a global value destruction of approximately 900 billion USD. One main reason for the numerous failures is the lack of transparency concerning dependencies within IT portfolios. This paper draws on graph theory to present a rigorous assessment of systemic risk that is based on different types of direct and indirect dependencies within IT portfolios. Based on this assessment, an integrated, novel, and quantitative approach to IT portfolio evaluation is presented that strives to mitigate IT project failures as it helps decision makers to evaluate their IT portfolios more adequately.

Keywords: Ex ante IT portfolio evaluation, project dependencies, intra-temporal dependencies, inter-temporal dependencies, systemic risk, risk quantification, network analysis, α-centrality

[2] This research was carried out in part in the context of the Project Group Business and Information Systems Engineering of the Fraunhofer Institute for Applied Information Technology FIT.

Grateful acknowledgment is due to the DFG (German Research Foundation) for their support of the project "ITPM (FR 2987/2-1, BU 809/13-1)" making this paper possible.

II.2.1 Introduction

New trends, such as digitalization, intensify the already high importance of information technology (IT) to companies all over the world. Additionally, recent technological developments and associated changes in customer expectations are forcing companies to develop innovative ideas and creative solutions (Nguyen and Mutum, 2012) that can be translated into a vast increase in IT projects to fulfill these demands. As a consequence, more and more IT projects are being split into several stand-alone but interrelated IT solutions with customer impact to satisfy this continuous demand for innovation. To address this development and the resulting increase in IT project portfolio complexity, a holistic approach the valuation of IT project portfolios, hereinafter referred to simply as IT portfolios, is crucial. Although there are already a number of approaches for the valuation of IT projects and portfolios, investments in planning techniques for IT projects and IT portfolios continue to increase (Gartner 2014). Nevertheless, an alarmingly high number of IT projects fail. Flyvbjerg and Budzier (2011) contend that approximately 16% of IT projects cause an on average budget deficit of approximately 200%. Moreover, project failure rates greater than 25% have been reported (Mieritz 2012). The failure of so many IT projects could result in a global value destruction of approximately 900 billion USD (Gartner 2013). Recent studies have shown that existing methods for IT project and IT portfolio evaluation might not be sufficient (Flyvbjerg and Budzier 2011; Radar Group 2012).

IT projects are usually planned and implemented within aggregated and quite extensive portfolios of several different IT projects, such as mobile application development projects, database restructuring projects, and large software development projects for business system applications. Therefore, they incorporate high-order dependencies, in contrast to projects that are accomplished in isolation or in pairs (Graves et al. 2003). Consequently, one major reason for IT project failures may be inadequate reflection upon and consideration of dependencies regarding shared assets between IT projects (CA Research 2008). This premise is supported by a questionnaire survey of 560 IT decision makers in Scandinavia, conducted by the Radar Group, which revealed that one reason for IT project failure is a lack of transparency regarding dependencies (Radar Group 2012). The management of such dependencies could help to reduce overall IT project costs and increase the benefits achieved by IT projects (Santhanam and Kyparisis 1996). However, many existing IT project evaluation methods consider neither dependencies associated with IT portfolios nor their associated risks. Although there are some approaches for IT project or IT portfolio evaluation (cf. Beer et al. 2013; Kundisch and Meier 2011; Lee and Kim 2001; Wehrmann et al. 2006) that do consider dependencies, they do not consider the specific characteristics of IT portfolio dependencies. Different types of dependencies and the prevalence of transitive dependencies are almost consistently neglected in existing IT portfolio evaluation methods. Furthermore, some approaches that do consider the dependencies of IT project portfolios in more elaborate ways fail to evaluate them quantitatively and are therefore not regarded as reasonable decision support tools for IT portfolio managers (Müller et al. 2015). Most approaches also lack feasibility for practical application (Zimmermann 2008), which further emphasizes the need from praxis for adequate means for IT portfolio evaluation that incorporate a detailed assessment of risk based on interdependencies among IT projects.

As stated by Benaroch and Kauffmann (1999), "a major challenge for information systems (IS) research lies in making models and theories that were developed in other academic disciplines usable in IS research and practice." In fulfilling the need for a method for IT portfolio evaluation that incorporates a detailed assessment of risk based on inherent interdependencies, we consider IT portfolios as networks of interdependent nodes, where each node reflects an IT project and the arcs reflect dependencies between projects. We draw on concepts from sociological research based on graph theory that have already been applied to the analysis of several network-alike structures, in areas such as social network analyses (Wasserman and Faust 1994; Newman 2010), supply chain management (Kim et al. 2011; Fridgen and Zare Garizy 2015), and IT infrastructure management (Simon and Fischbach 2013). To be more precise, we focus on the application of centrality measures that identify the central nodes of networks based on their positioning and/or their connectivity to other nodes and are consequently considered suitable for use in assessing the systemic risk arising from dependencies among the nodes of the network, or rather, the projects in the portfolio. Furthermore, we integrated the resulting criticality score, derived from the centrality measure, to the existing classical portfolio theory approaches.

Thus, we are able to develop a novel and fresh approach for value-based IT portfolio evaluation that integrates costs, benefits, risks, and different types of dependencies in a thoroughly quantitative and feasible way. The appropriate consideration of different types of dependencies and in particular of transitive dependencies in IT portfolios is a main contribution of this research because these have been identified as important reasons for IT project failures but have not been sufficiently considered in previous research, to the best of our knowledge. The consideration of these dependencies is important for decision makers because it will result in better estimation of the values of IT portfolios. Better IT portfolio value estimation will make it possible for decision makers to request appropriate budget for IT portfolios and avoid the difficulty of applying for additional budget during project execution as a result of unseen dependency risks. Therefore, the results should empower decision makers to consider dependencies and associated risks accurately in their IT portfolio evaluations. Since, if considered properly, the risk associated with dependencies in some cases might result in a negative portfolio value (when costs and risk surpass benefits), this approach moreover reduces the risk of false investments.

To provide a relevant and rigorous approach to IT portfolio evaluation, we followed the recommendations of Hevner et al. (2004) and Gregor and Hevner (2013) and developed our approach as an artifact, according to their Design Science Research guidelines. To describe the *problem relevance* and the need for an integrated approach for value-based IT portfolio evaluation, we illustrate current developments and existing challenges in the motivation section. Based on a structured review of the literature and recent state-of-the-art articles, we furthermore explain and relate key terms associated with dependencies and summarize current methods for their appraisal in section 2. In section 3, we present our integrated approach step by step to ensure comprehensibility. To guarantee *research rigor*, the *artifact design* is based on well-established methods and theories prevalent in literature, extended or adopted to fit our purposes. We also performed some *evaluation* cycles during the development-phase to ensure rigor and relevance. We *evaluate* the artifact regarding *quality, utility* and *efficacy* in section 4. Therefore, we draw on simulation, which according to Hevner et al. (2004) is an established evaluation method. To demonstrate the applicability of our artifact, we moreover provide an application example and describe its benefits in comparison to other established theories and practices. Section 5 concludes the paper and includes a discussion of the limitations of our approach and future research needs.

II.2.2 Theoretical Background

For decades, IT project and IT portfolio evaluation and appropriate consideration of IT project dependencies have been highly relevant topics in research and practice. Hence, it is reasonable that over the last few decades, a great number of publications have been published on this subject. To develop a fresh approach that holistically assesses dependencies within a value-based IT portfolio evaluation, we need to understand and integrate three subtopics of research on the subject. Thus, we first present a general overview of methods for IT project and IT portfolio evaluation. We then identify and elaborate different types of dependencies before describing how they are currently appraised in literature. We performed a keyword-based search (using the terms dependency, interdependency, interaction, project, portfolio, information technology, information systems, model, method, requirements, approach, quantification, assessment, IT project, evaluation, value assurance, and valuation) of various data bases (AIS Electronic Library, EBSCOhost, EmeraldInsight, ProQuest, ScienceDirect, Wiley, Google Scholar, JStor, Springer, and ACM). Although this search identified many relevant articles, we found that most of these were already considered in the most recent articles summarizing the state of the art. On our first subtopic of IT project and IT portfolio evaluation methods, Beer et al. (2013) performed an extensive literature review as part of their research on an integrated project quantification method. The second subtopic, different types of dependencies, was outlined by Wolf (2015) and also, quite comprehensively, by Müller et al. (2015), who published a state-of-the-art article dedicated to different types of dependencies and their current appraisal. Therefore, based on our keyword-based search and the recently published state-of-the-art articles, we developed a brief, sound, and integrated overview of the existing literature. Our review, however, is structured to address all three of the aforementioned subtopics. For more detailed reviews of the literature on these subtopics, please refer to the articles of Müller et al. (2015), Wolf (2015), and Beer et al. (2013).

II.2.2.1 Methods for IT project evaluation and IT portfolio evaluation

It is important to note that the evaluation of IT portfolios typically includes the evaluation of IT projects. Furthermore, IT project evaluation methods are sometimes simply adopted to IT portfolio evaluation. Therefore, as it is almost impossible to differentiate strictly between IT project and portfolio approaches, this section gives only a brief overview of important IT project and portfolio evaluation methods, without distinguishing between them regarding their application within a project or portfolio context. There are indeed many approaches and methods in literature that address IT project and portfolio evaluation. Though, integrated evaluation approaches that consider benefits, costs, risks, and dependencies in a quantitative and feasible manner are quite rare, even though this has been identified as a highly relevant topic in research and practice (Müller et al. 2015). Existing approaches often account only for qualitative factors. Some models also use quantitative figures for the valuation of benefits and sometimes risks — but not, unfortunately, on a monetary basis. We present below a brief summary of some existing approaches to IT project and portfolio evaluation. Because the focus of this paper is on quantitative methods for IT project and portfolio evaluation, we focused on these types of approaches, although we are aware that many publications are focused on a more general evaluation that also accounts for qualitative factors.

Frequently used tools for IT project evaluation are so-called scoring models (e.g., Walter and Spitta 2004; Zangemeister 1976), which identify and weight all relevant evaluation criteria for a specific IT project. The resulting scores are aggregated to provide an overall value that enables the comparison of different alternatives. The Balanced Scorecard by Van Grembergen and De Haes (2005) is also a type of a scoring model. The cause-and-effect relations between key qualitative and quantitative figures are described to identify two general types of key figures: performance drivers and output figures. The project is evaluated on the basis of the degree of target achievement of each key figure. The so-called WARS-Model (Ott 1993) has the ability to estimate benefits and costs crudely by classifying them into three categories according to their tangibility. The risk aversion of decision makers is taken into account by assessing different risk stages for optimistic or pessimistic decision makers. A more quantitative approach for IT project evaluation was presented by Schumann (1993), whose approach is based on functional chains. In this approach, benefits can be expressed in monetary terms by focusing on their effects. However, this approach lacks a proper quantitative integration of risks and dependencies. Another approach that considers quantitative values for costs, benefits, risks, and dependencies in an integrated manner is the so-called benefits management approach of Beer et al. (2013). Using preference functions, they derive a risk-adjusted monetary project value. This has been proven a feasible approach by business experts. Like the approach proposed by Beer et al. (2013), many approaches for IT project and portfolio evaluation refer to or are based on the well-known methods of decision theory, as for instance μ/σ-decision rules (which means that the investment decisions of decision makers in companies are reached by comparing the expected values of investments while taking into consideration their respective risks). This seems to be an adequate way to derive a risk-adjusted IT portfolio value, although some approaches (e.g. Beer et al. (2013)) only applied these methods in a single project instead of a project portfolio context.

Despite the vast number of different approaches for IT project and portfolio evaluation in research and practice, to the best of our knowledge, there is no integrated, value-based evaluation approach that also considers the specific characteristics of dependencies between projects in an IT portfolio.

II.2.2.2 Different types of dependencies

As mentioned before, there are different types of dependencies between the projects within IT portfolios. This fact is also reflected in literature. We found that some articles just mention certain types of dependencies, while others try to integrate and structure these types of dependencies in specific frameworks. Most articles (e.g., Lee and Kim (2001); Santhanam and Kyparisis (1996); Tillquist et al. (2004), Zuluaga et al. (2007)) describe resource dependencies, technical dependencies, and dependencies regarding benefits. A further segmentation of resource dependencies distinguishes between personal and technical dependencies (Wehrmann et al. 2006). Personal dependencies refer to projects competing for personnel resources, and technical dependencies refer to projects competing for technical resources. In contrast to the segmentation provided by Wehrmann et al (2006), Kundisch and Meier (2011) developed a framework for subdividing resource dependencies into allocation, performance, and sourcing dependencies.

Technical dependencies are defined in many different ways in the literature, but in general, two major categories can be differentiated: technical dependencies can either arise from two projects competing for technical resources, as described by Wehrmann et al. (2006), or they can represent the fact that a specific project requires input from a precedent-associated project. Benefit dependencies may also be considered as synergies (Buchholz and Roth 1987) and can be realized if the value of at least one of the concerned projects increases when being implemented simultaneously with another. Examples of such synergies could be databases that have been built for specific projects but can also be used for other projects. Other examples are accumulated expert knowledge that is relevant to more than one project and the reuse of code fragments for two similar software development projects.

A well-established way of structuring dependencies is provided by Wehrmann et al. (2006) and Zimmermann (2008), who distinguish between intra- and inter-temporal dependencies. Intra-temporal dependencies refer to the dependencies of different projects that are assigned to the same period in time. Intra-temporal dependencies are presumed to encompass structural dependencies and resource dependencies (Wehrmann et al. 2006). Considering the number of related published articles, intra-temporal dependencies seem to be well recognized in literature, especially within the spectrum of Operations Research (e.g., Aaker and Tyebjee 1978; Carraway and Schmidt 1991; Fox et al. 1984; Gear and Cowie 1980; Medaglia et al. 2007; Kundisch and Meier 2011; Lee and Kim 2001; Santhanam and Kyparisis 1996; Stummer and Heidenberger 2003). In general, there is a common understanding in literature about the causes of resource dependencies in IT projects. They are presumed to arise from the sharing of scarce resources, such as personnel, hardware (servers), and software (database logic) resources (Graves and Ringuest 2003; Santhanam and Kyparisis 1996). Structural dependencies can be divided into the subcategories of process dependencies, data dependencies, and IT-functionality dependencies if two or more IT projects are, for example, based on the same processes, use the same data, or apply the same IT functionalities (Wehrmann et al. 2006).

Inter-temporal dependencies, in contrast, refer to dependencies between different projects that are assigned to different periods in time. Thus, inter-temporal dependencies describe a coherence by which a succeeding project is based on a preceding one. These dependencies can be distinguished as logical and technical or rather technological dependencies (Maheswari and Varghese 2005, Santhanam and Kyparisis 1996). Logical dependencies or integrative coherences are further subdivided into hard and soft dependencies by Bardhan et al. (2004). Other authors distinguish inter-temporal dependencies either in inter-temporal output interactions (e.g., Pendharkar 2014) or in inter-temporal output–resource interactions (e.g., Dos Santos 1991; Kumar 1996; Panayi and Trigeorgis 1998; Taudes 1998; Taudes et al. 2000). Most approaches, however, focus on output–resource-based dependencies, whereas output dependencies without the resource context are barely included.

To provide an overview of different types of dependencies and to enhance comprehensibility, Figure 1 summarizes the different types of dependencies in a revised framework based on those by Wehrmann et al. (2006) and Wolf (2015).

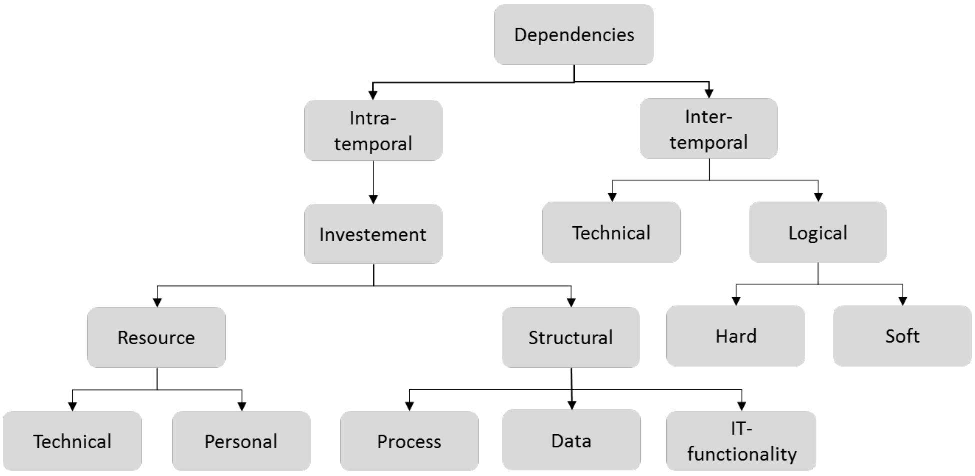


Figure 1. Dependencies in IT Portfolio

II.2.2.3 Methods for consideration of dependencies

To provide a more structured overview of existing research regarding the current appraisal of different types of dependencies, we structured this section according to the well-established classification of intra- and inter-temporal dependencies as described by Wehrmann et al. (2006).

Intra-temporal dependencies

Various approaches to account for intra-temporal dependencies among IT projects and IT portfolios exist. One approach is to integrate them as auxiliary conditions in an optimization model (Kundisch and Meier 2011; Lee and Kim 2001; Santhanam and Kyparisi 1996). Another approach, used by Beer et al. (2013), Butler et al. (1999), and Wehrmann et al. (2006), for example, is to draw on the portfolio theory of Markowitz (1952) to determine a risk- and return-optimized IT portfolio using the normalized covariances of the corresponding IT projects. A modified discounted cash flow approach, presented by Verhoef (2002), considers dependencies implicitly while focusing on cost and time risks for a given interest rate. However, many of these methods fall short to some degree because of their underlying financial restrictions (Zimmermann et al. 2012) or because they often do not consider the dependence structure of the whole portfolio but rather focus only on the dependencies between two specific projects. A wide number of publications concerning intra-temporal dependencies, particularly from problem-solving domains such as Operations Research, do not focus on ex ante evaluation alone (meaning that an evaluation takes place prior to the start of an IT project or IT portfolio) but rather provide procedures to consider dependencies continuously during the portfolio planning process. Thus, the contributions of these papers are methods, models, or algorithms that are aimed at solving specific capacity problems in the context of intra-temporal dependencies, rather than integrating these intra-temporal dependencies in the IT portfolio evaluation (Aaker and Tyebjee 1978; Carazo et al. 2010; Carraway and Schmidt 1991; Cho and Kwon 2004; De Maio et al. 1994; Doerner et al. 2006; Eilat et al. 2006; Fox et al. 1984; Gear and Cowie 1980; Klapka and Pinos 2002; Lee and Kim 2001; Liesiö et al. 2008; Medaglia et al. 2007; Nelson 1986; Santhanam and Kyparisis 1996; Stummer and Heidenberger 2003; Weingartner 1966).

Inter-temporal dependencies

Inter-temporal dependencies within IT portfolios are most commonly assessed by using real options-based approaches, which stem from options theory in the financial sector. Several methods described in literature are based on the Black–Scholes model, and some use binomial trees to represent inter-temporal dependencies (cf. Bardhan et al. 2004; Benaroch and Kauffmann 1999; Dos Santos 1991; Taudes et al. 2000). As both approaches were originally developed in the financial sector, they feature specific restrictions and assumptions that are only partly fulfilled in the context of IT portfolios (Emery et al. 1978; Schwartz and Zozaya-Gorostiza 2003). Therefore, their applicability to inter-temporal dependencies in the context of IT portfolios is doubtful. For a more detailed discussion of whether real options approaches are applicable in the IT portfolio context, please refer to Diepold et al. (2009) and Ullrich (2013), who present a detailed investigation into the transferability of these methods to the consideration of dependencies in IT project and IT portfolio evaluation.

There have also been some attempts to integrate the two types of dependencies, namely inter- and intra-temporal dependencies (cf. Bardhan 2004, Pendharkar 2014). However, based on the outlined examination of current approaches for IT project and portfolio evaluation, different types of dependencies in IT portfolios, and their current appraisal, we can conclude that different types of dependencies are almost always considered in isolation from one another. However, because in reality different types of dependencies are interconnected and can be found in every IT portfolio, they have to be considered in a holistic way, which is not done by any approach proposed so far (cf. Müller et al. 2015). Moreover, we found that none of the existing IT portfolio evaluation and management techniques explicitly considers transitive dependencies between IT projects within IT portfolios. An assessment of transitive dependencies is essential to an appropriate risk assessment and value-based evaluation in these network-like structures. Therefore, none of the investigated approaches can be considered completely appropriate for the purpose of integrated value-based evaluation of IT portfolios with consideration of their characteristic inherent dependency structures.

II.2.3 Modeling Procedure, Assumptions, and Requirements

In this section, we present an integrated, quantitative approach for holistic IT portfolio evaluation. This approach not only considers different types of dependencies but also accounts for transitive dependencies. We first introduce an integrated approach that is capable of accounting for the costs, benefits, risks, and dependencies of IT projects in a portfolio context. We then describe how this approach can be expanded to account for intra- and inter-temporal dependencies within an IT portfolio. We introduce a procedure to quantify the strength of intra- and inter-temporal dependencies and aggregate the strength assessments into a uniform dependency value. Based on this value and considering the IT portfolio as an IT project network, we use α-centrality to measure and quantify the dependence structure of an IT portfolio, including inherent transitive dependencies. Based on this procedure, we strive to determine a risk-adjusted IT portfolio value that considers costs, benefits, risks, and dependencies in a comprehensive und quantitative manner.

II.2.3.1 An Integrated view of IT project evaluation

For the purpose of quantitative assessment of an IT portfolio, we draw on an approach inspired by the portfolio theory of Markowitz (Markowitz 1952). More specifically, we adapt and modify the integrated approach of Beer et al. (2013), who integrate benefits, costs, risks, and a superficial kind of dependencies to determine a risk-adjusted IT project value using the preference function. This function is an established method in decision theory (Bernoulli 1738; Bernoulli 1954; Markowitz 1952; von Neumann and Morgenstern 1947) and has been used in a considerable number of IT project-related studies (cf. Bardhan et al. 2004; Fogelström et al. 2010; Fridgen and Müller 2011; Hanink 1985; Zimmermann et al. 2008). According to Beer et al. (2013), this risk-adjusted IT project value Φ is based on the overall cost C of the complete IT project i and the aggregated sum $\Sigma\mu_i$ of all projects' expected benefits μ_i. In a manner similar to that proposed by Markowitz, dependencies are considered in terms of the Bravais–Pearson correlation coefficient ρ_{ij} and offset within one term for the overall risk adjustment $\Sigma\Sigma\ \sigma_i\sigma_j\rho_{ij}$. The Bravais–Pearson correlation coefficient is a statistical measure of the linear correlation between two variables, or in the case of Beer et al. (2013), between two benefits of an IT project. Its value lies between -1 and 1, where -1 indicates a perfect negative linear correlation, 0 indicates that there is no linear correlation, and +1 indicates a perfect positive linear correlation. Since a negative correlation value decreases the overall value of risk adjustment, it is considered to represent synergies between the respective benefits. In contrast, a positive value is considered to refer to any other kind of dependencies that consequently increase the overall value of risk adjustment or rather the risk discount to the overall project value.

The other parameters of the term of risk adjustment are σ_i and σ_j representing the variances of the values of the expected benefits. Furthermore, to account for the level of risk aversion of the decision maker, this risk adjustment term is weighted by a risk aversion parameter, in our case referred to as γ. The risk aversion parameter γ is a linear transformation of the Arrow–Pratt characterization of absolute risk aversion (Arrow 1971) and reflects a decision maker's attitude toward risk in uncertain situations. The value of γ increases with the decision maker's level of risk aversion, which means that the higher the value of γ is, the more risk-averse the decision maker is. Highly risk-averse decision makers tend to invest in less risky investment options, whereas less risk-averse decision makers tend to invest in more risky investment options. In practice, the degree of risk aversion can be determined at the executive level using an elaborate questionnaire, according to Sauter (2007) and Beer et al. (2013). Based on this considerations, the risk-adjusted IT project value can be expressed by the following preference function:

$$\Phi(\mu, \sigma) = -C + \Sigma\, \mu_i - \gamma\, \Sigma\Sigma\, \sigma_i\sigma_j\rho_{ij} \qquad (1)$$

The approach described above is used for the evaluation of single IT projects with a particular focus on benefits management (through the integration of costs, benefits, dependencies among benefits, and risks). This approach lacks direct applicability in an IT portfolio context and does not take into consideration the different types of dependencies described previously. However because this approach is inspired by Markowitz portfolio theory, it can easily be adapted to the evaluation of IT portfolios. In contrast to Beer et al. (2013), we take a cash flow-based perspective, in a manner similar to that described by Fridgen et al. (2015), and state the following assumption:

Assumption 1: The cash flows of an IT project are normally distributed random variables $cf_i \sim N(\mu_i, \sigma_i)$.

Although project cash flows might not be normally distributed in every case, it is common in IT portfolio management to assume that they are (cf. Fridgen and Müller 2011, Fridgen et al. 2015; Wehrmann et al. 2006; Wehrmann and Zimmermann 2005; Zimmermann et al. 2008). Based on this assumption, we can derive the distribution parameters μ_i and σ_i for each IT project, where $i = 1 \ldots n$ indicates the respective IT project of the IT portfolio. Consequently, μ_i represents the expected value of IT project i, and σ_i indicates the variance of this expected value, or rather, the corresponding risk.

Whereas Beer et al. (2013) and Fridgen et al. (2015) took dependencies into consideration by means of a correlation coefficient between every pair of underlying investigation objects and derive an overall term for risk adjustment, we distinguish between an IT project risk term $\Sigma\ \sigma_i^2$ that refers to the risk related to a particular IT project and an IT portfolio risk term $\Sigma\Sigma\ \sigma_i \sigma_j \tilde{\rho}_{ij}$ that refers to the systemic risk originating from the inherent direct and indirect dependencies between IT projects in the IT portfolio. However, the Bravais–Pearson correlation coefficient $\rho_{ij}$was developed to determine the values of coherence based on statistically measureable historical data (e.g., covariance of the shares in the stock market), which implicitly describe transitive dependencies as well. However, in the context of the ex ante evaluation of IT projects, historical data for the statistical calculation of covariance are usually not available. Instead, in this case, the corresponding prevalent values are mostly represented by ex ante expert estimations of project dependencies. Because experts normally are asked for pairwise estimations of project dependencies, they usually are not aware of possible transitive dependencies, which are consequently mostly neglected in the resulting estimated covariance matrix of a corresponding IT portfolio. Therefore, the Beer at al. (2013) approach is able to consider dependencies in a very ingenuous way only, and is neither able to consider different types of dependencies nor transitive dependencies.

$$\Phi^*(\mu, \sigma) = \sum_i \mu_i - \gamma \sum_i \sigma_i^2 - \gamma \sum_i \sum_{j \neq i} \sigma_i \sigma_j \tilde{\rho}_{ij} \qquad (2)$$

As we strive to consider both, different kinds of dependencies as well as direct and transitive dependencies, we refrain from using the classical Bravais–Pearson correlation coefficient ρ_{ij}. Instead, we consider a value $\tilde{\rho}_{ij}$ with $0 \leq \tilde{\rho}_{ij} \leq 1$ to reflect the aggregated strength of dependencies between pairs of IT projects $i, j = 1 \ldots n$. We moreover draw on *α-centrality* to determine a corresponding IT portfolio risk term $\Sigma\Sigma\ \sigma_i \sigma_j \tilde{\rho}_{ij}$ that accounts not only for direct but also for transitive dependencies. However, before we are able to do so, we need to assess the different types of dependencies between pairs of IT projects in the IT portfolio and aggregate them into a single dependency value that we can quantify.

II.2.3.2 Assessing different types of dependencies

As described previously, there are different types of dependencies within an IT portfolio. We use the distinction made by Wehrmann et al. (2006) between intra- and inter-temporal dependencies. However, we do not consider synergies between different IT projects within our term of risk adjustment. This seems plausible though, since the coherence between IT projects have been reported to rather exist due to dependencies than to synergies (e.g. Häckel and Hänsch 2014). In the case of intra-temporal dependencies, IT projects can be dependent on each other because they share resources (e.g., personnel) or infrastructure (e.g., data or databases). Therefore, we use the word "asset" to refer to either resources or infrastructure components that are planned for an IT project. In addition, each IT project can be separated into many interdependent activities. Accordingly, the dependencies between two IT projects can be considered as the result of dependencies on a more granular level. To facilitate this characterization, we do not distinguish between different levels of granularity; rather, we consider an IT project to be the most granular level, which cannot be divided into further distinct categories of activities. Furthermore, we assume that every IT project is assigned to one specific period of time t, i.e., that the start and end date of the project are within the same period. In reality, IT projects often take place over several months. Consequently, we assume that these IT projects can be subdivided into smaller ones that can be assigned to specific periods of time. An IT portfolio usually has a specific planning horizon and encompasses IT projects that take place during many of the covered periods $t = 1 \ldots T$. There can also be 1 to n IT projects within the same period of time, because there might be more than one IT project going on at the same time, even in a small company.

There are two different perspectives on how assets are shared between IT projects: the asset pooling perspective and the asset accounting perspective. The *asset pooling perspective* considers different IT projects to draw on the same pool of assets. A specific asset can be used by $[1 \dots n]$ IT projects. However, if the IT projects take place at the same point in time, they have to share the asset, and consequently, each IT project only accounts for a specific percentage of the asset between $[0\% \dots 100\%]$. At each point in time, the sum of the asset shares of an IT project cannot exceed 100%. If asset a_1 is shared between IT projects $i, j,$ and k and the shares of the IT projects for asset a_1 are $a_{1_i}, a_{1_j},$ and a_{1_k}, then $a_{1_i} + a_{1_j} + a_{1_k} \leq 100\%$. If the asset is not shared between two or more IT projects, there is no dependency caused by this asset. This coherence is illustrated in Figure 2.

This perspective, however, seems unfavorable in the case of inter-temporal dependent IT projects. Because the asset pool and an IT portfolio are strictly segregated, an IT project would have to be considered an asset to serve as an input to another IT project. Consequently, it would have to be considered as an asset and an IT project at the same time, which seems inappropriate for the purpose of this research.

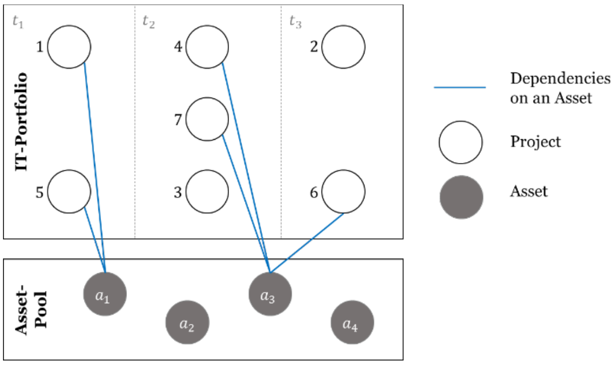


Figure 2. Asset Pooling in an Exemplary IT portfolio

In this context, the *asset accounting perspective* provides a more appropriate solution to the simultaneous consideration of intra- and inter-temporal dependencies. According to this perspective, assets are assigned directly to IT projects that depend upon them (cf. Figure 3). Consequently, $[1 \dots k]$ assets can be allocated to $[1 \dots n]$ IT projects with percentage shares between $[0\% \dots 100\%]$. However, in this case as well, the sum of the asset shares of an IT project cannot exceed 100% at any point in time. If the asset is assigned to one specific IT project alone, there is no dependency to another IT project caused by this asset. For instance, if a software developer (a personnel resource) is allocated exclusively to project i, other projects have no dependency on project i associated with this asset.

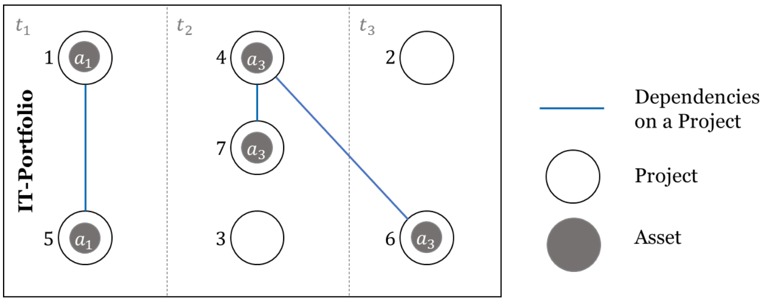


Figure 3. Asset Accounting in an Exemplary IT portfolio

As Figure 3 shows, according to the asset accounting perspective, dependencies are considered to exist between different projects but not between projects and assets. Therefore, in contrast to the asset pooling perspective, inter-temporal dependencies can easily be considered. However, it should be noted that an asset that is assigned to two consecutive IT projects (cf. projects 4 and 6 in Figure 3) does not constitute an inter-temporal dependency, because of our assumption that every IT project is assignable to one specific period of time. Therefore, if an asset is assigned to two projects that take place at different points in time, it does not cause any dependency, as the first project will have finished using the asset before the second project starts to use it.

In addition to the dependency caused by sharing a specific asset between IT projects, assets are typically able to cause a different type of risk: a risk associated with the availability of the asset itself. Each type of asset has an inherent risk of failure, which is independent of whether it is shared between different IT projects. In the context of personnel resources, the availability of a software developer, for instance, depends on the software developer’s health. Because this type of risk does not originate on the dependencies of different projects on specific assets, it is not considered within the IT portfolio risk term and thus is not considered in the following discussion.

II.2.3.3 Aggregating different types of dependencies into a single value

Since we strive to consider both inter- and intra-temporal dependencies, we need to aggregate them into a single quantitative value. Therefore, we take the asset accounting perspective, as described above, and draw on the idea presented by Wolf (2015), considering the IT portfolio to be an IT project network. Consequently, we model the IT portfolio as a connected and directed graph. Each IT project $i = 1 \dots n$ in the portfolio is represented by a node. A dependency (inter-/intra-temporal) between IT projects $i, j = 1 \dots n$ is represented by a directed edge between these IT projects. Inter-temporal dependencies are represented by a directed edge pointing from the dependent IT project to the IT project upon which it depends. Logically, when an IT project i is inter-temporally dependent on an IT project j, IT project j cannot be inter-temporally dependent on IT project i. Intra-temporal dependent IT projects share an asset within the same period of time. Hence, as these IT projects are affected at the same time, there is an edge from IT project i to IT project j and an edge from IT project j to IT project i. We define the weight of an edge in the graph as representing the strength of the dependency between two IT projects.

Figure 4 illustrates an example IT portfolio with inter- and intra-temporal dependencies between IT projects based on an IT project network perspective.

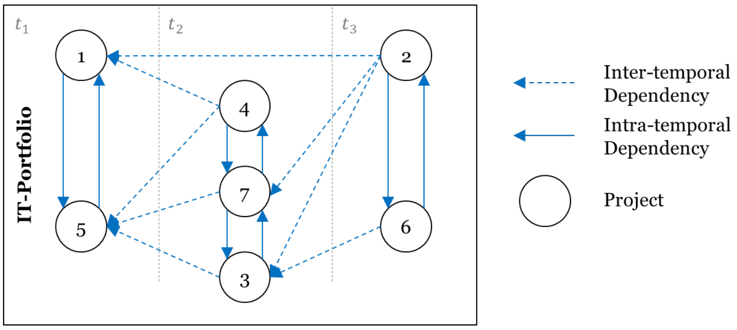


Figure 4. Exemplary IT portfolio

To aggregate intra- and inter-temporal dependencies to a single value, we quantify the strengths of these dependencies based on the same underlying factor. We identify "time" as the common factor that enables a quantitative determination of inter- and intra-temporal dependencies. More specifically, we consider the relative time lag that a particular IT project can cause to the other projects that depend on this particular project. We describe the quantification of intra- and inter-temporal dependencies below.

Intra-temporal Dependencies

In the case of intra-temporal dependencies, the relative time lag refers to the time that an IT project—given that all assets are available—would require for implementation. The lag describes the prolongation of this implementation time due to the struggle between two different IT projects regarding one critical asset. We thus consider two types of assets: uncritical assets a^{uc} that are not simultaneously required by different IT projects and critical assets a^{c} that are simultaneously required by at least two different IT projects. We strive to quantify the time lag in case all, none, or some percentage of the critical assets of a particular IT project are available. However, as the extent of such a time lag can differ based on the assets' importance to a particular IT project and the size of the project, we denote its value relative to the project size. Therefore, we consider each IT project $i = 1 \ldots n$ to have a size S^{p_i}, which is usually measured in time-related units, such as full-time equivalents (FTEs). However, we consider project size to represent the overall duration of the implementation of an IT project in working hours. Based on the average working hours of a specific company, this value can easily be converted into FTEs. Using the project's size, we are able to determine a project's duration D^{p_i} based on the number of assets that are assigned to the IT project.

Assumption 2: The coherence between the duration of an IT project and its assigned assets is linear.

Although this assumption might not be realistic for each type of asset, it seems plausible for at least the most important intra-temporal dependencies, and it is easy to grasp. Therefore, we consider it to be an appropriate assumption for the first step toward aggregation and consistent quantification of different types of intra-temporal dependencies. Based on this assumption, we are able to quantify the intra-temporal dependencies between two different IT projects. We calculate the prolongation of the project duration resulting from the reciprocal shortfall of required critical assets according to the following equation:

$$D_k^{p_i} = \frac{S^{p_i}}{(a_k^{uc} + \vartheta_k \cdot a_k^c)} \tag{3}$$

To do so, we use equation 3 to calculate two different scenarios, which will be related afterward. In the first (max-)scenario, we calculate the duration of the project for the case in which all planned assets a_k, uncritical assets a_k^{uc}, and critical assets a_k^cin each asset category $k = 1 \dots l$ (e.g., resources and infrastructure) are available. Whereas uncritical assets a_k^{uc} are presumed to be available without having any other project competing for them, the availability of critical assets a_k^c is reflected by the parameter ϑ_k, where $0 \leq \vartheta_k \leq 1$. This parameter represents the percentage of availability of the assets of a specific asset category. Consequently, in the case of the first scenario, $\vartheta_k = 1$ for each asset that is assigned to the IT project. In the second (min-)scenario, we calculate the duration of the project in the case of a rival IT project being given preference regarding all critical assets a_k^c. In this case, $\vartheta_k = 0$ for all competed-for assets. Combining the resulting values for the two scenarios, we can calculate the percentage of the project that can be accomplished with the available assets in the initially planned time frame (the originally planned period for the project duration when all assets are available). Consequently, we can determine the percentage of the project that remains incomplete during the initial time frame and is caused by asset category $k = 1 \dots l$ as follows:

$$\Delta D_k^{p_i} = 1 - \frac{D_{k_{max}}^{p_i}}{D_{k_{min}}^{p_i}} \qquad (4)$$

The result of equation (4) is the percentage of project i that remains incomplete because its critical assets are unavailable and blocked by project j. Therefore, the percentage of project i that might remain undone as a result of the critical asset dependency on project j is the weight of the edge from project i to project j or rather the strength of the corresponding dependency. Consequently, equation (3) quantifies the effects of IT projects competing for one or more critical assets. However, as mentioned before, equation (3) and (4) do not consider the prolongation of the project duration resulting from a shortfall of an assets (uncritical or critical). This is considered to be part of the project's individual risk (σ_i) in equation (2).

To illustrate the outlined coherence, we refer to Figure 3, where p_1 and p_5 have intra-temporal dependencies caused by a single asset category a_1. Let p_1 be a software development project with an approximate size of approximately 250 working hours, and let p_5 be a smaller project with an approximate size of 150 working hours. Project p_1 requires five assets a_1 from category $k = 1$ to be completed on schedule, and p_5 requires three assets. However, two specific software developers are required for both projects and thus are critical assets. Therefore, the critical assets $a_1^c = 2$ for both projects, whereas $a_1^{uc} = 3$ for p_1 and $a_1^{uc} = 1$ for p_5. According to equation (3), we can calculate the (max-)scenario with $\vartheta_1 = 1$ and the (min-)scenario with $\vartheta_1 = 0$ and relate the resulting values $D_{1_{min}}^{p_1} = 83.33$ and $D_{1_{max}}^{p_1} = 50$ to derive $\Delta D_1^{p_1} = 0.4$, which can be considered the percentage of project p_1 that remains incomplete during the initially planned time frame due to the critical asset category $k = 1$. The dependency of project p_1 on project p_2 is a result of the dependency on asset category k_1. Consequently, the weight of the edge from project p_1 to project p_2 is equal to 0.4.

In the case in which there is only one critical asset category, such as that described above, $\Delta D_k^{p_i}$ is considered to represent the quantification w_{ij} of the intra-temporal dependency between the dependent project p_i and another project p_j upon which it depends due to the specific asset category. However, if there are multiple critical asset categories $k = 1 \dots l$, we need to aggregate these categories to derive a single value for intra-temporal dependencies. In this case, $w_{ij} = \sum_{k=1}^{l} \Delta D_k^{p_i}$. However, this can potentially result in values of $w_{ij} > 1$. Because $w_{ij} = 1$ reflects the maximum dependency of 100%, we set $w_{ij} = 1$ for each aggregated value $w_{ij} > 1$.

Inter-temporal Dependencies

Inter-temporal dependencies are considered over the whole planning horizon of the IT portfolio. If two projects are inter-temporally dependent, they are assigned to different points in time that do not necessarily have to be consecutive. According to the precedence diagram method (Project Management Institute 2009), inter-temporal dependencies can be distinguished according to their start and finish points as follows:

- Finish-to-start (FS): The start of the successor project depends upon the completion of the predecessor project. Because the successor project is dependent on the result of the predecessor project, any delay in finishing the predecessor project can cause a delay in completion of the successor project. Consequently, we consider this as an inter-temporal dependency in the sense of our paper.
- Finish-to-finish (FF): The completion of the successor project depends on the completion of the predecessor project. This dependency describes a coherence where the completion of the succeeding project requires the preceding project to be completed to a specific extent. Since this dependency might cause a prolongation of the succeeding project, we consider it as an inter-temporal dependency in the sense of our paper.
- Start-to-start (SS): The successor and predecessor project should start at the same time and hence are allocated to the same period. As in this case there is no dependency between the successor and the results of predecessor project, we do not consider it as inter-temporal dependency in the sense of this paper.
- Start-to-finish (SF). The completion of the successor project depends on the start of the predecessor project. This implies that the predecessor project must be started before the successor project can be finished. Since this case does not reflect any kind of dependencies between the results of the predecessor project and the successor project either, but is mainly an issue for scheduling purposes, it is not considered as inter-temporal dependency in the sense of this paper.

In summary, we distinguish between only two types of inter-temporal dependencies: FS and FF dependencies, where incidents by predecessor projects might cause prolongations of successor projects, taking place at future points in time. As in the case of intra-temporal dependencies, we use the relative time lag to describe the prolongation of the project implementation time due to inter-temporal dependencies. In particular, we assess inter-temporal dependencies by calculating the relative prolongation of the project implementation of the succeeding project p_2 based on a delay in a preceding project p_1 (cf. Figure 4). In a case in which there is an FS dependency between p_2 and p_1, project p_2 cannot start before project $p_1$has been finished.

Therefore, we consider the strength w_{ij} of this dependency to be 100% and consequently declare $w_{21} = 1$. In contrast, if there is an FF dependency between p_2 and p_1, the completion of p_2 depends on the completion of p_1. Considering this coherence to be valid for partial completion as well, we can determine the strength of this type of dependency from the percentage of the predecessor project that has to be completed before the successor project can be completed. For example, if 60% of p_1 need to be completed before p_2 can be completed, we determine the strength w_{ij} of this dependency to be 60% and consequently declare $w_{21} = 0.6$.

II.2.3.4 Quantifying the dependence structure of IT portfolios based on α-centrality

As mentioned before, we strive to determine an IT portfolio risk term $\Sigma\Sigma\ \sigma_i\sigma_j\tilde{\rho}_{ij}$ that accounts for both direct and transitive dependencies in an IT portfolio. Therefore, we employ the idea presented by Wolf (2015), considering an IT portfolio to be an IT project network, where each node represents a project and each arc represents a dependency. Wolf (2015) identified the following five requirements that a centrality measure has to fulfill to be applicable in the context of IT portfolios:

1. The measurement accounts for directed relations between projects.
2. The result of the measurement for a specific project increases with the strengths of the relations with dependent projects.
3. The result of the measurement for a specific project increases with the number of directly dependent projects.
4. The measurement accounts for transitive dependencies, as the result increases with the number of indirectly dependent projects.
5. The result of the measurement of a specific project increases with the importance of directly and indirectly dependent projects.

Based on these requirements, Wolf (2015) introduced some common centrality measures and investigated whether and to what extent they are appropriate for use in the quantification of dependencies in IT portfolios. The result of this investigation was that α-centrality was identified as the most suitable measure for quantifying dependencies in IT portfolios. We consequently use α-centrality to assess the network dependence structure and the corresponding inherent systemic risk. According to Wolf (2015), α-centrality accounts not only for direct dependencies, such as the number of directly dependent projects, but also for indirect or transitive dependencies. It thereby considers more interconnected and therefore critical projects to contribute more strongly to the criticality of the projects upon which they are dependent than projects that are less critical (Wolf 2015). In the following discussion, we briefly introduce the elements of α-centrality and illustrate how the concept can be adapted to the derivation of an IT portfolio risk term that can be used within an integrated quantification approach. α-centrality can be calculated according to the following equation:

$$x = (\boldsymbol{I} - \alpha * \boldsymbol{A}^T)^{-1} * \boldsymbol{e} \tag{5}$$

Presuming the arcs of the IT project network to be weighted, the elements w_{ij} of the $n{\times}n$ adjacency matrix $\boldsymbol{A}$ represent the weighted conjunctions of the network, or rather, the strengths of the corresponding IT project dependencies. We previously outlined how we derive w_{ij} for intra- and inter-temporal dependencies. These values can be considered equivalent to the pseudo correlation values ρ_{ij} of (1), which represent the linear dependencies between every pair of investigation objects (e.g., IT projects), based on expert judgments. Therefore, we consider w_{ij} to equal $\tilde{\rho}_{ij}$ in our IT portfolio risk term $\Sigma\Sigma\ \sigma_i\sigma_j\tilde{\rho}_{ij}$. The remaining elements in equation (5) are the identity matrix $\boldsymbol{I}$ and the scalar $\alpha > 0$. The latter is an arbitrary ratio between the endogenous status of the nodes (projects), which is calculated based on the network (dependency) structure, and the exogenous status of the nodes, which can be arbitrarily assigned based on the vector $\boldsymbol{e}$. The parameter α can take values in the range of $0 < \alpha < \lambda_1^{-1}$, where λ_1^{-1} is the maximum value of the eigenvector of the adjacency matrix $\boldsymbol{A}$. Most researchers choose a value for α that is close to the maximum value of λ_1^{-1} (Bonacich and Lloyd, 2001) because this choice maximizes the consideration of the endogenous character, or rather, the network or dependency structure. The exogenous status represented by the vector $\boldsymbol{e}$ makes it possible to assign a value to each node in the network, independent of the actual network structure described by the adjacency matrix $\boldsymbol{A}$. Within an IT portfolio context, this exogenous status might, for instance, be the risks or the sizes of the projects. To integrate the dependency values w_{ij} or $\tilde{\rho}_{ij}$in a risk measure that is comparable to established approaches like the one of Beer et al. (2013), we in this case consider the estimated (not normalized) covariance of the IT projects (which do not account for transitive dependencies) to be the exogenous factor in the α-centrality calculation. Since we strive to derive an according IT portfolio risk term $\Sigma\Sigma\ \sigma_i\sigma_j\tilde{\rho}_{ij}$, each dependency values $w_{ij} = \tilde{\rho}_{ij}$ of the adjacency matrix $\boldsymbol{A}$ needs to be multiplied by the respective covariance $\sigma_i\sigma_j$ of a corresponding $n{\times}n$ matrix $\boldsymbol{E}$**.** Therefore, the exogenous vector $\boldsymbol{e}$ of α-centrality needs to be replaced by the described matrix $\boldsymbol{E}$ whose elements $\sigma_i\sigma_j$ represent the estimated covariance of all corresponding projects $i, j = 1 \ldots n$. This adaption makes possible a more accurate and holistic consideration of IT project dependencies. Based on this adaption, the equation for the modified α-centrality used in this paper is as follows:

$$x = (\boldsymbol{I} - \alpha * \boldsymbol{A}^T)^{-1} \circ \boldsymbol{E} \tag{6}$$

In this equation, the mathematical operator $\circ$ signifies an element-wise multiplication of the adjacency matrix $\boldsymbol{A}$, which contains the elements $\tilde{\rho}_{ij}$, and the exogenous matrix $\boldsymbol{E}$, which contains the covariances $\sigma_i \sigma_j$. The result of this multiplication is an IT portfolio risk term $\Sigma\Sigma\ \sigma_i \sigma_j \tilde{\rho}_{ij}$ that is comparable to the one introduced by Beer et al. (2013) but accounts for the specific characteristics of IT portfolio dependencies. We can thus calculate an integrated and adequately risk-adjusted IT portfolio value.

II.2.4 Evaluation

The evaluation of approaches for IT portfolio quantification is quite difficult because it is impossible to determine the “right” solution for an IT portfolio, which is based on several expert estimations and assumptions in each real-world case. Consequently, it is difficult to judge whether the result of an IT portfolio quantitation approach is right or wrong. It is rather a matter of how accurate or how plausible it seems. Since the approach of Beer et al. (2013) reflects an integrated approach of several well-established methods and approaches that themselves have often-times been evaluated and applied in practice and literature, we consider it an approved approach of suitable relevance and quality to serve as a benchmark for our evaluation purpose. To do justice to the Design Science Research principles, we evaluate our artifact regarding *quality, utility* and *efficacy* based on a comparison to the approach of Beer et al. (2013), henceforth referred to as benchmark approach. Therefore, we compute a simulation, which according to Hevner et al. (2004) is an established evaluation method in Design Science Research. We furthermore demonstrate the practicability of our artifact by providing an application example.

II.2.4.1 Simulation-based evaluation

Our evaluation procedure was as follows: For an exemplary IT portfolio, we calculated the IT portfolio value using our approach, which considers the systemic risk of IT portfolios based on their characteristic dependency structures. We also calculated the values for the exemplary IT portfolio based on the benchmark approach and compared the results of the two methods. Like previously explained, this approach reflects an integrated approach of several well-established methods and is therefore used as a benchmark for the purpose of this evaluation.

Since we were not yet able to gather real-world data for the evaluation presented below, we interviewed some experts to define approximate ranges for the input data based on their estimates. Table 1 presents an overview of the input data gained and used for the simulation.

The experts estimated values for a project's expected net present value (which is based on the discounted cash flows of the projects) and standard deviation, for small IT projects such as updates of existing applications or mobile application development projects. They furthermore estimated the risk aversion variable γ. To investigate the effects of considering different levels of network dependencies on the IT portfolio values, we chose three different values of α—low (almost ignoring the underlying IT portfolio dependencies), medium (considering half of the effect of underlying IT portfolio dependencies), and high (full consideration of the underlying IT portfolio dependencies).

We simulated three different IT project networks with three different connectivity degrees—low, medium, and high. We define the connectivity degree as the number of edges in the IT project network divided by the maximum possible number of edges. By increasing the number of edges, the connectivity of the IT project network, or rather the dependency of the IT portfolio, increases. However, it should be noted that the connectivity degree in an IT project network will never be 100%, as not all projects in an IT portfolio will be likewise dependent on each other. In our simulation, the IT portfolios consisted of 20 projects, which resulted in a maximum number of 190 ($\frac{n*(n-1)}{2}$) edges in the network. The simulated IT project networks have 20, 30, and 50 edges, which result in connectivity degrees of 11%, 16%, and 26%. For each edge between a project i and j within a specific IT project network, we use randomly generated weights $w_{ij} \in [0,1]$ to represent the strength of the underlying dependencies between projects i and j. As previously mentioned, we compared the results of our approach with the results of the benchmark approach. Therefore, as w_{ij} can be considered equivalent to the pseudo correlation values ρ_{ij} of equation (1), we used the simulated values of w_{ij} for ρ_{ij}.

As previously explained, the parameter α determines the trade-off between exogenous and endogenous factors in the α-centrality calculation. To investigate the coherence between α and the results of our approach, we simulated three different scenarios for low, medium, and high values of α. Because $0 < \alpha < \lambda_1^{-1}$, the minimum value is close to zero and the maximum value is close to the maximum eigenvector of λ_1^{-1}.

Table 1. Simulation Input Data

	Range	Distribution
Expected net present value of each project (μ)	$10{,}000 - 100{,}000$	equal
Standard deviation of each project (σ)	$0 - 10\%$ of project's net present value	equal
Parameter of risk aversion (γ)	$5 \cdot 10^{-15} - 15 \cdot 10^{-15}$	equal
Correlations (ρ) for projects = Weight of the edge (w)	$0 - 100\%$	equal
Parameter (α) for relative importance of endogenous versus exogenous factors	$0.05 * \lambda_1^{-1}, 0.5 * \lambda_1^{-1}, 0.95 * \lambda_1^{-1}$	low, medium, high
Number of projects	n	constant
Connectivity degree of the portfolio	low, medium, high	

Based on the input data summarized in Table 1, we generated 500 different IT portfolios. Table 2 presents the average results for the portfolio's value, based on the simulation for each chosen level of α and each connectivity degree.

Table 2. Average IT Portfolio's Value

Results of Φ for	IT Portfolio's Connectivity Degree		
	Low	Medium	High
Markowitz-based	1,065,436.82	1,058,239.24	1,042,966.11
$\alpha =$ low	1,079,836.90	1,079,852.78	1,079,817.76
$\alpha =$ medium	1,070,429.90	1,069,584.65	1,068,454.78
$\alpha =$ high	945,735.44	890,242.78	860,942.10

We performed the simulation several times and found that the results were reproducible. For a more convenient comparison of the results of our approach with the results of the benchmark approach, we provide the results of the evaluation in the following figures. Figure 5 presents the average results of our approach for three different values of α ($\Phi_1^*, \Phi_2^*, \Phi_3^*$). Figure 6 presents the average results of our simulation for three different IT portfolios with low, medium, and high connectivity degrees. For both figures, the vertical axis displays the risk-adjusted portfolio values derived using either the benchmark approach of Beer et al. (2013) (cf. equation (1)) or our approach (cf. equation (2)).

The results shown in Figure 5 indicate that increasing α, which implies a higher consideration of the underlying IT portfolio dependencies, leads to a lower risk-adjusted value of the IT portfolio. This shows the high impact potential of dependencies within the IT portfolio on the respective risk-adjusted portfolio value. Moreover, the results indicate that more interdependent IT portfolios are increasingly prone to systemic risk and thus have smaller risk-adjusted IT portfolio values. For low and medium values of α, the results of our approach differ from the results of the benchmark approach by between 0.5% and 3.4%. The risk of transitive dependencies seems to be comparably low for this parametrization. This, however, is quite plausible, as for low and medium values of α, the portfolio's dependence structure, represented by the weights w_{ij} of the connections, is almost neglected. In contrast, for a value of α which is close to the upper boundary λ_1^{-1}, the portfolio's dependence structure is considered to be more important, and the simulation shows significant differences between the two different IT portfolio evaluation approaches with respect to the consideration of characteristic dependency structures.

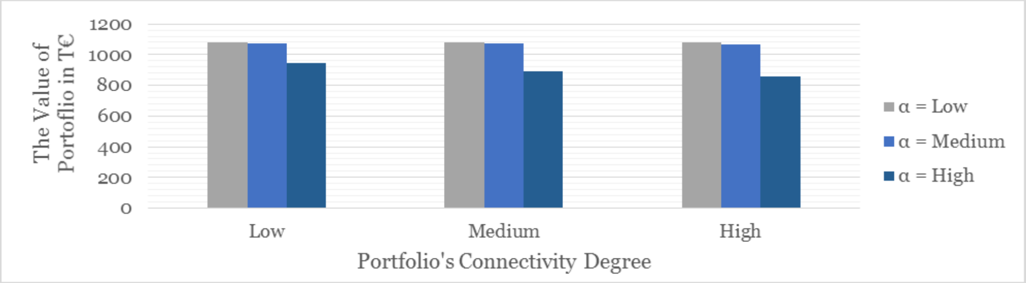


Figure 5. Evaluation of the Results

Depending on the connectivity of the specific IT portfolio, the benchmark approach leads to an overestimation of the risk-adjusted portfolio value by between approximately 11% and 17%, based on a high value of α. For connectivity degrees of 11%, 16%, and 26%, which are referred to as low, medium and high, this coherence is illustrated in Figure 6.

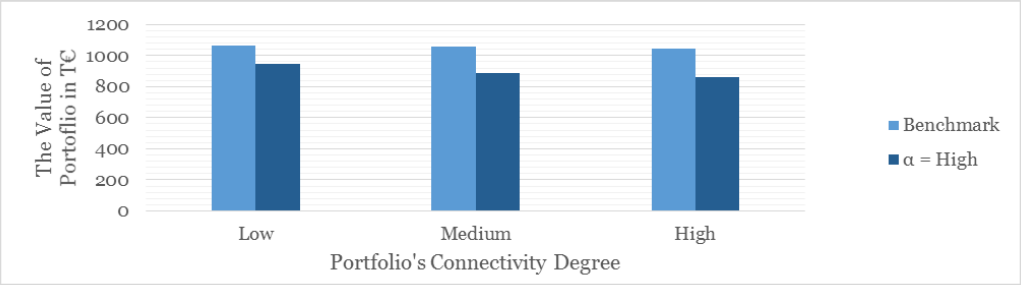


Figure 6. Evaluation of the Results

Based on our simulation results, we conclude that for IT portfolios with low degrees of connectivity, the risk-adjusted portfolio value determined using our approach and that determined using the benchmark approach are relatively similar, differing by approximately 11%. This implies that the risks of overestimation and underestimation in IT portfolios with lower connectivity degrees are comparably low. For IT portfolios with moderate (16%) degrees of connectivity, the difference is approximately 16%, and for portfolios with high (26%) degrees of connectivity, the difference is approximately 18%. We conclude that the probability of underestimating or overestimating the risk-adjusted IT portfolio value increases with the number and strength of directly and indirectly dependent projects in an IT portfolio.

II.2.4.2 Application example

The following example illustrates the applicability of our approach using data that has been shown to be obtainable in practice by Beer et al. (2013). We consider the exemplary IT portfolio shown in Figure 4 and calculate the IT portfolio's values using our method and the one of Beer et al. (2013) to illustrate the effects of integrating different types of dependencies and modeling IT portfolios from a network perspective. We defined the range of the IT project's expected values to be 266,700 € to 626,700 €, the standard deviations to be 20%, and the value of risk aversion γ to be 0.000031, based on the parameters given by Beer et al. (2013). Since we examined the exemplary IT portfolio of Figure 4, we generated random values for the weights (w) of the edges according to the ranges given in Table 1. However, as it has been shown by Beer et al. (2013), such weights representing the strength of dependencies between two projects of the IT portfolio can easily be determined based on expert estimations. We used the same input parameters for both methods. The results for the parameters of equations (1) and (2) are as follows: $\sum_i \mu_i$ is 3,060,759.70, $\gamma \cdot \sum_i \sigma_i^2$ is 461,647.02, $\gamma \cdot \sum_i \sum_{j \neq i} \sigma_i \sigma_j \rho_{ij}$ is 189,480.40, and $\gamma \cdot \sum_i \sum_{j \neq i} \sigma_i \sigma_j \tilde{\rho}_{ij}$ for low, medium, and high α values are 11,052.68, 201,348.68, and 3,870,817.02. The IT portfolio values obtained using Beer et al. (2013) and our method for low, medium, and high α values are as follows: 2,409,632.28 €, 2,588,060.00 €, 2,397,763.99 €, and

-1,271,704.34 €. The result of this application example indicates similar conclusions like the results of the simulation. In comparison to Beer et al. (2013), our approach leads to higher project values for low α values, since in this case almost all dependencies and corresponding risks of the IT portfolio are neglected. However, the results also show that in cases of high α values (as in our simulated example with the maximum α), our approach, in comparison, provides lower IT portfolio values that might even be negative due to the inherent risk of direct and indirect dependencies. Such values indicate IT portfolios that can cause financial losses for an organization. Such potential losses would probably be overlooked by the application of methods that do not appropriately consider the dependence structure of an IT portfolio.

II.2.5 Conclusion, Limitations, and Outlook

Our novel approach integrates various types of direct and indirect (transitive) dependencies between IT projects and thus enables holistic, quantitative, value-based IT portfolio evaluation in a feasible way. By considering IT portfolios as IT project networks and using α-centrality to investigate and evaluate underlying dependency structures, we addressed the major challenge stated by Benaroch and Kauffmann (1999) and adapted a model from another academic discipline to IS research. We combined α-centrality with an established and thoroughly evaluated, integrated approach for IT project and portfolio evaluation provided by Beer et al. (2013) to derive a comprehensive approach to value-based IT portfolio evaluation that appropriately considers risks emerging from characteristic dependency structures, as well as the costs and benefits of IT portfolios. This approach was developed and evaluated in line with Design Science Research principles. By means of simulation, we examined the quality and efficacy of our approach and compared it to the approach of Beer et al. (2013), which is based on the well-established methods from decision theory. The results of our simulation indicate that for low connectivity of the IT project network, which reflects a low number of dependencies in the corresponding IT portfolio, the results of our approach are comparable with the result of the one of Beer et al. (2013). This confirms the validity of the results of our approach. For IT portfolios with a high number of dependencies, our approach yields different results than the other approach of Beer et al. (2013) that is based on Markowitz's portfolio theory. This, however, seems quite plausible because the Markowitz-based approach does not consider systemic risks associated with transitive dependencies and consequently overestimates the overall IT portfolio value. We moreover illustrated an application example for further evaluate and demonstrate the feasibility and utility of the approach.

Nevertheless, our approach has some limitations. Because it is a deductive mathematical approach, we had to make a few simplifying assumptions and apply some constraints that are not entirely realistic. For instance, we defined an IT project as being assigned to one specific period in time. In reality, there may be IT projects which, even if subdivided into smaller subprojects, have to be assigned to more than one period of time. Our assumption of normally distributed cash flows might also be unrealistic in some cases, but it is a common assumption in IT portfolio management (cf. Fridgen and Müller 2011; Fridgen et al. 2015; Wehrmann and Zimmermann 2005; Wehrmann et al. 2006; Zimmermann et al. 2008). However, the more cash flows are considered within the evaluation of an IT portfolio, the better the central limit theorem and variations thereof apply, which supports the normal distribution assumption. Another assumption of our approach is that the coherence between the duration of an IT project and its assigned assets is linear. Although this assumption might not be realistic for each type of asset, it seems plausible for at least the most important intra-temporal dependencies, and we considered it to be appropriate for this first step towards an integrated value-based IT portfolio evaluation. Finally, the validity and contribution of our approach has only been demonstrated by means of simulation. For further evaluation and improvement of the method, it should be applied to real-world scenarios. This will be addressed in future research. Moreover, future research should investigate whether the integration of different risk measures can yield even more plausible results regarding the consideration of risk associated with direct and indirect dependencies or whether the existing limitations can be reduced. Furthermore, an extension of the integrated ex ante evaluation of IT portfolios to integrated ex nunc (continual) IT portfolio control and management may be of interest in holistic IT portfolio management.

II.2.6 References

Aaker, D., and Tyebjee, T.T. 1978. “A Model for the Selection of Interdependent R&D Projects,” IEEE Transactions of Engineering Management (25:2), May, pp. 30-36.

Arrow,K.J.:TheTheoryofRiskAversion.In:Arrow,K.J.(eds.)EssaysintheTheoryof Risk-Bearing, pp. 90-120. Markham, Chicago (1971)

Bardhan, I., Bagchi, S., and Sougstad, R. 2004. “Prioritizing a Portfolio of Information Technology Investment Projects,” Journal of Management Information Systems (21:2), Fall, pp. 33-60.

Beer, M., Fridgen, G., Müller, H., and Wolf, T. 2013. “Benefits Quantification in IT Projects,” in Proceedings of the 11th Conference on Wirtschaftsinformatik, R. Alt, and B. Franczyk (eds.), Leipzig, Germany, February–March 2013, pp. 707-720.

Benaroch, M., Kauffman, R.J. 1999. “A Case for Using Real Options Pricing Analysis to Evaluate Information Technology Project Investments,” Information Systems Research (10:1), March, pp. 70-86.

Bernoulli, D. 1738. “Specimen theoriae novae de mensura sortis,” Commentarii Academiae Scientarum Imperialis Petropolitanae (5:-), pp. 175-192.

Bernoulli, D. 1954. “Exposition of a New Theory on the Measurement of Risk,” Econometrica (22:1), January, pp. 23-36.

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

Buchholz, S., and Roth, T. 1987. Creating the High Performance Team, New York, USA, John Wiley & Sons.

Butler, S., Chalasani, P., Jha, S., Raz, O., and Shaw, M. 1999. “The Potential of Portfolio Analysis in Guiding Software Decisions,” in Proceedings of the First Workshop on Economics-Driven Software Engineering Research, IEEE Computer Society, May 1999, pp. 1-5.

CA Research. 2008. “Over Budget IT Projects Costing UK Plc £256m per Year”, http://www.ca.com/gb/press/Release.aspx?CID=155480 (Accessed: 28.11.2008).

Carazo, A.F., Gomez, T., Molina, J., Hernandez-Diaz, A.G., and Guerrero, F.M. 2010. “Solving a Comprehensive Model for Multiobjective Project Portfolio Selection,” Computing & Operations Research (37:4), April, pp. 630-639.

Carraway, R.L., and Schmidt, R.L.1991. “An Improved Discrete Dynamic Programming Algorithm for Allocating Resources among Interdependent Projects,” Management Science (37:9), September, pp. 1195-1200.

Cho, K.-T., and Kwon, C.-S. 2004. “Hierarchies with Dependence of Technological Alternatives: A Cross-Impact Hierarchy Process,” European Journal of Operations Research (156:2), July, pp. 420-432.

Cho, W., Shaw, M.J. 2009. “Does IT Synergy Matter in IT Portfolio Selection?” Proceedings of the 30th International Conference on Information Systems, Phoenix, AZ, USA, December 2009, Paper 160.

De Maio, A., Verganti, R., and Corso, M. 1994. “A Multi-Project Management Framework for new Product Development,” European Journal of Operations Research (78:2), October, pp. 178-191.

Diepold, D., Ullrich, C., Wehrmann, A., and Zimmermann, S. 2009. “A real options approach for valuating intertemporal interdependencies within a value-based IT portfolio management –a risk-return perspective,” in Proceedings of the European Conference on Information Systems, Verona, Italy, June 2009, Paper 10.

Doerner, K.F., Gutjahr, W.J., Hartl, R.F., Strauss, C., and Stummer,C. 2006. “Pareto Ant Colony Optimization with ILP Preprocessing in Multiobjective Project Portfolio Selection,” European Journal of Operations Research (171:3), June, pp. 830-841.

Dos Santos, B.L. 1991. “Justifying Investments in New Information Technology,” Journal of Management Information Systems (7:4), Spring, pp.71–89.

Eilat, H., Golany, B., and Shtub. A. 2006. “Constructing and Evaluating Balanced Portfolios of R&D Projects with Interactions: A DEA Based Methodology,” European Journal of Operations Research (172:3), August, pp. 1018-1039.

Emery, D.R., Parr, P.C., Mokkelbost, P.B., Gandhi, D., and Saunders, A. 1978. “An Investigation of Real Investment Decision Making with the Options Pricing Model,” Journal of Business Finance & Accounting (5:4), December, pp. 363-36.

Flyvbjerg, B., and Budzier, A. 2011. “Why Your IT Project May Be Riskier Than You Think,” Harvard Business Review (89:9), September, pp. 23-25.

Fridgen, G., and Mueller, H. 2011. "An Approach for Portfolio Selection in Multi-Vendor IT Outsourcing," in Proceedings of the International Conference on Information Systems, Shanghai, China, December 2011, Paper 8.

Fridgen, G., Klier, J., Beer, M., and Wolf, T. 2015. "Improving Business Value Assurance in Large-Scale IT Projects—A Quantitative Method Based on Founded Requirements Assessment," ACM Transactions on Management Information Systems (5:3), January, Paper 12.

Fridgen, G., and Zare Garizy, T. 2015. "Supply Chain Network Risk Analysis - A Privacy Preserving Approach," in Proceedings of the European Conference on Information Systems, Münster, Germany, May 2015, Paper 49.

Fogelström, N., Numminen, E., and Barney, S. 2010. “Using portfolio theory to support requirements selection decisions,” in Proceedings of the Fourth International Workshop on Software Product Management, Sydney, NSW, September 2010, pp 49-52.

Fox, G.E, Baker, N.R., and Bryant, J.L. 1984. “Economic Models for R and D Project Selection in the Presence of Project Interactions,” Management Science (30:7), July, pp. 890-902.

Gartner. 2013. http://www.gartner.com/newsroom/id/2292815 (Accessed 01.05.2014).

Gartner. 2014. http://www.gartner.com/newsroom/id/2643919 (Accessed 01.05.2014).

Gear, T.E., and Cowie, G.C. 1980. “A Note on Modeling Project Interdependencies in Research and Development,” Decision Science (11:4), June, pp. 738-748.

Graves, S.B., Ringuest, J.L., and Medaglia, A.L. 2003. Models and Methods for Project Selection: Concepts from Management Science, Finance and Information Technology, Boston, USA, Kluwer Academic Publishers.

Gregor, S., and Hevner, A.R. 2013. “Positioning and Presenting Design Science Research for Maximum Impact,” MIS Quarterly (37:2), June, pp. 337-355.

Häckel, B., Hänsch, F. 2014. “Managing an IT Portfolio on a Synchronized Level or: The Costs of Partly Synchronized Investment Valuation,” Journal of Decision Systems (23:4), October, pp. 388-412.

Hanink, D. M. 1985. “A Mean-Variance Model of MNF Location Strategy,” Journal of International Business Studies (16:1), Spring, pp. 165-170.

Hevner, A.R., March, S.T., Park, J., and Ram, S. 2004. “Design Science in Information Systems Research,” MIS Quarterly (28:1), March, pp. 75-106.

Kim, Y., T.Y. Choi, T. Yan, and K. Dooley 2011. “Structural investigation of supply networks: A social network analysis approach,” Journal of Operations Management (29:3), March, pp. 194-211.

Klapka, J., and Pinos, P. 2002. “Decision Support System for Multicriterial R&D and Information Systems Projects Selection,” European Journal of Operations Research (140:2), July, pp. 434-446.

Kumar, R.L. 1996. “A Note on Project Risk and Option Values of Investments in Information Technologies,” Journal of Management Information Systems (13:1), Summer, pp. 187–193.

Kundisch, D., and Meier, C. 2011. “A New Perspective on Resource Interactions in IT/IS Project Portfolio Selection,” in Proceedings of the 19th European Conference on Information Systems, Helsinki, Finland, June 2011, Paper 174.

Lee, J.W., and Kim, S.H. 2001. “An integrated approach for interdependent information system project selection,” International Journal of Project Management (19:2), February, pp. 111-118.

Linhart, A., Manderscheid, J., and Röglinger, M. 2015. “Roadmap to flexible Service Processes – A Project Portfolio Selection and Scheduling Approach,” to be presented at the 23rd European Conference on Information Systems, Muenster, Germany, May 2015.

Liesiö, J., Mild, P., and Salo, A. 2008. “Robust Portfolio Modeling with Incomplete Cost Information and Project Interdependencies,” European Journal of Operations Research (190:3), November, pp. 679-695.

Maheswari, J.U., and Varghese, K. 2005. “Project Scheduling using Dependency Structure Matrix,” International Journal of Project Management (23:3), April, pp.223-230.

Markowitz, H. 1952. "Portfolio selection," The Journal of Finance (1:7), March, pp. 77-91.

Mieritz, L. 2012. http://my.gartner.com/portal/server.pt?open=512&objID=202&&PageID=5553&mode=2&in_hi_userid=2&cached=true&resId=2034616&ref=AnalystProfile (Accessed 01.05.2014).

Medaglia, A.L., Graves, S.B., and Ringuest, J.L. 2007. “A Multiobjective Evolutionary Approach for Linearly Constrained Project Selection under Uncertainty,” European Journal of Operations Research (179:3), June, pp. 869-894.

Müller, M.P., Meier, C., Kundisch, D., and Zimmermann, S. 2015. “Interactions in IS Portfolio Selection – Status Quo and Perspectives,” in Proceedings of the 12th Conference on Wirtschaftsinformatik, Osnabrück, Germany, March 2015, pp. 737-751.

Nelson, C.A. 1986. “A Scoring Model for Flexible Manufacturing Systems Project Selection,” European Journal of Operations Research (24:3), March, pp. 346-359.

Newman, M. 2010. Networks: an introduction, New York, USA: Oxford University Press, Inc.

Nguyen, B., and Mutum, D.S. 2012. “A Review of Customer Relationship Management: Successes, Advances, Pitfalls and Futures,” Business Process Management Journal (18:3), pp. 400-419.

Ott, H. J. 1993. „Wirtschaftlichkeitsanalyse von EDV-Investitionen mit dem WARS-Modell am Beispiel der Einführung von CASE,“ WIRTSCHAFTSINFORMATIK (35:6), pp. 522-531.

Panayi, S., and Trigeorgis, L. 1998. “Multi-Stage Real Options: The Case of Information Technology Infrastructure and International Bank Expansion,” The Quarterly Revision of Economic Finance (38:3), pp. 675-692.

Project Management Institute. 2009. A Guide to Project Management Body of Knowledge (PMBOK® GUIDE), Pennsylvania, USA, Project Management Institute.

Radar Group. 2012. “White Paper: The Impact of Data Silos in IT Planning”.

Sautner, Z., Weber, M., Glaser, M.: What determines how top managers value their stock options?. (2007)

Santhanam, R., and Kyparisis, G.J. 1996. “A Decision Model for Interdependent Information System Project Selection,” European Journal of Operations Research (89:2), March, pp. 380-399.

Schumann, M. 1993. „Wirtschaftlichkeitsbeurteilung für IV-Systeme,“ WIRTSCHAFTSINFORMATIK (35:2), pp. 167-178.

Schwartz, E.S., and Zozaya-Gorostiza, C. 2003. ”Investment under Uncertainty in Information Technology: Acquisition and Development Projects,” Management Science (49:1), January, pp. 57-70.

Simon, D., and Fischbach, K. 2013. “IT landscape management using network analysis,” in *CONFENIS 2012, Ghent, Belgium, Poels, G. (ed), Enterprise information systems of the future, Lecture Notes in Business Information Processing (139), Berlin: Springer,* pp. 18-34.

Stummer, C., and Heidenberger, K. 1998. “Interactive R&D Portfolio Analysis with Project Interdependencies and Time Profiles of Multiple Objectives,” IEEE Transactions of Engineering Management (50:-), May, pp. 175- 183.

Taudes, A. 1998. “Software Growth Options,” Journal of Management Information Systems (15:1), Summer, pp. 165–185.

Taudes, A., Feurstein, M., and Mild, A. 2000. “Options Analysis of Software Platform Decisions: A Case Study,” MIS Quarterly (24:2), June, pp. 227–243.

Tillquist, J., King, J.L., and Woo, C. 2002 “A Representational Scheme for Analyzing Information Technology and Organizational Dependency,” MIS Quarterly (26:2), June, pp. 91-118.

Ullrich, C. 2013. “Valuation of IT Investments Using Real Options Theory,” Business & Information Systems Engineering (5:5), October, pp. 331-341.

Van Grembergen, W., and De Haes, S. 2005. “Measuring and improving IT governance through the balanced scorecard,” Information Systems Control Journal (2:-), pp. 35-42.

Verhoef, C. 2002. “Quantitative IT portfolio management,” Science of Computer Programming (45:1), October, pp. 1-96.

von Neumann, J., and Morgenstern, O. 1947. The Theory of Games and Economic Behavior, Princeton, USA: Princeton University Press.

Walter, S. G., and Spitta, T. 2004. “Approaches to the Ex-ante Evaluation of Investments into Information Systems,” WIRTSCHAFTSINFORMATIK (46:3), June, pp. 171-180.

Wasserman, S., and K. Faust 1994. Social network analysis: Methods and applications, New York, USA: Cambridge University Press.

Wehrmann, A., Heinrich, B., and Seifert, F. 2006. “Quantitatives IT-Portfoliomanagement: Risiken von IT-Investitionen wertorientiert steuern,“ WIRTSCHAFTSINFORMATIK (48:4), August, pp. 234-245.

Wehrmann, A., and Zimmermann, S. 2005. "Integrierte Ex-ante-Rendite-/Risikobewertung von IT-Investitionen," Business & Information Systems Engineering (47:4), August, pp. 247-257.

Weingartner, H. 1996. “Capital Budgeting of interrelated Projects: Survey and Synthesis,” Management Science (12:7), March, pp. 485-516.

Wolf, T. 2015. "Assessing the Criticality of IT Projects in a Portfolio Context using Centrality Measures," in Proceedings of the 12th Conference on Wirtschaftsinformatik, Osnabrück, Germany, March 2015, pp. 706-721.

Zangemeister, C. 1976. Nutzwertanalyse in der Systemtechnik: Eine Methodik zur multidimensionalen Bewertung und Auswahl von Projektalternativen, Winnemark, Germany, Wittmannsche Buchhandlung.

Zimmermann, S. 2008. “IT Portfoliomanagement – Ein Konzept zur Bewertung und Gestaltung von IT,“ Informatik Spekturm (31:5), October, pp. 460-468.

Zimmermann, S., Katzmarzik, A., Kundisch, D. 2008. “IT Sourcing Portfolio Management for IT Service Providers -A Risk/Cost Perspective,” in Proceedings of 29th International Conference on Information Systems, Paris, France, December, Paper 133.

Zimmermann, S., Heinrich, B., Kundisch, D. 2012. „IT Projektportfolios mit Abhängigkeiten gestalten,“ in Projektportfoliomanagement in der IT. Priorisierung, Investition, Steuerung, in Lang, M.; Kammerer, S.; Amberg, M. (eds.), Düsseldorf, Germany, Symposion, pp. 123-151.

Zuluaga, A., Sefair, J.A., and Medaglia, A.L 2007. “Model for the Selection and Scheduling of Interdependent Projects,” in IEEE Systems and Information Engineering Design Symposium, Charlottesville, VA, USA, April 2007, pp. 1-7.

III Systemic Risk in Supply Chain Networks: IT as a Chance

This chapter includes only one paper: “Systemic Risk in Supply Chain Networks – A Privacy Preserving Approach for Collaborative Analysis”, as described below.

III.1 Systemic Risk in Supply Chain Networks – A Privacy Preserving Approach for Collaborative Analysis[1]

Authors:	Tirazheh Zare Garizy, Gilbert Fridgen, Lars Wederhake

Abstract

Globalization, and outsourcing are two main factors which are leading to higher complexity of supply chain networks. Due to the strategic importance of having a sustainable network it is necessary to have an enhanced supply chain network risk management. In a supply chain network many firms depend directly or indirectly on a specific supplier. In this regard, unknown risks of network’s structure can endanger the whole supply chain network’s robustness. In spite of the importance of risk identification of supply chain network, companies are not willing to exchange the structural information of their network. Firms are concerned about risking their strategic positioning or established connections in the network. Combining the secure multiparty computation cryptography methods with risk identification algorithms driven from social network analysis, is the solution of this paper for this challenge. With this combination we enable structural risk identification of supply chain networks without endangering companies’ competitive advantage.

Keywords: Supply Chain Network, Systemic Risk, Risk Management, Multiparty Computation, Algorithms, Privacy.

[1] This research was (in part) carried out in the context of the Project Group Business and Information Systems Engineering of the Fraunhofer Institute for Applied Information Technology FIT.
Grateful acknowledgement is due to the DFG (German Research Foundation) for their grant “ITPM (FR 2987/2-1, BU 809/13-1)” making this paper possible.

III.1.1 Introduction

In March 2000, a thunderstorm in New Mexico caused a 400-million-dollar loss for the telecommunications equipment company Ericsson. The fire in a semiconductor plant, a single source key components provider for Ericsson, led to this damage. This loss could have been lower with an appropriate risk management within the supply chain network (SCN) of Ericsson (Peck 2003).

High complexity of SCNs and steady increase in vulnerability within the SCN are the results of globalization, digitalization, outsourcing and customer or supplier dependencies (Wagner and Neshat 2012). The complex structures of SCNs are vulnerable to systemic risk at all scales. Systemic risk is not just the risk of statistically independent failure, but also the risk of failure cascading within the whole interconnected system (Helbing 2013). This cascading effect impacts the whole system's performance and can lead to irrecoverable value disruptions (Acemoglu et al. 2015; Ellinas et al. 2016). 54% of companies are either extremely or very concerned about their sustainability performance (HBR Advisory Council 2010). Being one of the four emerging issues in global risk (World Economic Forum 2008,), it is inevitable to invest in risk management for supply chains. Managers and public policy makers need to identify risks to perform proper risk management and mitigation plans.

Simulation models (Fridgen et al. 2014; Giannakis and Louis 2011; Chu et al. 2010), descriptive case studies (Blome and Schoenherr 2011; Choi and Hong 2002), and development of taxonomies of SCNs (Wilding et al. 2012; Zhao et al. 2011) are common research results of the scholars on analysis of SCNs. The embedded positioning of firms within the SCN is important for each firm in the network as well as for the network as a whole. Innovation adoption, influence power or brokering activities of the firms can be derived from their structural positioning in the SCN. Moreover the structural positioning of the firms can affect the vulnerability or robustness of the SCN (Kim et al. 2011). Over the last few decades, the importance of adopting a network perspective in supply chain analysis and management has increased. Recently, the idea of adopting network measures for the investigation of SCNs is opening new potentials to evaluate supply chains (Vereecke et al. 2006, 2006; Mizgier et al. 2013).

There are several measures to quantitatively characterize the network structure. Each measure can be adopted to capture a specific feature of the network (Newman 2013). Betweenness, closeness, and degree centrality are some of the widely used measures in social network analysis (Freeman 1977; Wasserman and Faust 2009). Kim et al. (2011) mapped these measures within the SCN and defined their implication for two types of supply networks: material flows and contractual relationships. They identified that firms with higher betweenness centrality (BC) have a higher impact on the product quality, coordination cost, and lead time or can cause unwanted intervene or control among the SCN. These risky firms have a higher contribution to systemic risk. The BC is an indicator for identifying firms with the possibility of influencing information processing, strategic alignments, and perverting risk management within the supply network (Kim et al. 2011). Based on Hallikas et al. (2004) the risks in a SCN can affect the long-term sustainable competitive advantage of the network. Considering our focus and above mentioned findings, we assume the BC to be an appropriate measure to identify risky firms in the SCN.

One of the main challenges in studying supply chain risks is the scarcity of real life data on SCNs (Kersten et al. 2008; Kim et al. 2011). The fear of risking competitors' advantage by information sharing hinders companies' collaboration within the SCN. To calculate the BC, either based on definition (Freeman 1977; Newman 2013), or by means of widely used algorithms such as Brandes' (2001), having information about the network's structure is necessary. This structural information contains data on the network's firms and their possible connectivity to other firms. However, the strategic importance of the firms' position and connections within the network (Hochberg et al. 2007) dissuades firms from sharing this information. In this case, the application of secure multiparty computation (SMC) cryptographic algorithms (Yao 1986; Goldreich et al. 1987) would be one of the solutions to facilitate information sharing willingness within the network. SMC algorithms are based on simultaneous exchanges of encrypted data among parties. The result is calculated from the encrypted data, and is shared among all firms (parties) in the network. The algorithm prevents leakage of key information between the firms.

Given the importance of risk analysis in SCNs and the adequacy of the BC to identify the bottlenecks in SCNs. The main focus of this paper is to introduce an artifact – based on the design science paradigm – for privacy preserving calculation of the BC of a given SCN. This paper is an extended version of our prior research (Fridgen and Zare Garizy 2015), and includes detailed information on the developed artifact, pseudocode of the artifact, and a detailed description of the artifact's code. Our artifact consists of four main methods that are calculating the desired result. The main contributions of our paper are:

- Identification of risks: In the first step of risk management it is necessary to develop models and methods for risk identification in SCNs. In a small SCN, companies are more likely to keep the overview of the SCN topology and the companies in the network. Consequently, in such cases risks are relatively transparent and privacy is not the subject of interest. Our concern is the risk identification in large SCNs consisting of hundreds of inter-connected companies. In a large SCN, on the one hand the identification of unknown risks is important and on the other hand the privacy of members should be maintained. For an increasing size of the SCN and the inter-relationships among the firms, the network becomes more complex (Choi and Krause 2006; Lessard 2013). Due to the higher complexity the probability of unseen risks and the necessity of proper risk analysis increases. In the artifact proposed, we study the economic dependency (e.g. material or financial flow) between firms by means of BC calculation for the identification of risky firms in SCNs. We thereby assume that our artifact could be a module of standard ERP systems that use existing communication links to suppliers and customers.

- Preservation of Privacy: One of the main concerns of companies in a SCN is their strategic position in the network, so they avoid to risk their competitive advantage in order to identify their own risks. Our artifact keeps the network's structure mostly unknown to the firms within the network. The artifact prevents data leakage or reconstruction of information to ensure the firms' willingness for information sharing. In order to meet this objective, we base our approach on SMC algorithms in a semi-honest environment as outlined in the latter. Our modeling focus is on providing a privacy preserving artifact, whereas we omit the analysis and improvement of computational complexity.

Considering the guidelines of Hevner et al. (2004) and Gregor and Hevner (2013) for the conduction of design science research, the remainder of this papers is organized as follows: The first section covers a brief review on essential literature. It also includes specifying the problem's context and the relevance of the problem for SCNs. Subsequently, we discuss the modeling procedure and requirements that must be met for solving the problem. The fourth section illustrates the developed artifact. The section is followed by the evaluation of the artifact by means of testing and descriptive methods. The paper ends with a summary and an outlook on further research.

III.1.2 Literature Review

III.1.2.1 Supply Chain Networks

"Supply chains are interlinked networks of suppliers, manufacturers, distributors and customers that provide a product or service to customers" (Blackhurst et al. 2004). Current trends, like ecommerce, e-logistics, and e-business, increase the complexity of supply chains. Furthermore, the importance of staying competitive in the market gives supply chain management a higher importance (Arns et al. 2002). The SCN in a global economy consists of a large number of interdependent networks. This interdependency is very susceptible to external effects and defaults (Buhl and Penzel 2010). The risk type in SCNs can be specific disruption, general disruption, cost shock (e.g. exchange rates), product safety, commoditization, and shift in tastes (Lessard 2013). Weather, terrorism, firms manufacturing failures, or financial crises can cause a default in the supply chain (Babich et al. 2007). Risks in SCNs can lead to various types of losses such as financial loss, performance loss, physical loss, psychological loss, social loss and time loss (Yates and Stone 1992). Since the disruptions in SCN in extreme cases may lead to the bankruptcy of the SCN's firms, it is important for the firms to manage these risks and minimize the possible losses. A study of Gyorey et al. (2011) states that 67% of companies are not ready for geopolitical instability challenges. In the management of SCNs, one of the main tasks is risk management. The risk management process consists of risk identification and assessment, decision and implementation of risk management actions, and risk monitoring (Hallikas et al. 2004). Bellamy and Basole (2013) classified the themes in SCNs analysis as system architecture (network structure), system behavior, and system policy and control. Among these categories, system architecture analysis methods focus on structural investigation of SCNs, relationship of firms, and the importance of the relationship. Considering social networks, structural investigations based on network analysis methods are well-established. In the field of SCNs they are relatively new but evolving (Li and Choi 2009; Kim et al. 2011; Mizgier et al. 2013). These methods focus on network components' connections and patterns, and implication of these connections for the whole network (Wasserman and Faust 2009; Newman 2013). Among various measures on structural analysis of SCN, as it has been mentioned earlier, the BC can be a suitable indicator to identify the structural risks of a SCN (Kim et al. 2011) and it is our choice in this paper.

III.1.2.2 Privacy Concerns in Supply Chain Networks

On the one hand knowing the structure of a network is a prerequisite of calculating the BC (as outlined earlier) and on the other hand in a SCN, the competitive advantage of network firms is relying on the privacy of their contacts and network relations they have (Buhl and Penzel 2010). Solutions to these data privacy concerns of companies can be:

- A Trusted Third Party: If the firms trust a third party, it is easy to solve the problem by sharing their information with this trusted third party and letting it calculate the results. For instance, Brandes' algorithm for the BC (2001), works based on the idea of having a third party who collects the information and calculates the indices and returns the result. In practice such a party that all network's firms trust might be difficult to find and firms might have concerns about this third party revealing the information.

- SMC Algorithms: These cryptography algorithms enable different firms in the network to share their information privately and calculate the result jointly. The main advantage of these algorithms is that the individual's input stays mostly private.

SMC first was addressed by Yao (1982). Yao's (1982) algorithm is answering the question of SMC for two parties. This algorithm is a solution to the Millionaires' problem. The problem is that two millionaires want to know which of them is richer but they do not want to share the real amount of their wealth. Yao's (1982) algorithm provides a solution that lets them privately encrypt their input, share it, and jointly calculate the result. The main advantage is that their input stays private. SMC algorithms today enable us to do secure addition, multiplication, and comparison (Shamir 1979; Yao 1986; Sheikh et al. 2009; Cramer et al. 2013).

SMC algorithms are used in various fields of science. For instance they are used for secure auctions (Bogetoft et al. 2006). They are also used for sharing financial risk exposures (Abbe et al. 2012) with the focus on necessity of process and methods secrecy in financial industry. SMC algorithms are also applied for sustainable benchmarking in clouds without disclosing the individual's confidential information (Kerschbaum 2011).

"SecureSCM", secure collaborative supply chain management, the European research project (Kerschbaum et al. 2011), is an example of the application of SMC algorithms in the field of SCNs. The project enabled privacy preserving online collaboration among various firms in a SCN. The focus was on providing the possibility to better reaction on possible capacity concerns or short notices. The collaboration of the firms with the application of SMC algorithms results in better production planning in the SCN. However, they did not study SCN's risks and focused on cost minimization.

In this paper, SMC algorithms are our choice for the privacy preserving calculation of the result. To apply these algorithms, we develop an artifact that enables calculation of the result based on private shares of the firms. SMC algorithms have a high acceptance and are widely used in the field of cryptography since the 1980's (Dolev and Yao 1983; Beaver et al. 1990; Lindell and Pinkas 2009; Bogetoft et al. 2006; Reistad 2012). Therefore, we do not investigate the security of these algorithms and assume security is given.

III.1.2.3 Network Centrality Measures

To calculate the BC, we model the SCN as a graph $G(V, E)$. Each company v in the SCN is represented by a vertex $v \in V$. An economic dependency (e.g. material or financial flow) between companies $u, v \in V$ is represented by an edge $(u, v) \in E$ between these companies. In this case, we name u and v adjacent or neighbors. Since an economic dependency is undirected, in this paper graphs are undirected. Moreover the graphs are connected, as connected firms are forming a SCN. The BC is a centrality index based on the number of shortest paths and the frequency in which a vertex is appearing on shortest paths between two other vertices. A shortest path is a path between two vertices such that the sum of the weights of its constituent edges is minimized (as outlined in Section 3). The BC describes how other vertices potentially can influence the interaction between two non-neighboring vertices (Wasserman and Faust 2009; Newman 2013). Based on Newman (2013) the BC for vertex v is calculated as follows:

$$BC(v) = \sum_{s \neq v \neq t \in V} \frac{\sigma_{st}(v)}{\sigma_{st}} \tag{1}$$

In Equation (1), $\sigma_{st}(v) \in \mathbb{N}_0$ is the number of shortest paths between source vertex s and target vertex t, which pass through vertex v, and σ_{st} is the number of shortest paths between source vertex s and target vertex t.

The main aspect of the BC algorithms (Jacob et al. 2005; Klein 2010; Brandes 2001) is finding the shortest paths. Based on categorization of Cormen et al.'s (2001) on shortest paths algorithms we classify existing BC algorithms as follows:

- Algorithms based on single-source shortest paths: Brandes' (2001) algorithm is a widely used one among them. Brandes (2001) applies single source shortest paths algorithms (breadth-first (Moore 1959)) search for unweighted and Dijkstra's algorithm for weighted graphs (Dijkstra 1959; Cormen et al. 2001) to calculate the BC.
- Algorithms based on all-pairs shortest paths: The method developed by Edmonds et al. (2010) adopted modification of algorithms like the Floyd-Warshall (Floyd 1962; Warshall 1962; Cormen et al. 2001) to enable parallelism and space-efficiency in calculation of the BC.

Both categories of algorithms need the network topology as input and a stack to store information. For privacy concerns we strive to avoid a central stack for information. Having a central stack implies that there is a central player who owns this stack. This player can infer information, from the communication of the players via this stack or from the large amounts of available data (although the information is encrypted) in the stack. This can be a risk for privacy concerns of the firms in the SCN.

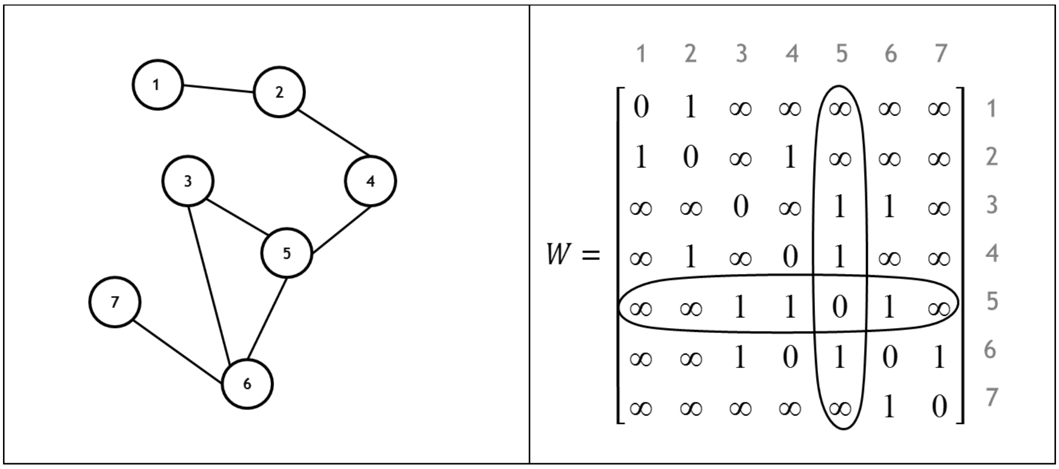
In this paper, inspired by the Floyd-Warshall (Floyd 1962; Warshall 1962; Cormen et al. 2001) algorithm as well as backtracking search (Russell and Norvig 2009) to identify shortest paths, we develop an artifact which does not need a central stack, stores information decentrally, and does not need the network's topology as input.

III.1.3 Modeling Procedure, Assumptions, and Requirements

The first part of this section focuses on modelling procedure and assumptions for our artifact. In this part before we focus on privacy concerns and information that each firm has, we define the general terms and construct of our artifact. The second part includes the more specific information on privacy preserving of the firms and requirements.

We label each company and its representing vertex with a unique number $1,2,\ldots,|V|$. The numbers are randomly assigned to each company and represent the row number for the player in the graph's weight matrix. The relation between the identity of a company and its number is only known to the company itself and to the neighborring companies. From now on, we name a company and its representing vertex as a "player" when we mean the company's row number and not the true identity of the company.

In the following, we illustrate an exemplary SCN (Figure 1). The SCN is chosen simple to make the visualization easier and the example more comprehensible. The SCN consists of 7 players. Each player is represented by its own unique number. The set of vertices (players) is: $V = \{1,2,3,4,5,6,7\}$.



$$W = \begin{array}{c} \begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \end{matrix} \\ \begin{bmatrix} 0 & 1 & \infty & \infty & \infty & \infty & \infty \\ 1 & 0 & \infty & 1 & \infty & \infty & \infty \\ \infty & \infty & 0 & \infty & 1 & 1 & \infty \\ \infty & 1 & \infty & 0 & 1 & \infty & \infty \\ \infty & \infty & 1 & 1 & 0 & 1 & \infty \\ \infty & \infty & 1 & 0 & 1 & 0 & 1 \\ \infty & \infty & \infty & \infty & \infty & 1 & 0 \end{bmatrix} \end{array} \begin{matrix} \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \end{matrix}$$

Figure 1. Exemplary network

For reasons of simplicity, the following assumptions are the basis for the development of our artifact.

Assumption 1. *The companies are semi-honest (honest-but-curious).*

Semi-honest adversaries are following the protocol, but they might try to gather information and draw conclusions from the messages they receive. Our artifact's construction preserves privacy assuming the companies are semi-honest. Moreover, related works on SMC algorithms are also based on a semi-honest model (Brickell and Shmatikov 2005; Canetti 2008; Huang et al. 2012; Schneider 2012).

Assumption 2. *The connections in the SCN are equally weighted.*

In general, our artifact is applicable for graphs with $w_{uv} \in \mathbb{R}$. However, Kim et al. (2011) did their analysis on the BC, assuming equal weight connections. Their focus is on links between firms and the number of firms that are engaged in transferring information or material. Therefore, without loss of generality, in this paper we do not focus on the determination of the intensity of connections and its analysis and we treat the connections as equally weighted and leave the topic of connections' intensity subject to further research. The weight of the edge $(u, v) \in E$ with arbitrary $u, v \in V$ is then defined by

$$w_{uv} = \begin{cases} 0 & if\ u = v, \\ 1 & if\ u \neq v\ and\ (u, v) \in E, \\ \infty & if\ u \neq v\ and\ (u, v) \notin E. \end{cases} \tag{2}$$

The $n \times n$ matrix $W = (w_{uv})$ contains all weights of edges in the graph with n nodes $\forall\, u, v \in V$ (Cormen et al. 2001). The (symmetric) matrix W in Figure 1 represents the weight matrix of our exemplary SCN.

The sequence of vertices that are forming the path from a source vertex $s \in V$ to a target vertex $t \in \mathrm{V}$ is represented by $path = \langle v_0, v_1, \ldots, v_k \rangle$. In this we assume that $v_0 = s$, $v_k = t$, and $(v_{i-1}, v_i) \in E$ for $i = 1\ to\ k$. The length of the path is the sum of the weights of its forming edges. Based on Equation (2) the weight of an edge is 1 therefore, if k vertices are forming a path, there are $k - 1$ edges on this path and $w(path) = k - 1$. We define the length of a shortest path, labeled as distance between s and t, as

$$d_{st} = \overset{path}{\min}\{w(path): v_s \rightsquigarrow v_t\} \tag{3}$$

The $n \times n$ matrix $D = (d_{st})$ contains the distances $\forall\, s, t \in V$. By our definition, if s and t are adjacent then $d_{st} = 1$. To find a shortest path from a source vertex s to the target vertex t, the existing distance and the distance of all alternative paths via intermediate vertices $\forall v \in V, v \neq s, t$ are compared (Equation (4)) and we choose the path with the minimum length.

$$\min(d_{st}, d_{sv} + d_{vt}) \tag{4}$$

In this part we represent the above mentioned figures with particular details which include privacy preserving concerns and information availability for the players.

In our artifact we restricted the information availability of the players mostly up to their neighbors. Therefore, although the set V is known to every player in the network, but the relation between the players' unique numbers and their true identities is in only known to neighboring players. Furthermore the network's structure as illustrated in the Figure 1 is not known to the players. Consequently W is unknown to the players. Each player p has access to the $p - th$ row/column (since the matrix is symmetric) of the weight matrix W. The accessible information for player 5, is the 5-th row of the matrix, as marked in the Figure 1. Moreover the distance matrix D is unknown to the players. Although, each player p has access to the p-th row of the matrix D.

For our artifact we state the following requirements:

Requirement 1. *The artifact should keep the SCN topology as private as possible.*

Requirement 1 is an extension to conditions of SMC on satisfying privacy (Cramer et al. 2013). In our case it is allowed that more information than the final result (BC) is shared. More specifically, we prohibit the sharing of the following information that can be used for reconstructing the SCN topology or interfering the real identity of the firms.

- The length of the shortest paths, to prevent firms from knowing the positioning of the players in the network.
- The number of the shortest paths between a given source and target player in the network, to prevent firms from knowing which alternatives for trading players have in the network.
- The number which shows how often a player is appearing on the shortest paths between a given source and target player, to prevent firms from knowing accessibility and connections to other firms.

Requirement 2. *The artifact should keep the identities of non-neighboring players private.*

In a large SCN, due to members' variety and multiplicity in the SCN, a company is not able to identify other companies in the network. Concluding the identity of a player via execution of the artifact can provide the possibility of reconstructing a part of the network's topology.

Therefore, the artifact should not enable a company to infer the real identity of non-neighboring companies.

III.1.4 Artifact Development

We choose an object oriented approach to design the artifact. To model the structure and behavior of the players in our artifact we model the class Player. We represent each player by an object of class Player running on a distributed system. Each player executes the methods on its own system and delivers the result. In our artifact we assume there is an initializing and synchronizing agent (ISA) (one of the SCN’s firms or an organization) who initializes, coordinates, and synchronizes the executions. The ISA does not have the possibility to access the private information of the players or monitor the communication between the players.

Figure 2 presents class Player. For reasons of simplicity, in the following we assume the players’ object references equal to their respective $rowNumber$ during the calculations. $rowNumber$ is the unique number assigned to each player in the network. $rowNumber = p$ implies the player is pointing the p-th row/column the weight matrix W.

We assume p is the number of the current object of the Player class. Table provides the description of the attributes of the Player class. Table 2 provides an overview and description of the commonly used variables in the methods. Table 3 provides the description of the methods of the Player class.

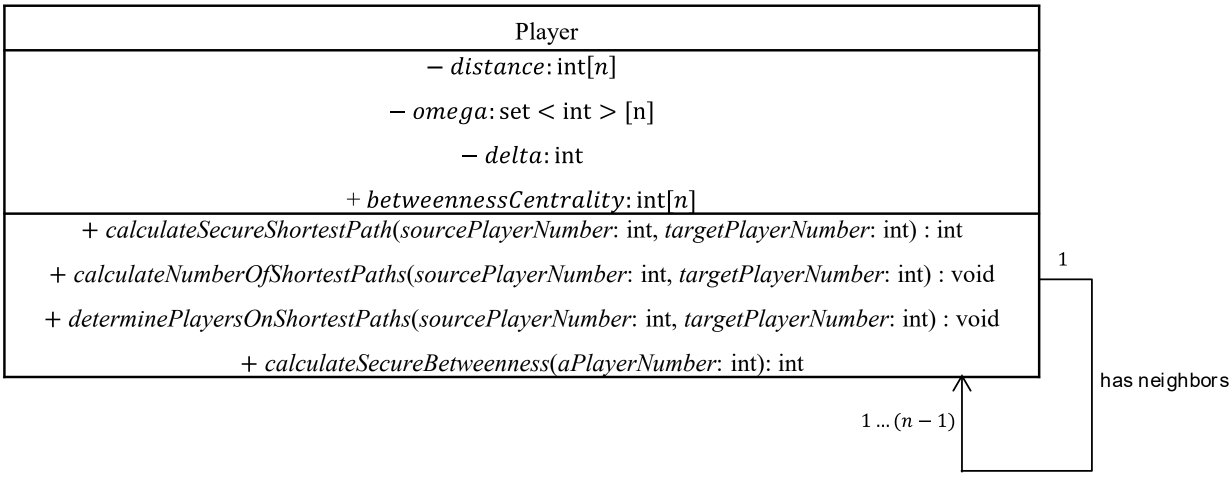

Player
− distance: int[n]
− omega: set < int > [n]
− delta: int
+ betweennessCentrality: int[n]
+ calculateSecureShortestPath(sourcePlayerNumber: int, targetPlayerNumber: int) : int
+ calculateNumberOfShortestPaths(sourcePlayerNumber: int, targetPlayerNumber: int) : void
+ determinePlayersOnShortestPaths(sourcePlayerNumber: int, targetPlayerNumber: int) : void
+ calculateSecureBetweenness(aPlayerNumber: int): int
1
has neighbors
1 ... (n − 1)

Figure 2. Visualization of the class Player in UML-oriented Notation

Table 1. Description of the attributes of the class Player

Attribute	**Mathematical Variable**	**Description**
$distance\text{: int}[n]$	$D = (d_t)$ $\forall\, t \in V$	Denotes a vector of the distances of player p to each target player t in the network. The distances are unknown at the beginning of the execution. Each member of this list is the output of the method *calculateSecureShortestPath()* for a given target player.
$omega\text{: Set} < \text{int} > [n]$	$\Omega = (\Omega_t)$ $\forall\, t \in V$	Denotes a vector which contains the set of neighboring players of player p that are connecting the player with the shortest paths to the target player t The method *calculateSecureShortestPath()* sets the values of this set.
$delta\text{: int}$	δ	Denotes a random generated number of the player. We use it to modify the distance value to preserve privacy. Each player generates δ before participating in the execution of methods. For each player, this number stays constant during the execution of the artifact. It assures an identical response of the player to all calculation requests.
$betweennessCentrality\text{: int}[n]$	$BC =$ (bc_v) $\forall\, v \in V$	Denotes a vector which is filled with the BC of all players in the network. Each member of this list is the output of the *calculateSecureBetweenness()* method for each given player v.

Attribute	Mathem-atical Variable	Description
$busy$: bool$[n][n]$	$BZ = (bz_{st})$ $\forall\, s,t \in V$	Denotes an $n \times n$ matrix of flags (true/false). This flag serves implementation purposes and especially access management of the players (as described in Table 6, Line 1-4).

Table 2. Description of the commonly used variables

Variable	Mathematical Variable	Description
$sourcePlayerNumber$: int	s	Denotes the unique number of the source player.
$targetPlayerNumber$: int	t	Denotes the unique number of the target player.
$currentPlayerNumber$: int	p	Denotes the unique number of the current instance of the class Player.
$neighboringPlayerNumber$: i	a	Denotes the unique number of a neighboring player.
$aPlayerNumber$: int	v	Denotes the unique number of a given player.

Table 3. Description of the methods of class Player

Method	Description
Name *calculateSecureShortestPath* **Input** sourcePlayerNumber: int	The method recursively identifies the shortest paths from the given source player to the given target player. It returns the encrypted value of the distance and keeps other variables local. If the target player is not the current player, the method calls itself at all neighboring players to determine their distances to the target. The method compares the delivered

Method	Description
targetPlayerNumber: int **Output** distance: int	results of the neighboring players and chooses the path via the neighboring player/s which has/have the minimum distance value. For privacy preserving purposes the comparisons in this method are based on Yao's (1982) secure comparison protocol. The method also identifies the neighboring players who are forming the shortest paths and fills the set Ω.
Name *calculateNumberOfShortestPaths* **Input** sourcePlayerNumber: int targetPlayerNumber: int **Output** void	The method recursively calculates the *number* of shortest paths between given unique numbers of source player s and given target player t via players forming the shortest paths. If t is not a neighboring player of s, the method calls itself at all neighboring players forming the shortest paths between s and t. The method determines the number of shortest paths which passes through current player p by means of the size of the set Ω_t. The method saves the results of the calculation in an intermediate storage and later uses it to participate in *calculateSecureBetweenness* method.
Name *determinePlayersOnShortestPaths* **Input** sourcePlayerNumber: int targetPlayerNumber: int **Output** void	The method recursively determines how often players are appearing on the shortest paths from source player s to target player t via current player p. If t is not a neighboring player of s, the method calls itself for all neighboring players which are forming the shortest paths between s and t. At each recursion the members of the set Ω_t determine the players which are on the shortest paths through player p. The method determines the players which are on the shortest paths through current player p by means of the members of the set Ω_t. The method saves the results of the calculation in an intermediate storage and later uses it to participate in *calculateSecureBetweenness* method.

Method	Description
Name *calculateSecureBetweenness* **Input** sourcePlayerNumber: int targetPlayerNumber: int **Output** BC(v): int	This method calculates the BC(v) for the given player in the network. It is based on SMC algorithms and requires information exchange among the players in the network. The method performs all arithmetic based on secure protocols of Cramer et al. (2013). These protocols for SMC are extension of Shamir's algorithm (1979) and providing us the possibility to calculate the BC preserving the privacy concerns. Furthermore the method applies the distributive property of binary operations to calculate the result of Equation (1). This provides us the possibility that private shares of players stay private.

For privacy preserving concerns, in methods *calculateSecureShortestPath(), calculateNumberOfShortestPaths(),* and *determinePlayersOnShortestPaths()* players only communicate via their neighboring players. Each object routes its messages through neighboring players in the network. The methods *calculateNumberOfShortestPaths*() and *determinePlayersOnShortestPaths*() calculate values of σ_{st} and $\sigma_{st}(v)$ decentrally. Each player has a portion of these values from its own perspective. We denote the portion of information which player p has by σ_{st}^{p}, and $\sigma_{st}^{p}(v)$. The final values of σ_{st} and $\sigma_{st}(v)$ are the sum of the decentrally calculated values of all players as follows.

$$\begin{aligned} \sigma_{st} &= \sum_{p \in V} \sigma_{st}^{p}, \\ \sigma_{st}(v) &= \sum_{p \in V} \sigma_{st}^{p}(v). \end{aligned} \tag{5}$$

The method *calculateSecureBetweenness*() uses the decentral values (σ_{st}^{p}, and $\sigma_{st}^{p}(v)$) to calculate the betweenness centrality, and applies SMC algorithms to preserve privacy.

Table 4 elaborates sequences of our artifact. Steps 1 to 5 and 9 in Table 4 are not in the focus of this paper and are not influencing our artifact's construction therefore, these steps are not documented in this paper. Furthermore, we provide the illustration of the methods of the artifact.

Table 4. The artifact's structure

Step	Executor	Description
Initialization		
1	ISA	Identifies the number of players, n, in the network.
2	ISA	Assigns each participating company a $rowNumber$ (without knowing the real identities of the firms).
3	ISA	Shares the number of players, n, with all players in the network and notifies the players to initialize.
4	Player	Each player initializes a new object of class Player and informs ISA.
5	ISA	Notifies all players that the players' objects exist and they are available to execute the methods.
Decentral calculation of the shortest paths and path forming players		
6	Player	Each player executes the *calculateSecureShortestPath*() method for itself as the source player and all given targets in the network.
7	Player	Each player executes the *calculateNumberOfShortestPaths*() method to decentrally set the values of σ_{st} for each given target t.
8	Player	Each player executes the *determinePlayersOnShortestPaths*() method to decentrally calculate the values of $\sigma_{st}(v)$ for itself as source player s and each given target t. By termination of the method for all given targets, the player informs ISA.
Synchronization		
9	ISA	ISA informs every player in the network that the *determinePlayersOnShortestPaths*() is terminated when it receives the notification of termination from all players. This implies that the variables to calculate the BC are available.
Calculation of the BC		
10	ISA	ISA coordinates players for execution of the *calculateSecureBetweenness*() method. With termination of the method

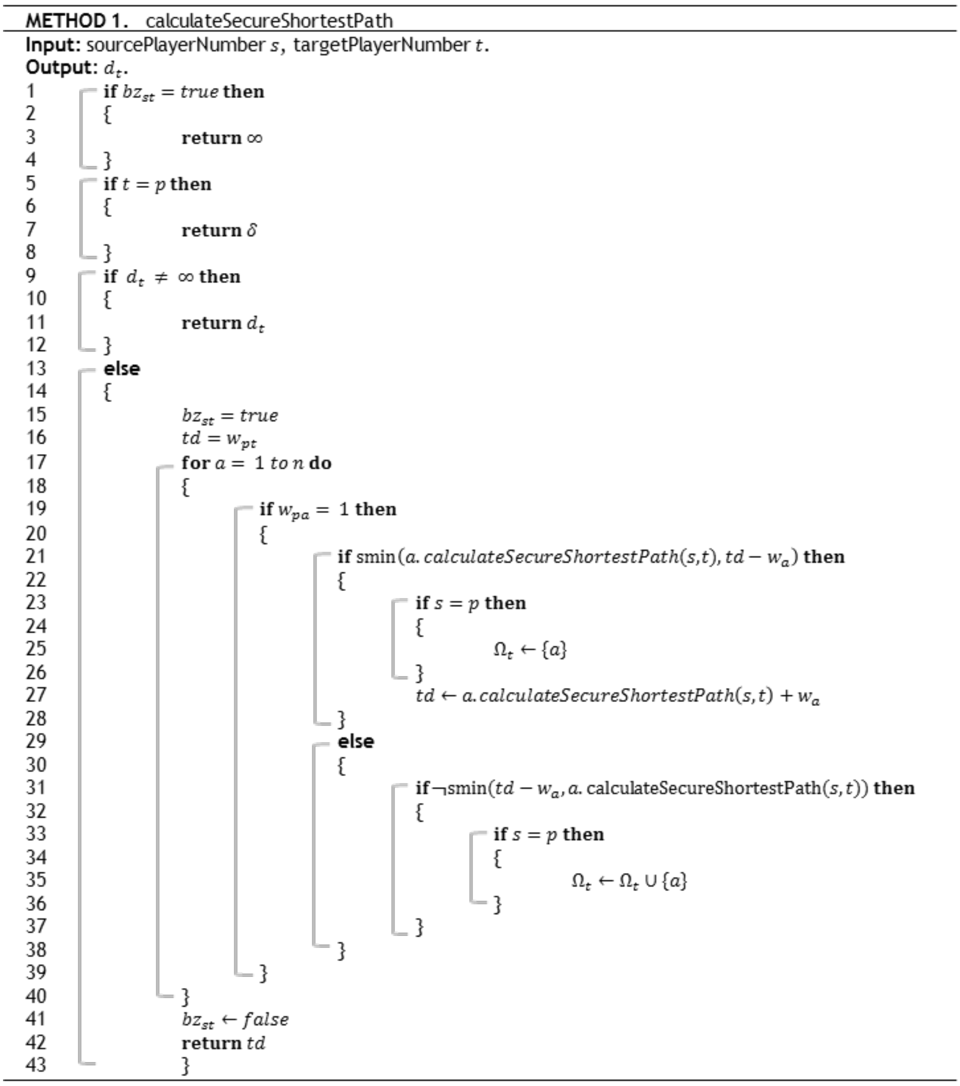
Step	Executor	Description
		for all players in the network, all firms have their own BCs as well as the BC of all players in the network.

In the following, we provide the pseudocodes and a detailed description of the methods of our artifact.

In Figure 3 we provide the pseudocode of *calculateSecureShortestPath*() method. This method requires an additional variable td for calculation purposes. Table 5 provides the description of this variable.

Table 5. Description of the variable defined for calculateSecureShortestPath() method

Variable	Mathematical Variable	Description
$temporary\ Distance$: int	td	Denotes a temporary variable saving the distances during calculation of the shortest paths. This variable ensure data consistency.



```
METHOD 1.  calculateSecureShortestPath
Input: sourcePlayerNumber $s$, targetPlayerNumber $t$.
Output: $d_t$.
if $bz_{st} = true$ then
{
        return $\infty$
}
if $t = p$ then
{
        return $\delta$
}
if $d_t \neq \infty$ then
{
        return $d_t$
}
else
{
        $bz_{st} = true$
        $td = w_{pt}$
        for $a = 1$ $to$ $n$ do
        {
                if $w_{pa} = 1$ then
                {
                        if smin$(a.calculateSecureShortestPath(s,t), td - w_a)$ then
                        {
                                if $s = p$ then
                                {
                                        $\Omega_t \leftarrow \{a\}$
                                }
                                $td \leftarrow a.calculateSecureShortestPath(s,t) + w_a$
                        }
                        else
                        {
                                if$\neg$smin$(td - w_a, a.$calculateSecureShortestPath$(s,t))$ then
                                {
                                        if $s = p$ then
                                        {
                                                $\Omega_t \leftarrow \Omega_t \cup \{a\}$
                                        }
                                }
                        }
                }
        }
        $bz_{st} \leftarrow false$
        return $td$
        }
```

Figure 3. Pseudocode of the method calculateSecureShortestPath

Table 6 provides a detailed description of the *calculateSecureShortestPath*() method.

Table 6. Description of the calculateSecureShortestPath() method

Line	**Description**
1-4	The *calculateSecureShortestPath*() is a recursive method, which sequentially routes the requests of the calculation of shortest paths via the neighboring players. Therefore, each player should not receive a duplicate request for the calculation of a specific path. However, a player may receive such a request, since the graph of the SCN is not necessarily acyclic. Once current player p routes the message of the calculation of a specific shortest path via a neighboring player, due to the possible graph cycles, after few message routings player p might receive its own message from a neighboring player causing endless loop. To avoid such conditions, the method uses a busy flag (bz_{st}). As long as player p is busy with the calculation of the shortest paths between players s and t, if it receives a message for the calculation of the same path, it implies that the message is its own message. Therefore, Line 1 identifies this message as a duplicate message. Furthermore, Line 3 prevents further calculations of the method and returns ∞. Returning ∞ ensures that the duplicate request has no influence on the result of the calculations, and the method terminates.
5-8	To calculate the BC (c.f. Equation (1)), it is important to know the number of the shortest paths between two players, and to know which players are forming the shortest paths. The *absolute numeric value of the length* of the shortest paths does not change the result of BC. Thus, for privacy preserving concerns, we can modify the *absolute numeric value* of the distances between players by adding an offset to the target players given that the number of shortest paths and their forming players remain intact. Still, we obtain the same results as without modification of the distances. In our method, each player uses its own private number $\delta \in \mathbb{N}$ (delta explained in Table 1) to modify the distance value (Line 7). Note that, this number must not be the players' unique number, because if it is so, the positioning of the players might be disclosed. Please note, since the communication is only via neighboring players, this private number is only known to the player and its neighboring players. Players use the private number δ only if they are the target player t. This assures a consistent modification of the distances to a specific target player t and the comparability of the results for the source player s.

Line	Description
	The following scenario elaborates the importance of using δ to modify the value of distance. In our exemplary network (Figure 1), if the method does not modify the value of distances, and player 6 shares 1 as its distance to players 7 ($d_{67} = 1$), player 5 (as a neighboring player of player 6) infers that players 6 and 7 are adjacent. But if the method uses a modified value of the distance (we define, δ for player 7 be 70), player 6 shares 71 as its distance to players 7 ($d_{67} = 71$). This modification hinders unwanted information sharing in terms of inferring the positioning of players in the network. To find the shortest paths, we must be able to compare the distances of the paths. Although the modified distance values (Line 7) eliminate many sorts of privacy concerns, yet there is a chance to reconstruct parts of the network structure by comparing the modified values. For instance in Figure 1 we set δ for player 7 to 70. The distance of player 3 to 7 via player 5 is $d_{37} = 73$ and the distance of player 3 to 7 via player 6 is $d_{37} =$ 72. Based on this information, player 3 reveals that players 5 and 6 are adjacent. Therefore, in addition to modifying the shortest path we apply a privacy preserving method to compare the shortest paths (See Line 17-40).
9-12	If the player already calculated the distance to target player t, then it returns this calculated value of distance. This part increases the efficiency of the method by preventing recalculation of the shortest paths, which are already calculated.
13-43	If the current player p receives a request for the calculation of a specific path for the first time and is not the target player, this part of the method (Line 17-40) recursively calculates the shortest paths between source player s and target player t. To avoid data inconsistency during the execution of various instances of the method, Line 16 sets the temporary distance variable td_{st} to w_{pt} which is the initial distance value of the current player to the target. The method does not use its distance attribute (d_t) for calculations, because the value of d_t, may change during the calculation of a specific shortest path, leading to inconsistency of the result. The following example elaborates the necessity of the temporary distance variable. We assume player 5 is executing *calculateSecureShortestPath*(1,7) and it is the first request to player 5 for calculating the path to player 7. Players 5 and 7 are not adjacent and the initial value of the distance is $d_7 = w_{57} = \infty$. In the meantime, player 5

Line	Description
	receives the request for calculation of the path from source player 2 to target player 7 ($calculateSecureShortestPath(2,7)$). If the execution of this request ends faster than $calculateSecureShortestPath(1,7)$, player 5 updates the distance to player 7 (d_7) to 72. Consequently, the value of d_7 for the player 5 varies during the execution of $calculateSecureShortestPath(1,7)$.This leads to inconsistent values of the distance for the comparisons within the execution of the method. Using td, the method prevents this sort of inconsistencies. When player p starts the calculation of the path between source player s and target player t via its neighboring players, Line 15 sets the bz_{st} to true. When player p finishes calculating the shortest paths between players s and t, Line 41 sets bz_{st} to false. It allows the player to respond to the messages which are not originating from itself. At Line 42 the method returns the value of distance (td), which is the distance of player p to the target player t (d_t).
17-40	Current player p routes the message of the calculation of the path via all neighboring players to calculate the result recursively. For this purpose Line 17 goes through each player 1 to n, where n is the number of players in the network. Furthermore, the method identifies the neighboring players and only routes the request for calculating the shortest path via them.
19-39	Player p identifies its neighboring players at Line 19. For this purpose it considers a given player a as a neighboring player when the distance of the current player to the player is equal to one ($w_{pa} = 1$ (Equation (2))). The player routes the request of calculation only via its neighboring players, since for privacy preserving concerns we limit direct communication of players and only allow communication via neighboring players. Please note that in this paper we assume the connections in the SCN are equally weighted. In a weighted graph, another mechanism to identify the neighboring players will be necessary. Furthermore, this part of the method determines a new shortest path (Line 21-28), or the additional shortest paths (Line 29-38).

Line	Description
21-28	This part of the method determines if the path via the neighboring player is a new shortest path. We define, $smin(m, n)$ as a function which performs the comparison of given input parameters m and n based on Yao's secure comparison algorithm as $$smin(m,n) = \begin{cases} \text{true} & \text{if}\, n < m, \\ \text{false} & \text{otherwise} \end{cases}$$ which keeps the input parameters of the players n and m private. In method *calculateSecureShortestPath()* we are interested in finding the result of $smin(w_a + d_t^{(a)}, d_t)$. The values of d_t and w_a are known to player p. The distance of the neighboring player a to target player t, $(d_t^{(a)})$ is known to player a. To use $smin()$, and keep the input variables of each player private, we do the comparison as $smin\left(d_t^{(a)}, d_t - w_a\right)$ which uses the input of the current player and the neighboring player separately. The value of $d_t^{(a)}$ is not known for the current player, therefore it routes the requests to its neighboring player to participate in the calculation of the $smin$ by $smin(a.calculateSecureShortestPath(), td - w_a)$. Please note, as mentioned at Line 16 current player uses a temporary distance value td instead of d_t during the calculation. Player a does not share the distance value, and takes part with its encrypted input in the secure comparison of the distances. If the result of smin($d_t^{(a)}, d_t - w_a$) is true, it implies that the alternative path via a is shorter than the existing path(s), so this path is a shortest path in this iteration. In this case current player, at Line 27, assigns the calculated value of distance to its temporary variable of distance td. For privacy preserving concerns, we share as little information as possible. Consequently, if the alternative path via player a is not shorter than the existing one(s), current player will not find it out.
23-26	Since the method is recursive, it is important to prevent assignment of values during the execution and before the source player which initiated the request receives the final result. Line 23 examines if p is source player s, which implies the initiating player received its own request, and then allows the method to update Ω_t.

Line	Description
	By finding a new shortest path (at Line 21), the previously found path(s) and the players which are forming these paths are not relevant anymore. Player a is the neighboring player, which connects player p with the shortest path to the target. Therefore, the method updates Ω_t, and sets player a as its only member.
29-38	If the path via the neighboring player is not shorter than previously found shortest path(s), this part of the method determines if the path via this neighboring player is an additional shortest path.
31-37	This part of the method aims to determine if the path via the neighboring player is an additional shortest path. If the following equation is true, it implies that the alternative path via player a, and the already calculated path are equal. $$\neg smin(m,n) \land \neg smin(n,m) = true$$ In our case we evaluate the following expression: $\neg smin(d_t^{(a)}, d_t - w_a) \land \neg smin\left(d_t - w_a, d_t^{(a)}\right) = true$. In the case of $\neg smin\left(d_t^{(a)}, d_t - w_a\right) = true$, we only need to examine $\neg smin\left(d_t - w_a, d_t^{(a)}\right)$ = *true*. Line 31 of the methods performs this comparison. For privacy preserving concerns (as already elaborated at Line 21-28) player a does not share the distance value, but only takes part with its encrypted input for secure multiparty calculation of $smin(\ td - w_a, a.calculateSecureShortestPath())$. It should be noted that for the comparison of the shortest path distances (Line 31) the current player does not know $d_t^{(a)}$, and therefore routes the request to the neighboring player a by *a.calculateSecureShortestPath(s,t)*. Please note, the neighboring player a, already calculated this path (as Line 21) and therefore immediately returns this value.
33-36	Since the method is recursive, it is important to prevent the assignment of values before the source player, which initiated the request receives the final result. Line 33 examines if p is source player s and then allows the method to update Ω_t. Finding an additional shortest path implies that player a is connecting player p with the shortest path to target player t. Therefore, Line 35 adds player a to Ω_t.

For reasons of simplicity we provide the sequence diagram of the method for a specific path. Figure 4 provides the *calculateSecureShortestPath*(5,7) from player 5’s perspective for our exemplary network (Figure 1). We assumed δ for player 7 is 70.

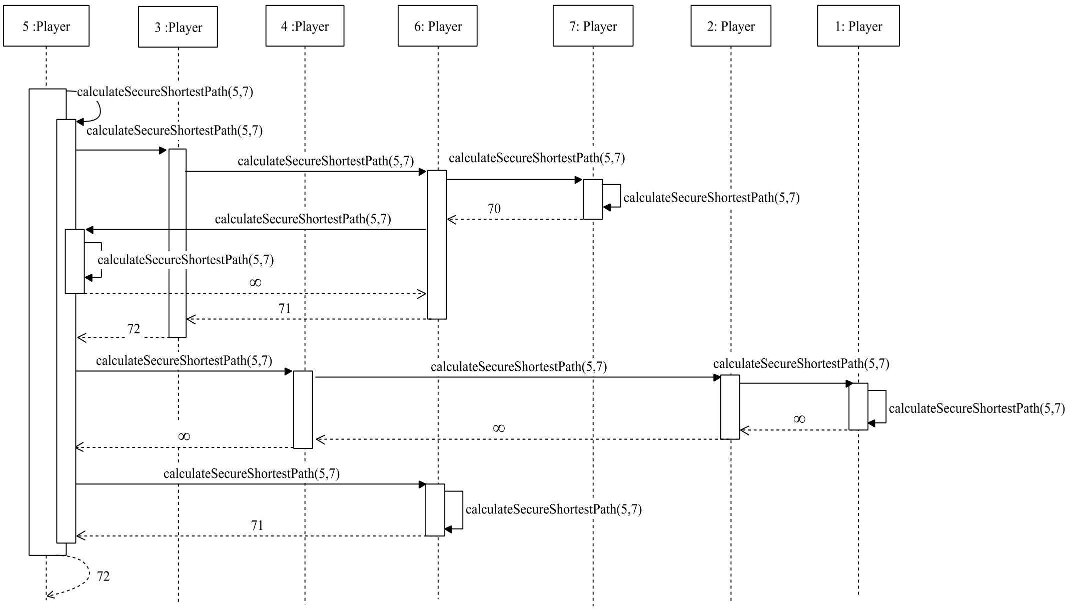

5 :Player
3 :Player
4 :Player
6: Player
7: Player
2: Player
1: Player
calculateSecureShortestPath(5,7)
calculateSecureShortestPath(5,7)
calculateSecureShortestPath(5,7)
calculateSecureShortestPath(5,7)
calculateSecureShortestPath(5,7)
70
calculateSecureShortestPath(5,7)
calculateSecureShortestPath(5,7)
∞
71
72
calculateSecureShortestPath(5,7)
calculateSecureShortestPath(5,7)
calculateSecureShortestPath(5,7)
calculateSecureShortestPath(5,7)
∞
∞
∞
calculateSecureShortestPath(5,7)
calculateSecureShortestPath(5,7)
71
72

Figure 4. Sequence diagram for calculateSecureShortestPath(5,7) from player 5’s perspective

In the following, (Figure 5) we provide the pseudocode of *calculateNumberOfShortestPaths*() method.

```
METHOD 2.    calculateNumberOfShortestPaths
Input: sourcePayerNumber $s$, targetPlayerNumber $t$.
if $s = p$ then
{
        if $w_t = 1$ then
        {
                $\sigma_{st} \leftarrow 1$
        }
        else
        {
                $\sigma_{st} \leftarrow |\Omega_t|$
        }
}
else
{
        $\sigma_{st} \leftarrow \max(|\Omega_t| - 1, 0)$
}
for each $\omega \in \Omega_t$ do
{
        $\omega.calculateNumberOfShortestPaths(s, t)$
}
```

Figure 5. Pseudocode of the method calculateNumberOfShortestPaths

Table 7 provides a detailed description of *calculateNumberOfShortestPaths*() method.

Table 7. Description of the calculateNumberOfShortestPaths () method

Line	Description
1-11	This part of the method sets the number of the shortest paths (σ_{st}) when the current player is the source player s.
3-6	This part of the method sets the number of the shortest paths (σ_{st}) when the target player is a neighboring player of source player s. If target player t is a neighboring player of source player s (Line 3), Line 5 sets the number of the shortest paths to one ($\sigma_{st} = 1$) because there is only one shortest path between two neighboring players in an unweighted graph.
7-10	This part of the method sets the number of the shortest paths (σ_{st}) when the target player is not a neighboring player of source player s. If target player t is not a neighboring player of source player s, the size of set Ω_t (that includes all neighboring players which connect current player p as source to the target) is the number of shortest paths between player p and the target t (σ_{st}). As already mentioned, the player has a portion of this value from its own perspective. The final value of σ_{st} is the sum of the decentrally calculated values of all players as shown in Equation 5.
12-15	This part of the method sets the number of the shortest paths (σ_{st}) when the current player is not the source player s. This player received the request of *calculateNumberOfShortestPaths(s,t)* because it is one of the players which is forming the shortest path between source and target player. Already one of the shortest paths on which the player lies, is considered by the source player s. Consequently, we need to consider the additionally identified shortest paths via this player. If there is an additional path via this player to the source, Line 14 sets the value of σ_{st} to $\|\Omega_t\| - 1$, otherwise set it to zero. We decrease the value of $\|\Omega_t\|$ by one, to prevent double consideration of the already considered path.
16-19	To consider additional shortest paths which might be identified by the players which are forming the shortest paths between the source and target player, the method recursively routes the message for calculating the number of shortest paths via the neighboring players which are forming the shortest paths (Line 18). The method identifies this neighboring player by Line 16, when $\omega \in \Omega_t$.

The *calculateNumberOfShortestPaths*() method identifies the number of the shortest paths from the source player and recursively identifies additional shortest paths via the players who are forming the shortest path(s). The following example elaborates an exemplary scenario of the method's execution. For instance player 5 executes the *calculateNumberOfShortestPaths*(5,7) and identifies $\sigma_{57}^{(5)} = 1$. Since player 7 is not a neighboring player of player 5, and player 6 is in Ω_7 player the method calls itself from player 6. Player 6 does not identify any additional path (since player 6's $\Omega_7 = 0$) therefore, it sets $\sigma_{57}^{(6)} = 0$. At this point the method terminates while player 7 (the target) is a neighboring player of player 6.

Figure 6 provides the pseudocode of *determinePlayersOnShortestPaths*() method.

```
METHOD 3.    determinePlayersOnShortestPaths
Input: sourcePlayerNumber $s$, targetPlayerNumber $t$.
    if $|\Omega_t| > 1$ and $s \neq p$ then
    {
        $\sigma_{st}(p) \leftarrow \max(|\Omega_t| - 1, 0)$
    }
    for each $\omega \in \Omega_t$ do
    {
        $\sigma_{st}(\omega) \leftarrow 1$
        $\boldsymbol{\omega.calculatePlayersOnShortestPaths(s, t)}$
    }
```

Figure 6. Pseudocode of the method determinePlayersOnShortestPaths

Table 8 provides a detailed description of *determinePlayersOnShortestPaths*() method.

Table 8. Description of determinePlayersOnShortestPaths() method

Line	Description
1-4	This part of the method sets the values of the frequency of the appearance of a player on a shortest path for itself $\sigma_{st}(p)$. When current player p is not source player s and the number of shortest paths (size of set Ω_t) from the current player to the target is greater that one, Line 3 sets the value of $\sigma_{st}(p)$ to $\lvert\Omega_t\rvert - 1$. The player is already considered on the shortest paths by the neighboring player which called it. Therefore, to prevent double consideration of the player we decrease the value of $\lvert\Omega_t\rvert$ by one. As already mentioned, the player has a portion of this value from its own perspective. The final value of $\sigma_{st}(p)$ is the sum of the decentrally calculated values of all players as shown in Equation 5.
5-9	This part of the method sets the values of the frequency of the appearance of a the neighboring players that form the shortest path on the shortest path between players s and t ($\sigma_{st}(\omega)$) and routes the message via the neighboring players forming the shortest paths. Line 7 sets the value of $\sigma_{st}(\omega)$ for the neighboring player ω to one because the player ω is on the shortest path from s to t. Player p can only update the values of $\sigma_{st}(\omega)$ for its neighboring players, but the frequency of appearance of a player on the shortest paths should be updated for all of the players on the shortest paths between source player s and target player t. The method calls itself to route the message via its neighboring player and update the values recursively.

The *determinePlayersOnShortestPaths*() method subsequently considers a player on the shortest paths between source player s and target player t when the player is in Ω_t of the current player. The following example elaborates an exemplary scenario of the method's execution. Moreover it reconsiders the current player (except the case where $s = p$) on the shortest paths when current player p has more than one shortest path to the target. For instance the *determinePlayersOnShortestPaths*(5,7), identifies $\sigma_{57}^{(5)}(6) = 1$ while player 6 is in player 5's Ω_7. Since player 7 is not a neighboring player of player 5, the method calls itself from its neighboring player (player 6). Player 6 is the neighboring player of the target (player 7) therefore, no further calculation takes place and the method terminates.

The *calculateSecureBetweenness*(v) method calculates the BC for player v based on SMC algorithms. In order to facilitate all-to-all communication, ISA coordinates the simultaneous exchange of information. To ensure that the real identities of the firms stay private in an all-to-all communication, existing tools for anonymization can be adapted.

The BC for player v based on Equation (1) is as follows:

$$\mathrm{BC}(v) = \sum_{s\neq v\neq t\in V} \frac{\sigma_{st}(v)}{\sigma_{st}} = \frac{\sigma_{12}(v)}{\sigma_{12}} + \frac{\sigma_{13}(v)}{\sigma_{13}} + \frac{\sigma_{14}(v)}{\sigma_{14}} + \cdots + \frac{\sigma_{n,n-1}(v)}{\sigma_{n,n-1}}, \text{ where } n = |V|\,.$$

For the calculation of the BC we use SMC algorithms. Secure addition and secure multiplication algorithms will, however, reveal a party's input as inverse functions can easily be applied for only two input factors. To keep the input variables in arithmetic operations private, it is necessary that more than two players deliver input. In the above mentioned equation we address this problem. By division of two variables delivered by two players, even with the application of SMC algorithms, the end result reveals the input variables for the players. Therefore, by using a common denominator we solve the problem as follows:

$$\mathrm{BC}(v) = \frac{\sigma_{12}(v)\cdot\left(\sigma_{13}\cdot\ldots\cdot\sigma_{n,n-1}\right) + \sigma_{13}(v)\cdot\left(\sigma_{12}\cdot\ldots\cdot\sigma_{n,n-1}\right) + \cdots + \sigma_{n,n-1}(v)\cdot\left(\sigma_{12}\cdot\ldots\cdot\sigma_{n,n-2}\right)}{\sigma_{12}\cdot\sigma_{13}\cdot\ldots\cdot\sigma_{n,n-1}} \qquad (6)$$

Please note, Equation (6) does not include the values of $\sigma_{st}(v)$ and σ_{st} where $s = v$ or $t = v$. Furthermore, the values of σ_{st} and $\sigma_{st}(v)$ $\forall s \neq v \neq t \in V$ are the results of Equation (5). For privacy preserving concerns, as addressed in Requirement 1, we do not calculate and share the final values of σ_{st} and $\sigma_{st}(v)$ in the network. Hence, we use the distributive property of arithmetic operations to distributedly consider the components of Equation (5) in Equation (6). Using the mentioned modification on the BC calculation's equation we provide the possibility to keep the private shares of the players private and calculate the BC. The implementation of the artifact with the application of SMC algorithms, anonymization methods, and necessary communication protocols are not covered in this paper.

III.1.5 Evaluation

This section provides the evaluation of our artifact. Concerning characteristics of our artifact, we chose the "testing" and "descriptive evaluation" methods based on Hevner et al. (2004) and Gill and Hevner (2013). We implemented a simplified prototype of the artifact. The prototype covers the methods of class Player. However, the prototype does not cover the implementation of SMC algorithms and assumes they are given. Moreover, the prototype models each player as a local thread, and it is not executed on a distributed system. Furthermore, a third person other than the authors manually evaluated the artifact with a structural walk through the code.

In the following we cover general evaluation of completeness, termination, complexity, utility and privacy of the artifact. Furthermore, we illustrate the privacy evaluation based on an application example. Although based on the acceptance and wide application of SMC algorithms we did not analyze their properties. We assume SMC algorithms are complete and secure.

Completeness: To evaluate the artifact in terms of completeness we executed the prototype with various scenarios and evaluated the results. It proved that our approach creates complete results for each given network. Moreover, the structural walk through the code resulted the same.

Termination: By means of testing the prototype in various scenarios as well as structural walk through the code we conducted that the artifact terminates.

Complexity: Analysis of our artifact pointed both the time complexity and the message complexity are polynomial in the maximum distance between the source and the target player, and number of network members. In our artifact we focused to achieve a privacy preserving method. To preserve privacy, it is necessary for the players to encrypt and exchange data more often compared to some widely used algorithms (e.g. Brandes' algorithm (2001)). Further improvements of computational complexity of the artifact is subject to further research.

Utility: Based on Gregor and Hevner (2013) an artifact evaluation must address the utility of the artifact. Due to the complexity of implementation and evaluation of the artifact's utility in reality, in this paper we evaluated the utility of the artifact based a simplified prototype, and used an application example. Our artifact's characteristics based on Gill and Hevner (2013) are: it is a novel method, which is open because it is possible to modify it, and is interesting because it addresses risk management and sustainability as one of the main concerns of the firms in SCNs.

Privacy: The privacy requirements of our artifact (Requirement 1 and 2) are addressed as follows.

- The application of Yao's (1982) comparison algorithm and using the modified values for distances ensure that the distances of non-neighboring players stays unknown. Although in a small network, we illustrate in our application example, the distances might be inferable. However, in larger networks (which are in the focus of our research) players cannot infer the distance during the execution of the artifact.

- The number of the shortest paths, and the frequency of appearance of a player on the shortest path are saved decentrally, as mentioned in Equation (5). Therefore, the final values of σ_{st} and $\sigma_{\mathrm{st}}(v)$ are not available to the players and stay private.
- By restricting communication via neighboring players and application of anonymization methods, we addressed Requirement 2.

However, we will appreciate if other researchers challenge our artifact in terms of privacy. In specific cases players might infer information when they are called from neighboring players to execute the methods. However, the inferred information of the players are limited to the information from their perspective. For instance if the shortest path of a neighboring player to target t is via the current player it implies for the current player that the neighboring player and target t are not neighbors. Whereas it does not contain the information about the players which are forming the shortest paths and the number of shortest paths.

Furthermore, to illustrate the potential of our artifact to preserve privacy, we describe the artifact's outcome in a short example. Figure 7 provides the network structure (See Figure 1) from player 5's perspective before and after execution of the method. Based on the result of the BC calculation, players are prioritized and colored as shown in the figure. Player 5 has the highest BC. Player 4 is the second. Players 6 and 2 are having the same BC and are standing at the third place. The BC of players 1, 3 and 7 is zero, because they are not on any shortest path. This is a valuable information for all network's members. For instance it implies that if player 5 faces any failure, the whole network's robustness might be at risk. The BC of the players is available for all players in the SCN.

In our exemplary network through execution of the methods, player 5 infers some information. It knows that player 3 and 6 are neighbors, since player 6 and 3 are 5's neighboring players and their shortest paths are not via player 5. Player 5 knows also that players 1 and 6, 2 and 6, as well as 4 and 6 are not neighboring players. The latter information is inferred based on the information that their shortest path is via player 5. But the player is not knowing their exact positioning and if there exists any other alternative shortest path.

It is to conclude that the gained information about the network's structure, even in a small network is limited. By increasing the network's size and complexity the possibility of inferring information decreases. Additionally, the inferred information on non-neighboring vertices is limited. This is similar to a common situation of a SCN. In reality, in a SCN, a company knows more information about its neighbors. The company can partially reveal information about the neighbors of its own neighbors. By going further in the SCN, the company is less capable to deduce the underlying topology or identity of the companies. Moreover, in most of the SCNs, there are some main players that are known by everyone. If other companies identify these firms and their importance, it is not a risk for these players. Their importance and positioning in the network is predictable for most of the firms in the SCN.

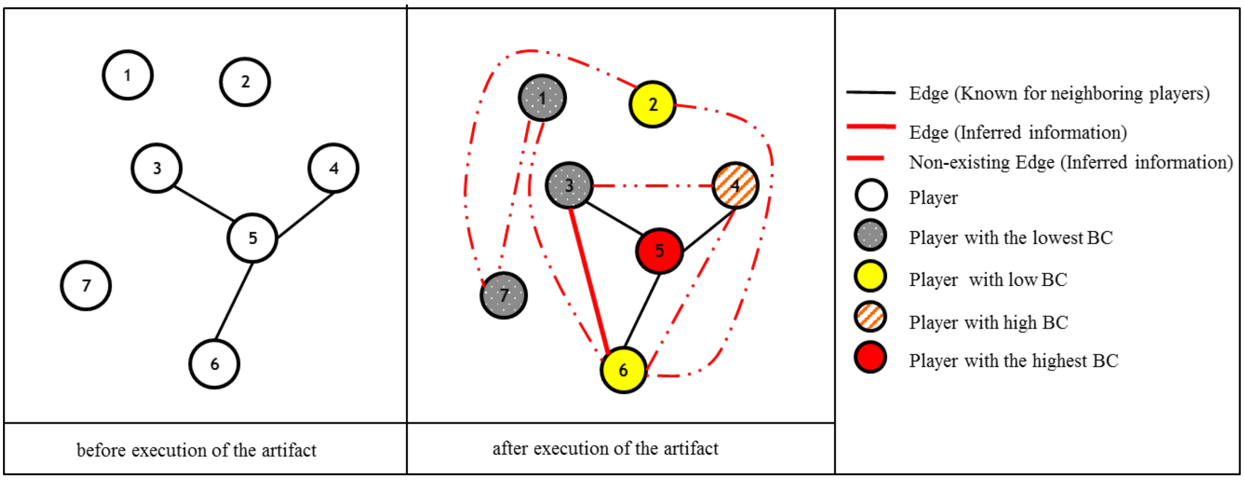

1
2
3
4
5
6
7
before execution of the artifact
after execution of the artifact
Edge (Known for neighboring players)
Edge (Inferred information)
Non-existing Edge (Inferred information)
Player
Player with the lowest BC
Player with low BC
Player with high BC
Player with the highest BC

Figure 7. The network's structure from player 5's perspective

III.1.6 Conclusion

In this paper, we proposed an artifact which preserves privacy and identifies the risky players in the SCNs applying the BC measure. Based on the guidelines of Hevner et al. (2004), and Gregor and Hevner (2013) for conducting design science research, we can summarize our work as follows: Our artifact consists of four main methods. It is an exaptation solution, because we adopted the existing methods in social networks and cryptography algorithms to identify risks in SCNs. Our artifact is formally noted and therefore is well-defined. Based on the literature (e.g. (Buhl and Penzel 2010)) we addressed two relevant problems: the risk identification in SCNs and privacy concerns of firms in SCNs. We focused on the study of Kim et al. (2011) and decided to calculate the BC as a measure to identify risky firms. In the evaluation section, beside the testing and descriptive evaluation, we illustrated that in our artifact, even in a small exemplary network, the inferred information is limited. To develop a rigorous artifact, we applied well established methods of other fields and extended them to our problem context. Regarding the contribution of our result, we choose the evolving technical solutions in computer science and network theory, to answer the question of risk management in SCNs.

In this paper, we focused on identifying risks and kept the information as private as possible. However, higher visibility in the network facilitates improved risk management (Basole and Bellamy 2014). Therefore, it might be necessary that companies agree on sharing more information than the BCs. For instance they might decide to reveal the identities of companies with the BC among top 10%, because they are the most risky ones for the network. On the one hand the more information is shared, the highest is the privacy at risk, and on the other hand it is inevitable to share extra information to reach the network's robustness. Hence, the companies in the network should deal with the trade-off between sharing additional information to facilitate risk management in the network or preserve their privacy.

Although the BC measure identifies the risks in the SCN, integration of complementary network analysis approaches (e.g. (Newman 2013)) in our artifact for an enhanced risk identification, is subject to further research. It is also important to study the intensity of connection and their impacts on the network. These subjects as well as improvement of computational complexity are subject to further research.

III.1.7 References

Abbe, E. A., Khandani, A. E., & Lo, A. W. (2012). Privacy-preserving Methods for Sharing Financial Risk Exposures. *The American Economic Review, 102*(3), 65–70.

Acemoglu, D., Ozdaglar, A., & Tahbaz-Salehi, A. (2015). *Networks, Shocks, and Systemic Risk.* Cambridge, MA: National Bureau of Economic Research.

Arns, M., Fischer, M., Kemper, P., & Tepper, C. (2002). Supply Chain Modelling and Its Analytical Evaluation. *Journal of the Operational Research Society, 53*(8), 885–894.

Babich, V., Burnetas, A. N., & Ritchken, P. H. (2007). Competition and diversification effects in supply chains with supplier default risk. *Manufacturing & Service Operations Management, 9*(2), 123–146.

Basole, R. C., & Bellamy, M. A. (2014). Supply Network Structure, Visibility, and Risk Diffusion: A Computational Approach. *Decision Sciences, 45*(4), 753–789.

Beaver, D., Micali, S., & Rogaway, P. (1990). The Round Complexity of Secure Protocols. In H. Ortiz (Ed.), *twenty-second annual ACM symposium on Theory of computing* (pp. 503–513): ACM.

Bellamy, M. A., & Basole, R. C. (2013). Network Analysis of Supply Chain Systems: A Systematic Review and Future Research. *Systems Engineering, 16*(2), 235–249.

Blackhurst, J., Wu, T., & O'grady, P. (2004). Network-based Approach to Modelling Uncertainty in a Supply Chain. *International Journal of Production Research, 42*(8), 1639–1658.

Blome, C., & Schoenherr, T. (2011). Supply chain risk management in financial crises—A multiple case-study approach. *International Journal of Production Economics, 134*(1), 43–57.

Bogetoft, P., Damgård, I., Jakobsen, T., Nielsen, K., Pagter, J., & Toft, T. (2006). A Practical Implementation of Secure Auctions Based on Multiparty Integer Computation. *Financial Cryptography and Data Security, 4107*, 142–147.

Brandes, U. (2001). A faster algorithm for betweenness centrality*. *Journal of Mathematical Sociology, 25*(2), 163–177.

Brickell, J., & Shmatikov, V. (2005). Privacy-preserving graph algorithms in the semi-honest model. *Advances in Cryptology-ASIACRYPT 2005*, 236–252.

Buhl, H. U., & Penzel, H.-G. (2010). The Chance and Risk of Global Interdependent Networks. *Business & Information Systems Engineering, 2*(6), 333–336.

Canetti, R. (2008). Theory of cryptography. In R. Canetti (Ed.), *Fifth theory of cryptography conference, TCC* : Springer.

Choi, T. Y., & Hong, Y. (2002). Unveiling the structure of supply networks: case studies in Honda, Acura, and DaimlerChrysler. *Journal of Operations Management, 20*(5), 469–493.

Choi, T. Y., & Krause, D. R. (2006). The supply base and its complexity: implications for transaction costs, risks, responsiveness, and innovation. *Journal of Operations Management, 24*(5), 637–652.

Chu, L. K., Shi, Y., Lin, S., Sculli, D., & Ni, J. (2010). Fuzzy chance-constrained programming model for a multi-echelon reverse logistics network for household appliances. *Journal of the Operational Research Society, 61*(4), 551–560.

Cormen, T. H., Leiserson, C. E., Rivest, R. L., & Stein, C. (2001). *Introduction to algorithms* (Vol. 2): MIT press Cambridge.

Cramer, R., Damgard, I., & Nielsen, J. B. (2013). *Secure Multiparty Computation and Secret Sharing: An Information Theoretic Approach*. Aarhus Unoversity, Denmark: Aarhus University.

Dijkstra, E. W. (1959). A note on two problems in connexion with graphs. *Numerische mathematik, 1*(1), 269–271.

Dolev, D., & Yao, A. C. (1983). On the security of public key protocols. *Information Theory, IEEE Transactions on, 29*(2), 198–208.

Edmonds, N., Hoefler, T., & Lumsdaine, A. (2010). A space-efficient parallel algorithm for computing betweenness centrality in distributed memory. In *International Conference on High Performance Computing (HiPC)* (pp. 1–10): IEEE.

Ellinas, C., Allan, N., & Johansson, A. (2016). Project systemic risk: Application examples of a network model. *International Journal of Production Economics, 182*, 50–62 (2016). doi:10.1016/j.ijpe.2016.08.011

Floyd, R. W. (1962). Algorithm 97: shortest path. *Communications of the ACM, 5*(6), 345.

Freeman, L. C. (1977). A Set of Measures of Centrality Based on Betweenness. *Sociometry, 40*, 35 (1977). doi:10.2307/3033543

Fridgen, G., Stepanek, C., & Wolf, T. (2014). Investigation of exogenous shocks in complex supply networks–a modular Petri Net approach. *International Journal of Production Research*(ahead-of-print), 1–22.

Fridgen, G., & Zare Garizy, T. (2015). Supply Chain Network Risk Analysis: A Privacy Preserving Approach. In *23^rd^ European Conference on Information Systems (ECIS 2015)*.

Giannakis, M., & Louis, M. (2011). A multi-agent based framework for supply chain risk management. *Journal of Purchasing and Supply Management, 17*(1), 23–31.

Gill, T. G., & Hevner, A. R. (2013). A fitness-utility model for design science research. *ACM Transactions on Management Information Systems (TMIS), 4*(2), 5.

Goldreich, O., Micali, S., & Wigderson, A. (1987). How to Play any Mental Game - A Completeness Theorem for Protocols with Honest Majority. In A. V. Aho (Ed.), *Nineteenth annual ACM Symposium on the Theory of Computing* (pp. 218–229).

Gregor, S., & Hevner, A. R. (2013). POSITIONING AND PRESENTING DESIGN SCIENCE RESEARCH FOR MAXIMUM IMPACT. *MIS Quarterly, 37*(2), 337-A-6.

Gyorey, T., Jochim, M., & Norton, S. (2011). The challenges ahead for supply chains. *McKinsey on Supply Chain: Select Publications*, 10–15.

Hallikas, J., Karvonen, I., Pulkkinen, U., Virolainen, V.-M., & Tuominen, M. (2004). Risk management processes in supplier networks. *International Journal of Production Economics, 90*, 47–58 (2004). doi:10.1016/j.ijpe.2004.02.007

HBR Advisory Council. (2010). Is Your Supply Chain Sustainable? *Harvard Business Review;, 88*(10), 74.

Helbing, D. (2013). Globally networked risks and how to respond. *Nature, 497*, 51–59 (2013). doi:10.1038/nature12047

Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75–105.

Hochberg, Y. V., Ljungqvist, A., & Lu, Y. (2007). Whom you know matters: Venture capital networks and investment performance. *The Journal of Finance, 62*(1), 251–301.

Huang, Y., Katz, J., & Evans, D. (2012). Quid-pro-quo-tocols: Strengthening semi-honest protocols with dual execution. In *2012 IEEE Symposium on Security and Privacy (SP)* (pp. 272–284): IEEE.

Jacob, R., Koschützki, D., Lehmann, K. A., Peeters, L., & Tenfelde-Podehl, D. (2005). Algorithms for Centrality Indices. In D. Hutchison, T. Kanade, J. Kittler, J. M. Kleinberg, F. Mattern, J. C. Mitchell, et al. (Eds.), *Network Analysis* (Vol. 3418, pp. 62–82, Lecture Notes in Computer Science). Berlin, Heidelberg: Springer Berlin Heidelberg.

Kerschbaum, F. (2011). Secure and sustainable benchmarking in clouds. *Business & Information Systems Engineering, 3*(3), 135–143.

Kerschbaum, F., Schroepfer, A., Zilli, A., Pibernik, R., Catrina, O., Hoogh, S. de, et al. (2011). Secure Collaborative Supply-Chain Management. *Computer, 44*, 38–43 (2011). doi:10.1109/MC.2011.224

Kersten, W., Hohrath, P., & Winter, M. (2008). Risikomanagement in Wertschöpfungsnetzwerken–Status quo und aktuelle Herausforderungen. *Supply Chain Risk Management*, 7.

Kim, Y., Choi, T. Y., Yan, T., & Dooley, K. (2011). Structural investigation of supply networks: A social network analysis approach. *Journal of Operations Management, 29*(3), 194–211.

Klein, D. J. (2010). Centrality measure in graphs. *Journal of mathematical chemistry, 47*(4), 1209–1223.

Lessard, D. R. (2013). Uncertainty and Risk in Global Supply Chains. *MIT Sloan Research Paper No. 4991-13*.

Li, M. E., & Choi, T. Y. (2009). Triads in Services Outsourcing: Bridge, Bridge Decay and Bridge Transfer*. *Journal of Supply Chain Management, 45*(3), 27–39.

Lindell, Y., & Pinkas, B. (2009). A proof of security of Yao's protocol for two-party computation. *Journal of Cryptology, 22*(2), 161–188.

Mizgier, K. J., Jüttner, M. P., & Wagner, S. M. (2013). Bottleneck identification in supply chain networks. *International Journal of Production Research, 51*(5), 1477–1490.

Moore, E. F. (1959). The shortest path through a maze. In Harvard University Press (Ed.) (pp. 285–292): Bell Telephone System.

Newman, M. E. J. (2013). *Networks: An introduction*. Oxford: Oxford Univ. Press.

Peck, H. (2003). *Creating Resilient Supply Chains: A Practical Guide*. United Kingdom: Cranfield University.

Reistad, T. I. (2012). Multi-party secure position determination. In *Norsk Informatikkonferanse NIK 2006* (pp. 137–142, A General Framework for Multiparty Computations). Trondheim: Norwegian University of Science and Technology.

Russell, S., & Norvig, P. (2009). *Artificial Intelligence: A Modern Approach* : Prentice Hall.

Schneider, T. (2012). *Engineering Secure Two-Party Computation Protocols: Design, Optimization, and Applications of Efficient Secure Function Evaluation*. Berlin, Heidelberg: Springer.

Shamir, A. (1979). How to share a secret. *Communications of the ACM, 22*(11), 612–613.

Sheikh, R., Kumar, B., & Mishra, D. K. (2009). Privacy Preserving k Secure Sum Protocol. *International Journal of Computer Science and Information Security, 6*(2), 184–188.

Vereecke, A., van Dierdonck, R., & Meyer, A. de. (2006). A typology of plants in global manufacturing networks. *Management science, 52*(11), 1737–1750.

Wagner, S. M., & Neshat, N. (2012). A comparison of supply chain vulnerability indices for different categories of firms. *International Journal of Production Research, 50*(11), 2877–2891.

Warshall, S. (1962). A theorem on boolean matrices. *Journal of the ACM (JACM), 9*(1), 11–12.

Wasserman, S., & Faust, K. (2009). *Social network analysis: Methods and applications* (19th ed., Structural analysis in the social sciences, Vol. 8). Cambridge: Cambridge Univ. Press.

Wilding, R., Miemczyk, J., Johnsen, T. E., & Macquet, M. (2012). Sustainable purchasing and supply management: A structured literature review of definitions and measures at the dyad, chain and network levels. *Supply Chain Management: An International Journal, 17*, 478–496 (2012). doi:10.1108/13598541211258564

World Economic Forum. (2008,). *Global Risks 2008: A Global Risk Network Report*.

Yao, A. C. (1982). Protocols for secure computations. In *23rd Annual Symposium on Foundations of Computer Science* (pp. 160–164).

Yao, A. C. (1986). How to generate and exchange secrets. In *27th Annual Symposium on Foundations of Computer Science* (pp. 162–167): IEEE.

Yates, J. F., & Stone, E. R. (1992). The risk construct. In J. F. Yates (Ed.), *Risk-taking behavior* (pp. 49–85). New York: John Wiley & Sons.

Zhao, K., Kumar, A., Harrison, T. P., & Yen, J. (2011). Analyzing the resilience of complex supply network topologies against random and targeted disruptions. *Systems Journal, IEEE, 5*(1), 28–39.

IV Conclusion and Future Research

This chapter gives a summary of the main findings of this doctoral thesis (Section IV.1), and outlines the further research agenda (Section IV.2) on the subject of systemic risk assessment in complex network structures, considering IT as a challenge and as a chance.

IV.1 Conclusion

The embedded papers in this doctoral thesis not only introduce approaches to assess the challenges of IT in today's digital age (Chapters II), but also introduce IT solutions for the assessment of systemic risk in supply chain networks as the first step towards the deployment of the chances of IT in the management of systemic risk (Chapter III).

IV.1.1 Chapter II: Systemic Risk in IT Project Portfolios: IT as a Challenge

Research Paper 1 provides a solution for the monetary assessment of the criticality of each IT project in an IT project portfolio (ITPP). First, the paper sets the main requirements for the criticality assessment of IT projects in an ITPP. Second, existing methods of criticality assessment are evaluated to disclose their shortcomings. Third, the paper assesses the applicability of Bayesian network modelling in the criticality assessment of ITPPs. The proposed approach considers IT projects and shared resources as nodes, the dependencies between them as edges, and interprets the ITPP as a network structure. Further, it quantifies the strength of the dependencies based on *the probability that one particular project failure causes the failure of another project*. The quantification is based on a common underlying factor that enabled the integration of various types of dependencies and their impacts in the model. Finally, applying Bayesian network modelling, along with the *with-without* principle from risk management (Tasche 2008), the paper provides the risk exposure of each IT project as the measure of criticality. The monetary assessment of criticality, which is evaluated by means of a demonstration example, a sensitivity analysis, and simulations, underlines the applicability of Bayesian network modelling for criticality assessment. The result of the method should support IT portfolio managers in the assessment of systemic risk which is the first step towards the management of systemic risk in ITPPs.

Furthermore, Research Paper 2 integrates the assessment of systemic risk in a value-based ITPP evaluation approach. The proposed approach interprets ITPPs as network structures and quantifies the strength of dependencies based on the *relative time lag* that a particular project can cause to another project. The approach applies alpha centrality to investigate the systemic risk in ITPPs. The method uses a pseudo-covariance matrix of IT projects as the exogenous factor in the calculation of alpha centrality. This delivers a risk factor for the ITPP which includes the transitive effect of dependencies. Combining the alpha centrality with the well-established methods of IT project and ITPP evaluation (Fridgen et al. 2015; Beer et al. 2013), enabled developing a comprehensive value-based ITPP evaluation approach.

To sum up, Research Papers 1 and 2 provide a comprehensive and thorough insight into the topic of systemic risk and its assessment in ITPPs. However, this field has great potential for further research that will be addressed in section IV.2.1.

IV.1.2 Chapter III: Systemic Risk in Supply Chain Networks: IT as a Chance

So far, we introduced solutions for organizations to handle the challenges of IT. However, the organizations which handle the challenges of IT, can profit from IT solutions in the assessment of systemic risk. Research Paper 3 focuses mainly on the development of a technical solution to enable the assessment of systemic risk in supply chain networks. It also consider how to overcome the concerns of organizations about information sharing and risking their strategic connections by means of a privacy preserving solution. This paper uses betweenness centrality to identify risky organizations, for which the cascading effect of their failure has a high impact on the supply chain network's performance. To determine the risky organizations while preserving their privacy, the approach applies secure multiparty computation cryptography methods (Yao 1986; Cramer et al. 2010). To benefit from secure multiparty computation metohds, a modification of the existing algorithms for calculation of betweenness centrality and the shortest paths, are necessary. These modifications enable joint calculation of the results based on encrypted private information of each organization. Finally, the developed artifact based on the modified algorithms, assesses systemic risk in supply chain networks, preserving the privacy of the organizations. Evaluation based on testing, application example, and informed arguments (c.f. descriptive evaluation (Hevner et al. 2004)) confirmed the completeness, termination, utility and privacy of the artifact for the assessment of systemic risk in supply chain networks. Our artifact is an exaptation solution (Gregor and Hevner 2013), in that it adopts the existing methods of cryptography and social network analysis to identify risky organizations in supply chain networks.

However, the area of the assessment of systemic risk in supply chain networks still has a great potential to benefit from the chances of IT. Section IV.2.2 provides an outlook of further research in this field.

In all, this doctoral thesis contributes to the field of systemic risk assessment in complex network structures. Most notably, the research papers given here in Chapters II and III account for the role of IT as a challenge and as a chance as described above in this context. However, there is still a great potential for further research in the area of systemic risk assessment and the role of IT, respectively. The following section (Section IV.2) details this.

IV.2 Future Research

The following sections highlight possible extensions of these papers, and outline topics for further research in the area as a whole.

IV.2.1 Chapter II: Systemic Risk in IT Project Portfolios: IT as a Challenge

This section outlines potential for future research in systemic risk assessment within ITPPs. It addresses the potential of each research paper's further development, followed by an outline of the overarching aspects of future research.

The Bayesian network modelling approach for criticality assessment of IT projects in Research Paper 1, relies on the ex-ante estimation of the failure probabilities in order to determine the risk exposure of each IT project. Its relevant aspects for future research are as follows:

- The method focused on the assessment of the negative effects of dependencies between of IT projects. However, the dependencies between IT projects can have synergistic effects. Therefore, it is important to consider the benefits of the dependencies between IT projects as well. Consequently, future research should extend the method by assessing benefits and integrating both risks and benefits of the dependencies within a holistic ITPP evaluation method.
- The paper relies on an expert estimation of the variables. However, expert estimation has a certain degree of intra-person inconsistency (Grimstad and Jørgensen 2007). Therefore, further research should develop methods to increase the quality of estimation by for example using real-world data and applying methods like fuzzy reasoning.

Research Paper 2 states a few simplification assumptions in order to develop a holistic approach for ITPP evaluation. These assumptions lead to the following aspects for future research:

- The method relies on linear coherence between the duration of an IT project and its assigned resources in order to quantify the dependencies. Although this assumption might seem plausible to start out, it is not applicable to all types of resource dependencies and especially not to personnel resources. Therefore, further research is necessary to develop quantification approaches which are applicable for different types of resource dependencies.
- The method's evaluation is based on a simulation and an application example. However, it is also necessary to evaluate the methods in real-world context. Therefore, further research should investigate the result of the approach in real-world scenarios. Researchers are further encouraged to benefit from approaches like action design

research (Sein et al. 2011) to shape the method in organizational context and increase the method's applicability.

In addition, three overarching topics can enrich the research area and increase the applicability of the methods in practice. First, the proposed approaches mainly regarded the ex-ante assessment of systemic risk. However, in a comprehensive ITPP management ex-nunc (continual) and ex-post assessments are also important (Blumberg et al. 2012). Therefore, further extensions of the methods for ex-nunc and ex-post assessment should be the subject of further research.

Second, in the aforementioned approaches for the assessment of systemic risk in ITPPs, the traditional project management methods are the main focus. However, the number of organizations that are applying agile project management is increasing. Therefore, it is important to analyze the implications of such a shift using the described approaches. Eventually, the methods will need further adjustments for suitable application in the context of agile project and portfolio management.

Third, the proposed approaches for the assessment of systemic risk are based on the network interpretation of ITPPs. For this purpose, the approaches simplified the complex structure of an ITPP, considered IT projects and shared resources as its nodes, and the dependencies between the nodes as its edges. These approaches integrated nodes and the edges between them in a single-layer (i.e., "monoplex") network structure. However, ITPPs are more complex, consisting of multiple types of internal (e.g. IT projects or resources) and external components (e.g. stakeholders or regulatory) and the dependencies between them. Therefore, it is necessary to develop methods which model all multiple types of components (nodes) and dependencies (edges). A possible approach may be the application of multilayer network approaches. A multilayer network has multiple layers representing individual types of interaction (e.g., social relationships, business collaborations, etc.) and each layer has its own adjacency matrix (Domenico et al. 2013). Furthermore, based on the interaction between the various layers of multilayer networks, the layers can be interdependent (Domenico et al. 2013). They enable achieving a deep understanding of complex real-world systems (Domenico et al. 2013). In recent years, the application of multilayer network approaches in various fields like social network analysis, transportation systems analysis or trade network analysis are unfolding (Domenico et al. 2013; Boccaletti S. et al. 2014). However, multilayer network approaches, to the best of our knowledge, have not yet been applied in the context of ITPP. Therefore, assessing the applicability of a multilayer network approach to model the complex structure of ITPPs and evaluate the systemic risk can be the topic of further research.

IV.2.2 Chapter III: Systemic Risk in Supply Chain Networks: IT as a Chance

This section outlines the potential for future research in systemic risk assessment within supply chain networks, regarding IT as a chance. Firstly, the section addresses the areas of future research presented in Research Paper 3, followed by the overarching aspects of future research in this area.

Research Paper 3 proposes a solution for the assessment of systemic risk in supply chain networks. Future research topics emanating from this are the following:

- The paper identifies risky organizations by calculating the betweenness centrality. Although betweenness centrality identifies specific types of risky organizations, this centrality measure cannot identify all types of risky organizations within the supply chain network. For instance, betweenness centrality cannot identify a single source key provider which is a last tier supplier (leaf of the supply chain network's graph). Therefore, further research should cover the identification of complementary measures which identify further types of risky organizations in supply chain networks.
- The artifact determines the risky organization within the supply chain network and keeps the information about each organization's positioning in the network as well as their identity as private as possible. However, further research should provide concrete guidelines on how to use this private information for risk management in supply chain networks.

In addition, further research should cover the development of data-driven approaches to suggest suitable reshaping of the supply chain network's structure in order to reduce the systemic risk and improve sustainability. These approaches can benefit from the results of the method proposed in this study in combination with additional information from the supply chain network properties.

Last but not the least, further research should account for the influences of new eras like the Internet of the Things (IoT), the 4th industrial revolution (Industry 4.0), and the transformation towards Cyber-Physical-Cyber-Human Systems (Gimpel and Röglinger 2015) in the context of systemic risk assessment. The higher connectivity, complexity, ambiguity and volatility of these systems (Gimpel and Röglinger 2015) shape new challenges and chances of IT in the context of systemic risk assessment.

Finally, this doctoral thesis has adopted methods from other disciplines in information systems research, in order to address the current challenges of practice in the assessment of systemic risk. The study provides novel approaches to the assessment of systemic risk in ITPPs, in order to enable organizations to handle the challenges of IT. In addition, it proposes an IT solution to assess systemic risk in supply chain networks. This doctoral thesis sharpens the role of IT in the assessment of systemic risk in complex network structures, respectively. Nevertheless, researchers should feel challenged to drill down on the assumptions and limitations of this doctoral thesis, and to conduct further research in order to bridge the gap between systemic risk assessment research and practice.

IV.3 References

Beer M, Fridgen G, Müller H, Wolf T (2013) Benefits Quantification in IT Projects. In: 11th International Conference on Wirtschaftsinformatik, pp 707–720

Blumberg S, Chen X, Heidemann J, Beer M, Fridgen G, Müller H (2012) IT-Projektsteuerung? eine Methodik zum Benefits-Management mit integrierter Risikobetrachtung. Wirtschaftsinformatik & Management 4(5):56–60

Boccaletti S., Bianconi G, Criado R, del Genio CI, Gómez-Gardeñes J, Romance M, Sendiña-Nadal I, Wang Z, Zanin M (2014) The structure and dynamics of multilayer networks. Physics Reports 544(1):1–122. doi: 10.1016/j.physrep.2014.07.001

Cramer R, Damgard I, Nielsen JB (2010) Secure multiparty computation and secret sharing-an information theoretic approach. Citeseer

Domenico M de, Solé-Ribalta A, Cozzo E, Kivelä M, Moreno Y, Porter MA, Gómez S, Arenas A (2013) Mathematical Formulation of Multilayer Networks. Phys. Rev. X 3(4). doi: 10.1103/PhysRevX.3.041022

Fridgen G, Klier J, Beer M, Wolf T (2015) Improving Business Value Assurance in Large-Scale IT Projects? A Quantitative Method Based on Founded Requirements Assessment. ACM Transactions on Management Information Systems 5(3):11/1

Gimpel H, Röglinger M (2015) Digital Transformation: Changes and Chances: Insights based on an Empirical Study. http://www.fim-rc.de/Paperbibliothek/Veroeffentlicht/542/wi-542.pdf

Gregor S, Hevner AR (2013) Positioning and Presenting Design Science Research for Maximum Impact. MIS Quarterly 37(2)

Grimstad S, Jørgensen M (2007) Inconsistency of expert judgment-based estimates of software development effort. Journal of Systems and Software 80(11):1770–1777. doi: 10.1016/j.jss.2007.03.001

Hevner AR, March ST, Jinsoo Park, Sudha Ram (2004) Design science in information systems research. MIS Quarterly: Management Information Systems 28(1):75–105

Sein MK, Henfridsson O, Purao S, Rossi M, Lindgren R (2011) Action Design Research. MIS Quarterly 35(1):37–56

Tasche D (2008) Capital Allocation to Business Units and Sub-Portfolios: the Euler Principle. In: Resti A (ed) Pillar II in the new Basel accord: The challenge of economic capital. Risk Books, London, pp 423–453

Yao AC (1986) How to generate and exchange secrets. In: 27th Annual Symposium on Foundations of Computer Science (sfcs 1986), pp 162–167