Curse or Blessing? Exploring risk factors of digital technologies in industrial operations

Kessler, Melanie; Arlinghaus, Julia C.; Rosca, Eugenia; Zimmermann, Manuel

Published in:
International Journal of Production Economics

DOI:
10.1016/j.ijpe.2021.108323

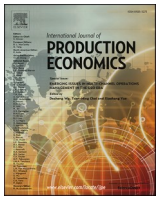
Publication date:
2022

Int. J. Production Economics 243 (2022) 108323

Contents lists available at ScienceDirect

International Journal of Production Economics

journal homepage: www.elsevier.com/locate/ijpe



Curse or Blessing? Exploring risk factors of digital technologies in industrial operations

Melanie Kessler [a,*], Julia C. Arlinghaus [b], Eugenia Rosca [c], Manuel Zimmermann [d]

[a] RWTH Aachen University, Templergraben 55, 52062, Aachen, Germany
[b] Otto von Guericke University, Universitätsplatz 2, Magdeburg, 39106, Germany
[c] Faculty of Business and Economics, University of Groningen, Groningen, the Netherlands
[d] FUNK Gruppe, Hamburg, Valentinskamp 20, 20354, Hamburg, Germany

ARTICLE INFO

Keywords:
Risk factors
Digitalisation
Technology life cycle
Normal accident theory
Industry 4.0 technologies
Technology vendors and users

ABSTRACT

Both practitioners and scholars emphasise the benefits of Industry 4.0 (I4.0) technology implementation, such as increased transparency and the availability of real-time data in operations processes. Current literature on I4.0 technologies tends to overemphasise the positive impact and transformational capabilities of digital technologies while there is little focus on evaluating potential risks associated with their adoption in industrial operations. An understanding of how supply chain risks are perceived in digitalisation projects within industrial operations and an understanding of decision-makers' responses to different types of risks has important managerial implications. Current literature, however, lacks systematic empirical evidence on the implementation of I4.0 applications and related risk factors. This study aims to address this research gap by exploring the relationship between I4.0 technologies and supply chain risks based on empirical evidence from 300 case studies of industrial practice in Germany and fifty-three interviews with relevant managers from selected use cases and with general experts in this field. Our findings show that digital technologies are frequently adopted to address certain existing supply chain risks but that their implementation introduces new sources of risks (e.g. cyber risks). Based on qualitative data analysis and drawing on Normal Accident Theory, we propose a framework to explicate the drivers and contingency factors of new sources of supply chain risks in the context of Industry 4.0 technologies. Practical recommendations are provided for supply chain managers to guide the process of managing supply chain risks based on the technological life cycle.

1. Introduction

New technologies, such as mobile applications, the Internet of Things (IoT), cloud services and artificial intelligence, are increasingly being adopted by industry to facilitate operations and supply chain processes. Digitalisation is driving a process of transformation into digital supply chains and smart industrial operations (Ivanov et al., 2019). This global trend is often viewed as part of the progression towards Industry 4.0 (I4.0), an idealised vision of future industrial manufacturing. A wide variety of technology components, also called I4.0 technologies, such as cyber-physical systems, IoT applications and cloud computing, which integrate virtual space with the physical world, form the basis of this concept (Xu et al., 2018). The main benefits promised by I4.0 and other similar initiatives include productivity gains, smaller environmental footprints, higher efficiency, lower costs, greater robustness and flexibility, higher quality and shorter time-to-market (McKinsey Digital, 2015; World Economic Forum, 2017). As events in the past few years have shown, however, these technologies are also accompanied by the emergence of new risks, such as data security or cyber risks. In 2015, for instance, hackers not only halted biscuit production at a Canadian factory but also made its complete renovation necessary because of dried dough in the pipes (Ries, 2015). Another example relates to radio frequency identification (RFID) technology: substantial investments were made in the early 2000s to implement RFID technology in industry but environmental factors (e.g. humidity, nearby metals) impeded the 100 % identification required, adversely affecting logistics performance and, consequently, return on investment (Bolić et al., 2010). These examples show that the implementation of digital technologies can render

* Corresponding author. Am Brühlbach 9, 72336, Balingen, Germany.
E-mail addresses: melanie.kessler@rwth-aachen.de (M. Kessler), julia.arlinghaus@ovgu.de (J.C. Arlinghaus), e.rosca@rug.nl (E. Rosca), m.zimmermann@funk-gruppe.de (M. Zimmermann).

https://doi.org/10.1016/j.ijpe.2021.108323
Received 11 February 2021; Received in revised form 24 August 2021; Accepted 4 October 2021
Available online 12 October 2021

industrial operations more vulnerable to a variety of risks and disruptions that are highly relevant to supply chains.

Literature on supply chain risk management (SCRM) provides numerous frameworks and models for types and sources of risks as well as mitigation strategies, yet little is known about supply chain risks in the I4.0 technology landscape (Hahn, 2019). Moreover, current literature on I4.0 technologies tends to overemphasise the positive impact and transformational capabilities of digital technology while underestimating the potential risks associated with its implementation (Flyverbom et al., 2019). Therefore, there is a strong need for a systematic understanding of supply chain risks driven by digital technologies (Tupa et al., 2017; Birkel et al., 2019) in order to mitigate and minimise new sources of risks in operations management (Ivanov and Dolgui, 2020).

Subsequently, this study aims to answer the following research question: *How does the adoption of I4.0 technologies alter the supply chain risk profile in industrial operations and what is the role of the technological life cycle?* Drawing on extensive analysis of 300 case studies of I4.0 technologies used in German industry and fifty-three interviews with relevant managers from selected use cases and general experts in the field, this study identifies and classifies sources of risk inherent to I4.0 technologies arising from their adoption in industrial operations. The methodological overview of this study is presented in Fig. 1.

The remainder of this article is structured as follows: Section 2 describes the theoretical background of SCRM, Industry 4.0, its risk implications, and relevant digital technology life cycle (DTLC) models. Section 3 presents the methods employed and provides an overview of the data used. Section 4 presents the findings and is followed by discussion and a conclusion in Section 5.

2. Theoretical background

The aim of this section is to provide an overview of the relevant theoretical constructs. These serve as the foundation for this study and outline the research gap addressed by this study. First, a brief overview of the supply chain risk management literature outlines the lack of frameworks and models to account for I4.0 technologies implementations in industrial operations. Second, an overview of classifications of I4.0 technologies is given. It acts as a foundation for the empirical analysis and provides the basis for linking risks with I4.0 technologies. Third, a systematic identification of studies addressing issues of supply chain risks and digital technologies is conducted in order to synthesise main insights and outline the research gap. In Subsections 2.4 and 2.5, we discuss the theoretical foundations of the study, namely Normal Accident Theory (NAT) and the digital technology life cycle model. The digital technology life cycle approach is adopted in this study to provide a more nuanced view of supply chains risks triggered by the adoption of digital technologies. Subsection 2.6 synthesises main insights and outlines the goal and intended contribution of the study.

2.1. Supply chain risk management (SCRM): the need for an adapted risk management approach toward I4.0 technologies

Several authors have examined different types of supply chain risks over the past years and have developed corresponding categorisations, which are presented in Appendix A. Rao and Goldsby (2009) developed a typological model of SCRM by incorporating risk factors from the literature (environmental factors, industry factors, organisational factors, problem-specific factors, and decision-maker factors) into the standard supply chain framework. Their approach conforms with the work of Ritchie and Marshall (1993), Kersten et al. (2007) and Christopher and Peck (2004), all of whom proposed three groups of risk factors: environmental factors, internal industry/supply chain factors and organisational/corporate factors. Rao and Goldsby (2009) developed a general typological model of risk intended to serve as a guide for structuring and organising future, more specific studies of supply chain risk. Other authors, such as Chopra and Sodhi (2004) and Tang and Tomlin (2008), focus on mitigation strategies and approaches for resilient supply chain design in the context of conventional supply chain risks. Christopher and Peck (2004) identified several risk factors in their research and demonstrated the interplay between supply chain risks and internal corporate risks within the supply chain as a whole. Tummala and Schoenherr (2011) compiled categories of common supply chain risks (e.g. disruption risks) and corresponding triggers (natural disasters, terrorism and wars) from prior studies.

The phases of risk management comprise three basic activities, regardless of the SCRM framework consulted. Although the wording varies from author to author, these successive phases are essentially (1) risk identification/determination, (2) risk evaluation/assessment and (3) appropriate risk mitigation/control. The initial phase of risk identification/determination is often considered the most important since it lays the foundation for all subsequent risk management activities. It involves comprehensively screening and understanding the current risk situation in order to identify all potential risks and determine which are relevant for further assessment and mitigation. The wide and fast adoption of digital technologies changes the setting and character of industrial operations. Therefore, current frameworks and models for traditional supply chain risks may be insufficient to fully explain the changes brought about by digital transformation. There is a strong need for research and development towards an adapted risk management approach for I4.0 technologies in industrial operations.

2.2. Industry 4.0 technologies: what are they?

While most studies discuss individual technologies and applications under the umbrella of I4.0, a systematic classification is needed to facilitate the development of a risk profile per technology group rather than individual technologies. The literature includes several attempts to synthesise and classify current I4.0 technologies. Some studies applied higher-order technology concepts (e.g. automation and machine-to-machine communication) as criteria for developing typologies, while others employed abstract ideas (e.g. horizontal/vertical integration and predictive maintenance), linking them with specific sets of hardware and software technologies required for implementation. More specifically, Schlüter and Hetterscheid (2017) comprehensively evaluated the recent literature to list relevant I4.0 technologies. They defined thirty criteria for I4.0 technologies and clustered them into fifteen higher-order technology groups, such as augmented reality, machine-to-machine communication or smart factory. For example, wearable is a higher-order technology group which consists of two technologies: data glasses and sensor gloves. Furthermore, Alcácer and Cruz-Machado, 2019 derived nine technological pillars from their analysis of recent literature on I4.0. The pillars represent higher-order concepts of technology-based solutions that are essential components of the I4.0 paradigm. Similarly, Rüssmann et al. (2015) proposed nine foundational technologies, i.e. nine pillars of technological advancement, which constitute the foundation of I4.0. In their study, Oztemel and Gursev (2018) analysed headings, abstracts and keywords of publications about I4.0 to create a hands-on library on the subject for both academics and industry practitioners. The authors identified ten basic components of I4.0 that serve as technological enablers of the paradigm. Altogether, these studies are valuable efforts to systematise the use of I4.0 technologies and related terminology. This is essential for ensuring research continuity in this field.

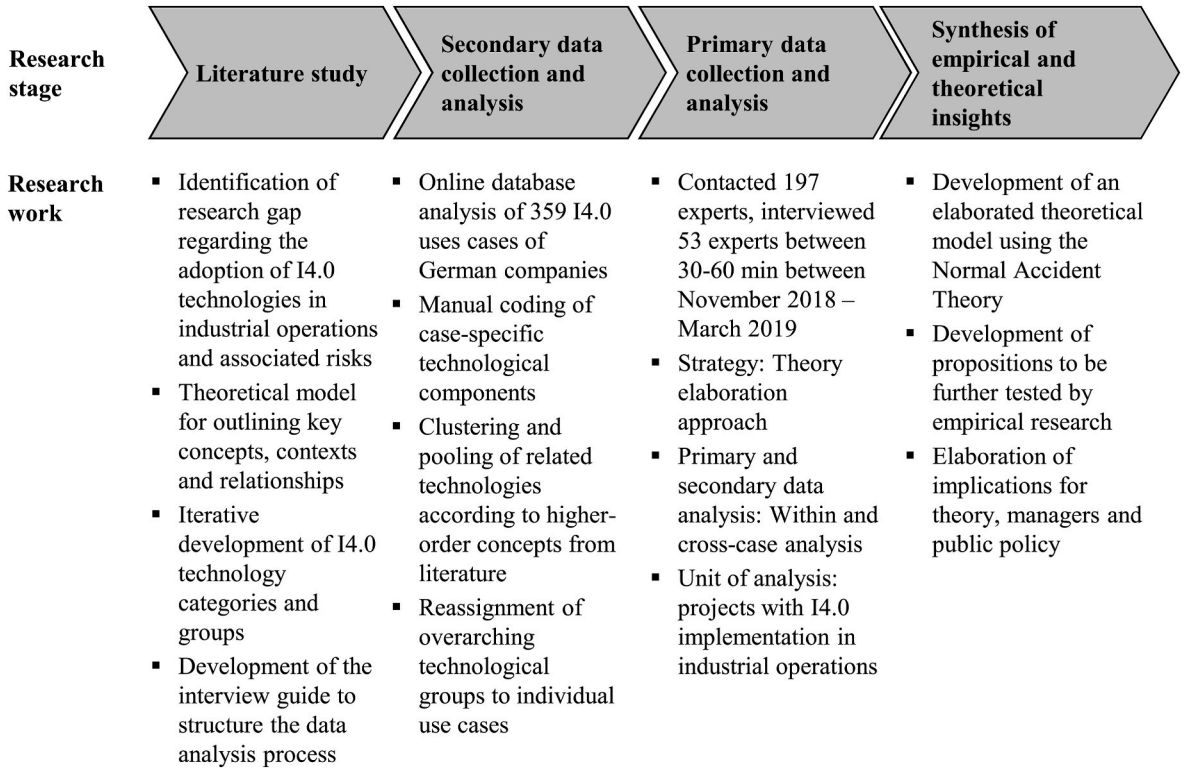


Fig. 1. Methodological overview.

2.3. SCRM in the context of industry 4.0: an important research gap

Relevant studies in the area of SCRM for I4.0 technologies applications have been identified through a systematic approach. Table 1 provides an overview of the investigated relevant studies.[1] The analysis of current studies shows that a systematic analysis of risk management practices for I4.0 technologies implementation based on empirical data is missing.

While the actual range and magnitude of benefits has been discussed frequently in the literature (e.g. Müller et al. (2018); Schmidt et al. (2015)), researchers have only recently begun raising questions about new risk factors accompanying the use of the I4.0 technologies introduced. Brocal et al. (2019), for instance, dealt with the risks of I4.0 in the current operational context and designate organisational and human factors as fundamental risks. Hertel (2015) emphasised potential technical risks in smart factories and proposed a classification model that distinguishes between cyberattacks and errors. Attacks in this context comprise malicious intentional and unintentional threats, e.g. hacking or phishing mails, while errors include human, technical or organisational failure as well as force majeure.

Based on recent literature on digitalisation applications in supply chain management (SCM), Ivanov et al. (2019) studied the influence of digitalisation and I4.0 on the ripple effect and disruption risk control analytics in the supply chain. While focusing on the opportunities of certain digitalisation applications in SCM, the authors expounded the simultaneously arising challenges and risk themes. Predictive analytics, for instance, can increase demand forecast quality or supply chain visibility but simultaneously raise challenges related to data safety or coordination complexity. Several studies have explored more specific issues subsumed by I4.0 technologies and associated risk factors. Rossmann et al., 2017, for instance, examined the future and the social impact of the use of big data analytics in SCM in general. They emphasised common cyber security risk, such as poor validity and quality of shared data and data tampering. Moreover, some authors have focused on certain industries to ascertain the risks of big data in specific areas of application. Guha & Kumar (2018), for instance, posited that big data applications in healthcare supply chains cause data security risks as well as increased implementation costs and hidden problems and costs even after projects have concluded. The authors identified privacy concerns and related legal issues as major risk factors and obstacles to big data applications. Overall, the current literature focuses on potential risks associated with the ultimate concept of I4.0 in several specific sectors using illustrative cases. Moreover, none of the literature examines the changing risk situation in companies that are introducing I4.0 applications.

2.4. Normal accident theory (NAT)

Various theories have been applied in the SCRM literature, with the most frequently used ones being transaction cost economics, agency theory, system theory and institutional theory (Fan and Stevenson, 2018). The incorporation of behavioural theories and models into the supply chain risks literature is an emerging and novel topic of study (Pournader et al., 2020; Arlinghaus et al., 2020; Bendul and Knollmann, 2016). While the application of theories can significantly enhance supply chain risk conceptualisations, SCRM research has not fully taken advantage of the existing body of theories (Pournader et al., 2020; Fan and Stevenson, 2018). These theories have been used to inform the conceptualisation of supply chain risks and inter-relationships among risk types, but also to guide hypotheses development and testing regarding capabilities, resources and mechanisms needed to identify, manage and mitigate supply chain risks (Fan and Stevenson, 2018).

The focus of this study is to understand how the adoption of digital

[1] To identify the relevant literature, we used the two search engines of Business Source Complete (EBSCOhost) and Web of Science. Therefore, we combined the terms 'risk', 'Industry 4.0', 'supply chain' and 'supply chain risk management' as search strings for the title, abstract and keywords. We investigated the identified papers and focused on articles which address specific I4.0 risks.

Table 1
Overview of risk factors relevant to I4.0 technologies: Synthesis of relevant studies.

Study	Approach	Technology focus	Risks
Brocal et al. (2019)	Literature review	Human-machine interaction, human-interaction	Accident risks, psychosocial and musculoskeletal risks, increased complexity and unpredictability of robot tasks, increased complexity in distributed instances
Hertel 2015	Literature review, case studies	Unspecified - smart factory	Cyberattacks (intentional and unintentional), errors (human, technical, organisational, force majeure)
Birkel et al. (2019)	Literature review, interviews with experts	Unspecified – Industry 4.0	Economic, ecological, social, technical/IT, legal/political
Ivanov (2018)	Literature review	Big data, Industry 4.0 (IoT, smart products, robotics, augmented and virtual reality), additive manufacturing, advanced tracking and tracing technologies	Aggravation of the ripple effect, increase in coordination complexity, data safety issues, information disruption risk
Roßmann (2017)	Delphi study, fuzzy c-means clustering	Big data, big data analytics	Risk of poor validity and quality of shared data, data tampering, data security, reduced necessity of human interaction, risk of interorganisational conflicts, synchronisation throughout the supply chain impeded by different technology readiness levels among partners
Guha (2017)	Literature review	Big data, especially applications for cloud computing, IoT/smart city, predictive manufacturing, 3D printing, smart healthcare	Data security, high implementation costs, hidden problems and costs after completion of projects, lack of technological knowledge
Fosso Wamba et al., 2015	Literature review, case study analysis	Big data, big data analytics	Inferior and/or poor quality of data, inappropriate data, waste of organisational resources, careless handling of personal and organisational privacy; challenges mentioned: data policies, technology and techniques, organisational change, access to data, industry structures

technologies influences the internal structure and decision making inside a company. To inform the conceptualisation of supply chain risks and inter-relationships with other system parameters, NAT has been chosen as a theoretical foundation. This theory has been previously used in a few supply chain risk studies to understand disruptions (e.g. Scheibe and Blackhurst, 2018; Bendul and Skorna, 2016; Skilton and Robinson, 2009). NAT focuses on the system conditions and how they are influenced by external parameters, for instance, through the implementation of new technology. Therefore, NAT is used in this study to inform the understanding of risk and the influence of external drivers, such as the adoption of a digital technology. NAT holds that a system's complexity and its tightly coupled processes increase the likelihood of failures (Perrow, 1999). Complexity can be defined broadly as 'the sum of information required to entirely describe the system' (Cohen and Stewart, 1994). Supply chain complexity is the product of the number of suppliers, differentiation of suppliers and the level of interrelationship between suppliers (Skilton and Robinson, 2009; Choi and Krause, 2006). Coupling of system components comprises the number of variables shared among subsystems and the strength of the coupling (Weick, 1976). Tight coupling of system components determines the ease with which disruptions spread across the entire system (Marley et al., 2014). NAT holds that even small disturbances can cause major disruptions in operations and affect the entire supply chain's functionality (Bendul and Skorna, 2016).

2.5. Digital technology life cycle

The understanding, identification and mitigation of supply chain risks is closely linked with the stages of the technological life cycle. The digital technology life cycle approach is adopted in this study to provide a more nuanced view of supply chain risks triggered by the adoption of digital technologies. This is important because several risks may present strong manifestations during the implementation stage (e.g. employee resistance) but can be more easily addressed during later operational stages. The technology life cycle model serves as a guide to map interrelationships between supply chains risks occurring at different stages of technology implementation.

The literature provides numerous life cycle models for various technologies. All of them describe the readiness level at different stages over time (Jamnia, 2018; Project management institute, 2017). The standard life cycle consists of four stages: introduction, growth, maturity/stabilisation and saturation/decline (Levitt, 1965; Anderson and Zeithaml, 1984). These stages follow one another in chronological order and describe a technology's interaction with its environment, for instance. One common approach depicts a product's market life cycle over time in terms of performance indicators, such as sales, revenue, profit and number of customers. The view of the life cycle varies depending on the perspective and motivation (Stark, 2015). The industrial product life cycle and the technology life cycle, for instance, address the perspective of manufacturers of (technology) products. Both concepts thus focus on processes related to the research and development, manufacture, sales, after-sales and disposal of technology products (Saaksvuori and Immonen, 2008). Variations such as the market-driven product life cycle, however, are concerned with the use and adoption of such technologies by users and operators in their own manufacturing processes. The generic project life cycle similarly comprises the essential phases of corporate projects by introducing sequential stages. Even though projects vary in content, size and complexity, a typical project can be mapped to the life cycle structure.

Companies usually initiate a project to introduce I4.0 technologies. The market-driven product life cycle and the project life cycle can be combined into a digital technology life cycle (DTLC) that describes the subsequent stages of a technology's life cycle in a company in order to identify the risk factors relevant to the implementation and operation of I4.0 technologies. Fig. 2 presents the proposed DTLC model with its different phases.

The DTLC based on the market-driven product life cycle also consists of the four stages of introduction, growth, maturity/stabilisation and disposal/replacement during the two relevant technology implementation project phases, i.e. implementation and operation (Levitt, 1965; Anderson and Zeithaml, 1984). A technology is initially implemented in its area of application in the introduction stage. The growth stage includes the transition from the implementation phase to the operation phase, and thus upscaling, through operational optimisation and adaptation by employees. Once the maturity/stabilisation stage has been reached, the technology is established in its area of application and its usability and efficiency remain largely constant (Taylor and Taylor,

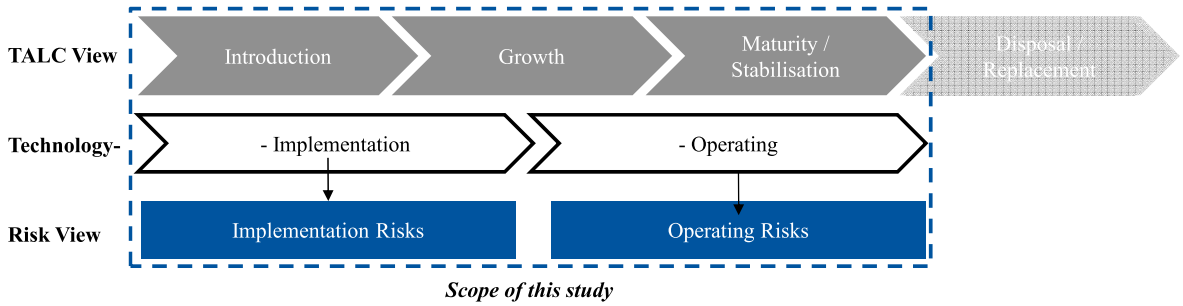


Fig. 2. Scope of this study in the DTLC framework.

2012). After transitioning to the stage of disposal/replacement, the technology is done away with or replaced.

2.6. Research gap and theoretical model guiding the empirical investigation

Current literature grounded in conceptual arguments suggests that I4.0 technologies curtail exposure to certain risks and introduce new risk sources (Ivanov et al., 2019). A synthesis of main concepts, main relationships and scope of the study is presented in Fig. 3. This theoretical model has guided the empirical investigation. While the supply chain risk management literature and the technology life cycle literature provide an analytical basis for the external and decision-making-specific risk factors, NAT provides a foundation for understanding the problem-specific context through the lens of two constructs: system complexity and its tightly coupled processes (Perrow, 1999). These two constructs are important to further advance the understanding of risks posed by digital technologies because previous studies have shown that digital technologies can increase process complexity and enable tighter integration of value chain processes across functions and company boundaries (Ivanov et al., 2019; Hanelt et al., 2020). Regarding the research gap, most studies address these aspects conceptually or focus on specific technologies and applications (e.g. big data in healthcare) and lack exhaustive empirical evidence (Guha & Kumar, 2018). Current models and frameworks for supply chain risks fail to explain the phenomena of I4.0 technologies adequately because they depict major transformation capability across an entire organisation. Digital technologies diffuse across entire organisations and their supply chains, triggering organisational changes that are distinct from previous changes related to information technology (Hanelt et al., 2020). Since the rapid diffusion of digital technologies is changing the empirical reality, established models of supply chain risks need to be revisited (Busse et al., 2017). Empirical studies are needed to expand and theorise new frameworks and models. This study addresses this research gap with an empirical analysis of case studies of I4.0 technology implementation in German industrial operations.

3. Methodology

This study explores risk factors and their relationships to digital technologies used in industrial operations. Since this constitutes a novel empirical context, the study at hand adopts a theory elaboration approach that employs an existing theory to explore the new empirical context and to develop testable hypotheses (Ketokivi and Choi, 2014).

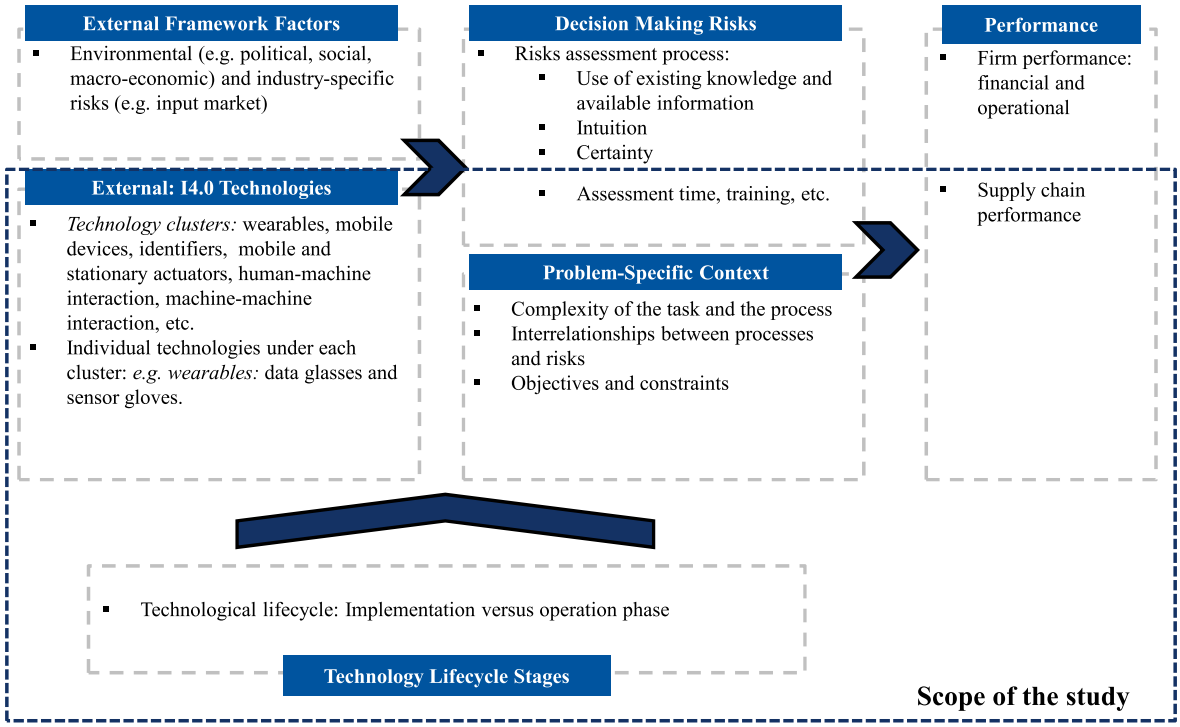


Fig. 3. Theoretical model: Main variables and relationships (based on Rao and Goldsby, 2009; Tazelaar and Snijder, 2013 and other insights from the theoretical background).

Guided by this theory elaboration approach, we employ a five-step approach in our study that is described in the following subsections.

3.1. Use cases: selection, data collection and data analysis

First, we analyse a comprehensive online database with 300 I4.0 use cases, shedding light on which technologies actually are currently in commercial use and thus relevant to state-of-the-art industrial practice. Second, we conduct interviews with experts in order to explore the risks associated with the use of the identified I4.0 technologies in practice. Third, we ascertain risk themes of the different DTLC phases that emerge from the interviews with experts. Fourth, we link these risk themes of I4.0 technologies with established SCRM risk categories from the literature in order to identify interdependences between I4.0 technologies and SCRM. In the final step of our study, we synthesise the findings by identifying patterns emerging from the data across use cases in order to develop hypotheses. Drawing on the principles of abductive reasoning, our empirical research is guided by a systematic iteration between theory and empirical data (Ketokivi and Choi, 2014). The specific projects in which a digital I4.0 technology has been applied in industrial operations are the unit of analysis in this study.

3.1.1. Selection of use cases: 'Plattform Industrie 4.0' online database

A multiple case study design has been employed in this paper to study the underlying technologies of I4.0 solutions empirically. To this end, this study initially draws on insights from 300 I4.0 use cases in Germany taken from the 'Plattform Industrie 4.0', created and managed by the German Federal Ministry for Economic Affairs and Energy in collaboration with the Federal Ministry of Education and Research (Federal Ministry for Economic Affairs and Energy and Federal Ministry of Education and Research, 2019). This platform was launched by the German government with the objective of sharing knowledge and best practices for I4.0 project implementation in German companies. The database is reliable and valid as it was launched and is maintained by an official government institution, and companies voluntarily share their best practices and insights related to I4.0. Moreover, there is a verification process prior to the publication on the website which ensures that the necessary data are included, that data are reliable, that the cases are I4.0-specific and that there are no hidden goals (e.g. it is not allowed to make concealed sales offerings). It provides standardised categories with present data field options for each case, specifically company size, region, examples of products, value creation, examples of applications and development stage. Moreover, several guiding questions are answered for each project. These questions include targeted benefits, technologies applied, approach adopted and lessons learned. This database was selected for several reasons. First, the use cases on the platform represent the current state-of-the-art of I4.0 implementation in Germany. Second, the database is comprehensive and representative since it includes projects from every region of Germany, different types of companies and industries, and the different applications and technologies employed.

By drawing on a large number of use cases, this study can develop empirical insights into technology components relevant to the implementation and operation of I4.0 solutions. Several use cases from the initial database of 359 were eliminated from this study because they lacked key information about the technologies applied. We eventually drew on a final data set of 300 use cases with complete information for further investigation. The data set has several descriptive characteristics. First, the majority of use cases are located in Baden-Württemberg, North Rhine-Westphalia, Bavaria and Lower Saxony – Germany's four largest federal states and industrial regions. Second, as Fig. 4 shows, a large share of the participating companies on the platform are small and medium-sized businesses (SMB, 1–250 employees), just as the vast majority of German businesses are. Each of the three other company size categories (250–5000, 5000–15000, >15000 employees) account for approximately 20 % apiece. Altogether, the database is representative of German industry and valuable because it covers all company sizes and different industries and is not limited to certain technologies or areas of application.

3.1.2. Use case analysis based on secondary information

A Web crawler was used to gather all information available on each

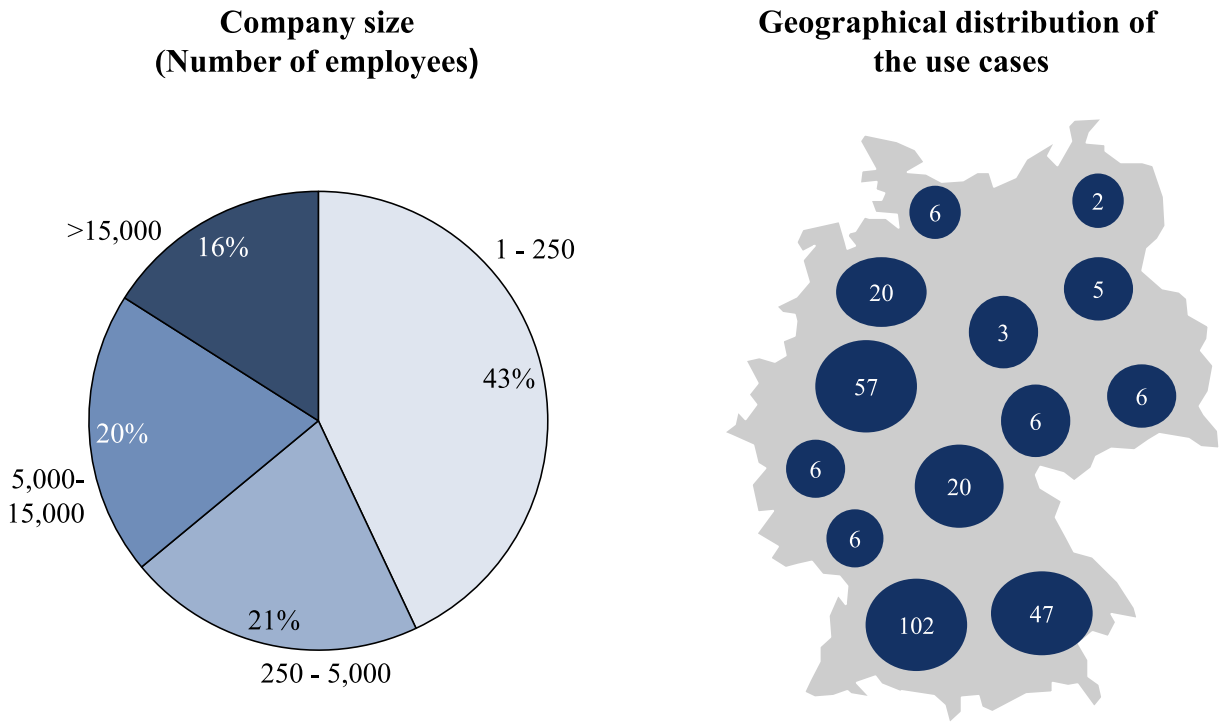


Fig. 4. Descriptive statistics of the online database, N = 300 (Federal Ministry for Economic Affairs and Energy and Federal Ministry of Education and Research, 2019).

case in an Excel file. Next, the information on all 300 use cases was screened using the five or fewer answer text blocks and the default filter categories. The third step entailed extensively coding the individual case data sets manually to record the I4.0 technologies applied. An overview of twelve higher-order technology groups, which covers all technology components relevant to I4.0, was developed based on Schlüter and Hetterscheid (2017), Oztemel and Gursev (2018) and Alcácer and Cruz-Machado's (2018) comprehensive studies of different I4.0 key technologies. This was used to assign as many as four of the technologies employed in the solution described to each of the use cases. The fourth step involved pooling of all the technologies from the bottom up, following corresponding higher-order constructs from the literature. In the final step, the higher-order constructs were reassigned to the individual use cases, thus rendering them comparable and establishing a basis for exploring overarching themes of the relationships between I4.0 technologies and risks.

This bottom-up approach was chosen for several reasons. First, it makes the broad range of technology components and the size of the overall database manageable without losing track of the variety of technology. Second, analysing groups of technologies instead of individual technologies makes it possible to transfer this study's findings to future technologies too. New generations of smart clothes, for instance, will still fit in the wearables technology group, based on their technical features. The insights gleaned from this study will thus be transferable to that specific new technology based on its technology grouping. Moreover, technology pooling reveals the overarching and thus most relevant risk factors of I4.0. Table 2 provides an overview of the technology groups and examples of the underlying technology components.

3.1.3. Interviews with experts: selection, procedure and data analysis

Following extensive analysis of the data from the online platform, in-depth interviews were conducted with practitioners involved in the use cases from the online database and with additional experts on digitalisation and I4.0 from business and academia. Interviewing practitioners from the database cases also enables us to verify and enhance the information on solution approaches and technologies from our secondary data. Interviewing general experts on digitalisation and I4.0 provides an additional and broader look at specific technologies' impact on risk situations. All interviews were conducted in German by phone or face-to-face between November 2018 and March 2019. Interviewees were selected based on their past or present involvement in I4.0 projects. Along with the contacts from the online database, potential interviewees were approached at conferences related to I4.0 or found through personal contacts from earlier projects in the field. We anonymised individual information, e.g. names of interviewees and companies and specific attributes, for reasons of confidentiality. We were able to conduct fifty-three of the 197 interviews that we had requested, resulting in a total response rate of 27 %. All interviews were recorded, transcribed or extensively summarised (whenever interviewees did not agree to being recorded). The robust project selection strategy employed covered a wide range of organisational attributes in order to ensure representativeness and facilitate analytical generalisations (Eisenhardt, 1989).

Twenty-two interviewees work for companies classifiable as SMBs with up to 250 employees. We placed special emphasis on this group in our sample since SMBs are particularly relevant to the national economy in Germany in general and to the field of I4.0 in particular. Seventeen interviewees work for companies with 250–5000 employees, six for companies with 5000–15000 and eight for large companies with over 15000. Nineteen interviewees represent companies in the manufacturing sector, comprised of such subsectors as electrical and electronics manufacturing, automotive manufacturing, equipment manufacturing and automation equipment manufacturing. In addition, twelve interviewees work in industrial consulting and provide an outside view of I4.0 projects in various companies. Moreover, nine IT companies, eight logistics companies and five representatives of academia are involved. The heterogeneity of our sample permits overarching insights and prevents potential adverse effects from sample distortion. Fig. 5 visualises the composition of our set of interviewees in terms of company size and industry.

The main goal of the interviews was to identify risks associated with applying and operating the technology solutions that we identified by evaluating the online database. Table 3 provides some examples of interviewees and their backgrounds.

Interviews lasted between twenty-five and 50 min and followed a semi-structured approach, which allows gathering data in a structured way while maintaining the necessary openness to include additional and unexpected information. The questionnaire consists of three main sections. In the first section, the interviewees describe their company's I4.0 use case, specifically naming all relevant basic technologies, their areas of application, their functionalities and the desired goals. The second and main section of the questionnaire incorporates the DTLC devised in section 2.4 and surveys potential types of risks. This overview, compiled from the literature presented in sub-sections 2.1, 2.2 and 2.3 combines the established risk categories of SCRM with those of I4.0. The overview thus comprises adaptation risks, the established SCRM framework factors of environmental, industry and corporate risks, and technical risks of errors and cyberattacks (Rao and Goldsby, 2009; Hertel, 2015). This ensures that interviewees cover and consider as many recent risks as possible while analysing their use cases. Interviewees could either assign actual risks from their own experiences to an existing category or add risk factors to the categories provided. The complete translated questionnaire can be found in Appendix C.

3.2. Data analysis strategy

The data analysis strategy followed an iterative dialogue between theory and data (Ragin, 1994). The overall empirical investigation was guided by theory in several ways. The analysis of cases from the online database used established theoretical concepts from risk management and I4.0 higher-order technologies as codes, while the interview guide used for primary data collection is based on the theoretical background. The steps undertaken for primary and secondary data collection and analysis are presented in Fig. 6.

The combination of primary and secondary data enables us to conduct a within-case analysis where each case or project was evaluated based on a number of criteria (e.g. technology, implementation stage, risk) and a cross-case analysis was performed to identify emerging patterns (Miles and Huberman, 1994). Combining primary and secondary data on different projects and digital technologies employed in industrial operations enabled us to develop two deliverables. First, we proposed a typology of risks relevant to digital applications in industrial operations. This overview of technologies that are relevant in practice together with associated risks during the implementation phase and the ongoing operation phase can be found in (Appendix D: Risk Table). These risk patterns are explored by deriving 2nd order risk themes from 1st order risk factors from the interviews conducted (see Appendix E for

Table 2
Technology groups with examples.

Technology components	Technology groups
AGV, UAV …	Mobile actuators
Industrial robot …	Stationary actuators
Temperature sensor, humidity sensor …	Sensors
RFID/NFC, QR-Code …	Identifiers
Smartphone, handheld …	Mobile devices
Data glasses, data gloves …	Wearables
Touchpad, motion capture …	Human-machine interfaces
Bluetooth/BLE, WLAN, 3G …	Machine-machine interfaces
Private/public cloud …	Cloud computing
ERPS, MES, dashboards …	Software solutions
Analytics, data mining …	(Big) data
Selective laser sintering …	Additive manufacturing

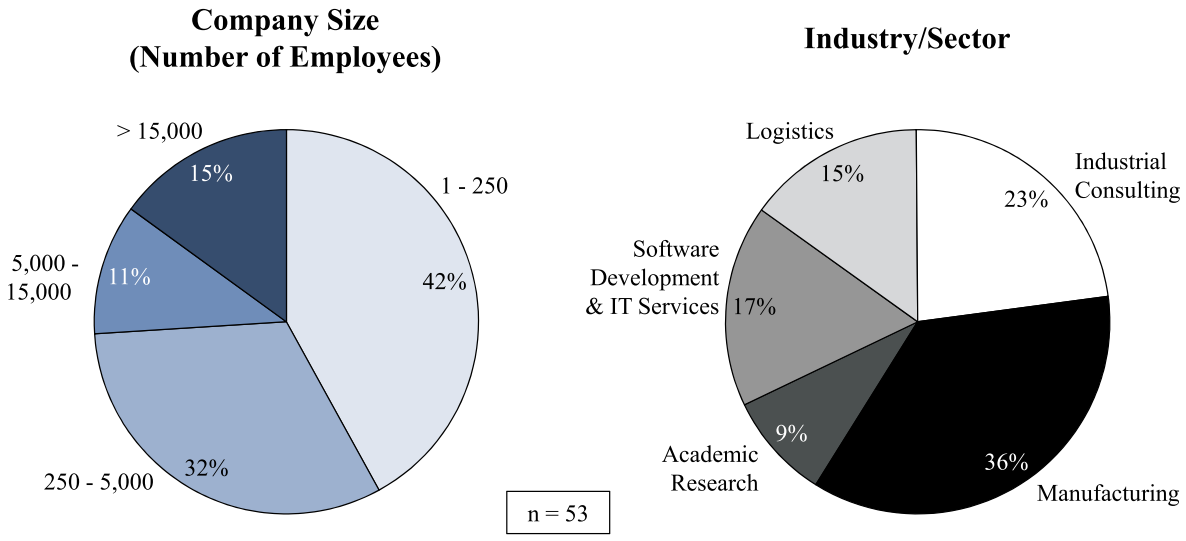


Fig. 5. Interviewees' company sizes and industries, N = 53.

Table 3
Examples of interviewees.

	Position	Industry/ Company	Company Size	Technologies
1	Head of Engineering and Robotics Division	Metalworking	250–5000	Industrial robots, WLAN
2	Chief executive officer	Software development	1–250	AGV, identifiers
3	Project manager and support	Steel industry	>15000	Wearables, Bluetooth
4	Head of IT manufacturing and internal logistics	Automotive industry	5000–15000	Apps, sensors, Bluetooth
5	Chief technical officer	IT infrastructure development	1–250	Data glasses, WLAN
…				
53	IoT risk analyst	Industrial consulting	250–5000	UAV, 4G

the data structure). The distinction between technology users and vendors emerging from the risk analysis constitutes an important aspect of I4.0 technologies. Together with the data from the interviews, several contextual factors were developed which are characteristics of I4.0 technologies.

In a second step, this study explored the shifting role of risks in the different phases of introduction, growth and maturity. The emerging risk themes were linked with established risk classification schemes from the literature, especially Rao and Goldsby's (2009) comprehensive supply chain risk model, in order to embed the results in the general and established field of SCRM. This integrated approach enhanced the validity and reliability of our findings, as suggested by prior studies (Barratt et al., 2011; Carter et al., 2020). Finally, several hypotheses and an elaborated framework combining the insights from the empirical analysis and NAT were proposed. Appendices C, D and E, which are available in the online supplementary materials, provide further evidence and details for the data analysis.

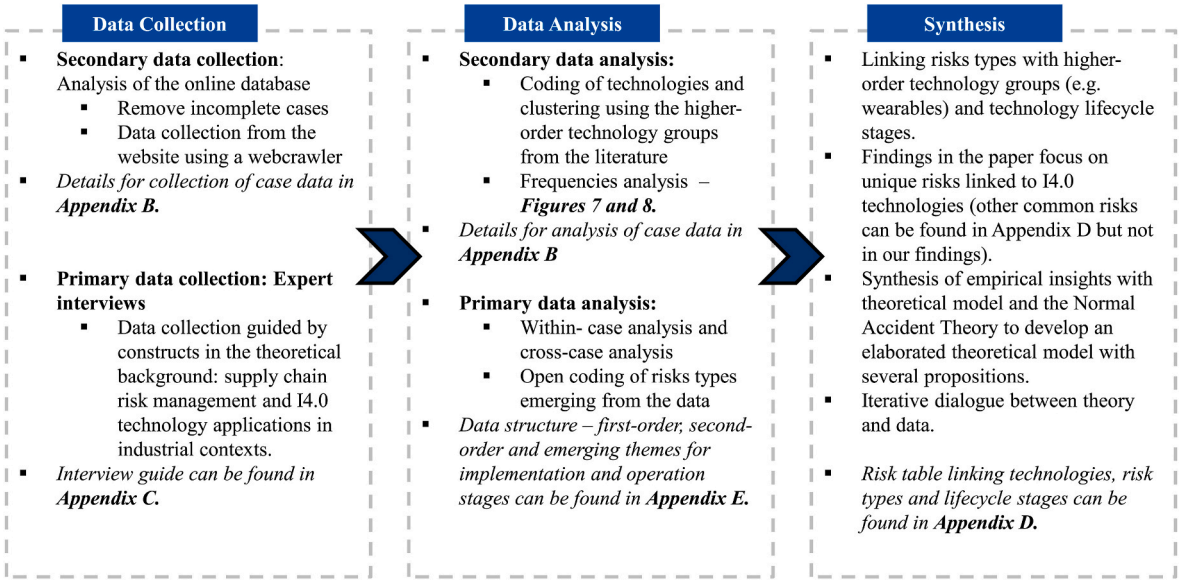


Fig. 6. Data collection and analysis strategy.

3.3. Validity and reliability

By combining the insights from both primary and secondary data, this study incorporates principles of triangulation by building on multiple sources to enhance construct validity (Yin, 2003; Denzin and Lincoln, 2003). In the first step, several internal meetings were held with experts to supplement the insights gained from the literature review, to develop the procedure for the database analysis and to refine an interview guide. Secondary data were collected by Web crawling an online case database and manually coding the collected raw data. Primary data were collected by conducting semi-structured interviews with experts on I4.0, who were involved in I4.0 technology projects from the database. This method assures consistency and comparability of data among the use cases as well as flexibility to pursue information about relevant topics and contextual elements beyond the guiding questions. Moreover, the cross-case approach is an established starting point for theory development that provides a good basis for analytical generalisation (Eisenhardt, 1989). The interviews followed an interview guide developed beforehand, which incorporates insights from desk research of I4.0 technologies, risk categories and life cycle models. Information was crosschecked with interviewees to ensure validity (Denzin and Lincoln, 2003). All interviews were recorded, transcribed and summarised extensively. The study thus adhered to criteria of internal validity, construct validity, external validity and reliability (Gibbert et al., 2008), as shown in Table 4.

Table 4
Components of the research design based on Gibbert et al. (2008).

Methodological criteria	Components	Work performed
Internal validity	• Research framework derived from literature • Pattern matching • Theory triangulation	• The analytical constructs employed draw on theoretical insights from SCRM models, related risk classifications and life cycle models. • Comparison of patterns from different contexts of various use cases and interviews during data collection. • Use of different bodies of literature as research framework and as a tool to interpret findings
Construct validity	• Data triangulation • Review of derived data by peers • Explanation of data analysis	• Combination of primary (original interviews conducted by researchers) and extensive secondary data (archival data from online platform). • Review of drafts and interview recordings by peer academics who are not co-authors of this paper. • Structuring of collected secondary data in a database
External validity	• Multiple case study approach to cross-case analysis • Case study background	• Multiple case studies included in both primary and secondary data. • All the use cases examined (compared) concern the introduction of I4.0 technology but have different backgrounds in terms of company size, industry, areas of application.
Reliability	• Case study protocol • Case study database	• Data collection according to a set of guiding questions following the analytical constructs and project-specific anomalies. • Development of a case study database with all data sources (available documents, interview files, archival data, etc.).

4. Findings

The findings are presented in three sections. First, we argue that digital I.40 technologies are driving the transition to a new industrial landscape and several unique contextual factors therefore govern the emergence of unique risks. Second, we present three major sources of risks unique to the implementation of I.40 in industrial operations. Third, we synthesise our findings and draw on insights from NAT to propose an elaborated framework and several hypotheses on contextual drivers of I.40, unique sources of risks and outcomes.

4.1. New landscape for traditional companies adopting digital technologies

Our data reveal that several contextual factors are driving the transition to a new industrial landscape in which I.40 is implemented: information asymmetries between technology vendors and users and external contextual drivers related to the technology market and the attributes of digital technologies.

First, the case analysis uncovered significant differences in how users and vendors understand I4.0 technologies in terms of risks and intended benefits (see Figs. 7 and 8). Technology vendors are the companies developing and selling digital technologies (e.g. Axoom, Bosch, Siemens), while technology users are all manufacturing and logistics companies in our sample that are using digital technologies for specific industrial operations (e.g. BASF, Kärcher, Pfizer). The content analysis of the 300 use cases delivered several interesting insights. Technology users of all sizes identify increasing complexity, insufficient flexibility and high production system latency as factors currently driving the adoption of digital technologies in industrial operations. Technology vendors do not necessarily view Industry 4.0 as particularly suited to mitigate these challenges. The discrepancy between vendors' and users' view of predictive maintenance and the category 'other' is striking. Both tend to be associated more with various vendor applications than with user applications. Specialised technology experts among vendors are generally more familiar with predictive maintenance than are potential users, especially in smaller companies, as the numbers show. Moreover, users do not necessarily consider predictive maintenance's positive impact on the current risk situation to be critical enough to justify the investments and expenditures required.

Apart from the information asymmetries between the users and vendors, other contextual drivers make the reality of I.40 distinctive from past IT implementation. These contextual drivers include increased dependability, susceptibility to disruptions, digitalisation of individuals (workers and consumers), and increased contextual turbulence and dynamism. The interviews revealed that practitioners are being confronted with the necessity and ongoing advance of industrial digitalisation and many decision-makers are experiencing strong pressure to make use of the technologies available to improve their own business processes and performance. One project manager stated, for instance, that *'Failure isn't an option: There is strong pressure on us to implement the technology because we have spent a lot of money on it.'* At the same time, practitioners from most sectors usually have only rudimentary knowledge of such technologies and have had few points of contact during their daily business to date. This pressure, combined with a lack of knowledge can spawn new risk sources, as one manger explained: *'There's strong pressure from unfocused innovation, and the result is risk factors being ignored.'* A lack of knowledge of technologies and technology markets and uncertainty about the utility or return on investment create hesitancy and anxiety among managers, as another project manager divulged: *'We had had no experience with I4.0 technologies until now. Our first project has shown us the weaknesses of our business processes.'*

Many decision-makers bring up uncertainties about the return on investment and technologies' long-term utility (see Table 5). Even though this financial risk does not threaten a technology's functionality or operations directly, it is a major recurring concern among

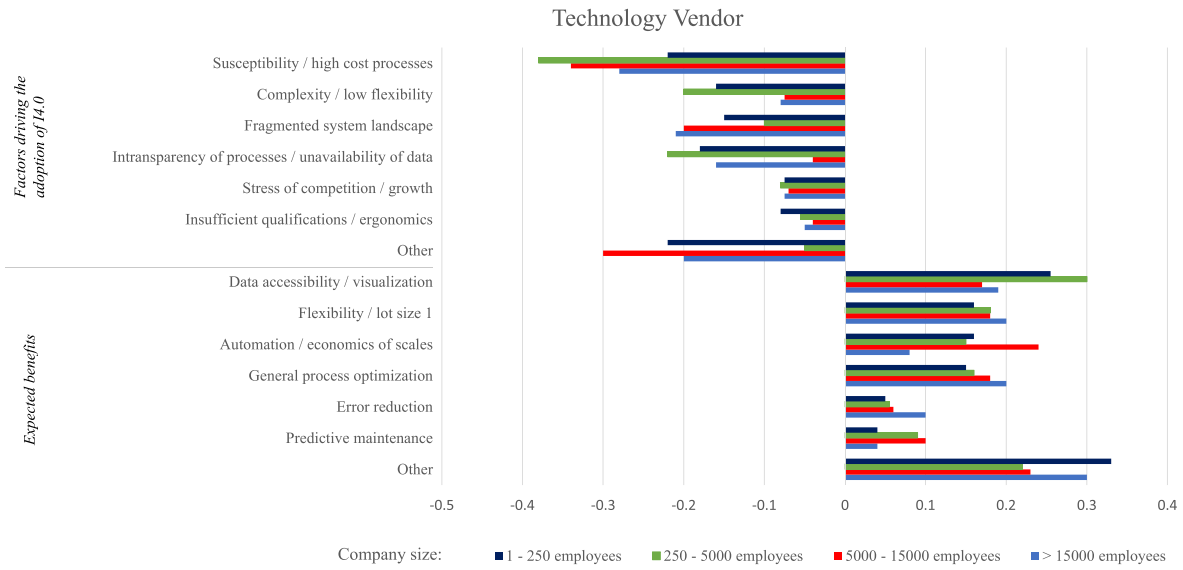


Fig. 7. Drivers of I4.0 technology adoption: technology vendors' responses.

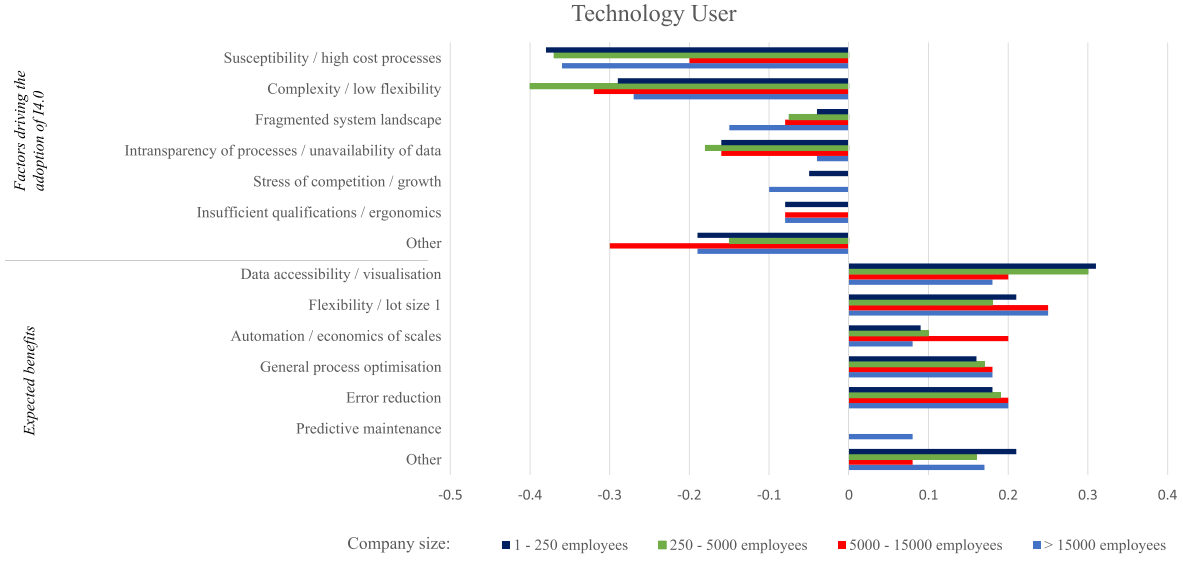


Fig. 8. Drivers of I4.0 technology adoption: technology users' responses.

practitioners during the implementation phase. Once a company commits to a certain technology, the failure und removal of that technology could be a substantial blow to the company. This is especially true for SMBs which have limited financial resources and for disruptive technologies with extensive interdependences with operations. This risk factor is exacerbated by the limited availability of practical experiences or empirical values which could be drawn on for independent study or evaluation. Management consequently exerts great pressure for projects to be implemented quickly and not allowed to fail, which often results in potential risks being overlooked.

The adoption of I4.0 technologies by traditional manufacturing and logistics companies reveals several contextual factors which make this new landscape unique and which relate to discrepancies between users' and vendors' knowledge and the uncertainty surrounding the technology market and the attributes of digital technologies. While uncertainty is relevant for all digital technologies, it is more severe for hardware-heavy solutions (e.g. mobile and stationary actuators, wearables, additive manufacturing) since new technology is expensive (e.g. high R&D costs and low production volumes) and life cycles are short. We therefore propose the following hypothesis:

Hypothesis 1. (H1): I4.0 constitutes a unique context due to several external drivers related to the attributes of digital technologies and uncertainty of the technology market, which is relevant in particular for hardware-heavy solutions, such as mobile and stationary actuators, wearables and additive manufacturing.

4.2. Major sources of risks of I.40 technologies in industrial operations

Content analysis of data from the interviews with experts reveals various sources of risks at different levels of analysis, specifically sources of environmental risks, organisational risks, industry risks, process risks and decision-maker risks (see Appendix E for the data structure and emerging risk categories during the implementation and operation of I4.0 technologies in industrial operations). The emerging risks fall into two categories. The first category includes traditional supply chain risks applicable to many other industrial processes, only the magnitude of which can be affected by digital technologies. Such risks include integration with existing information technology infrastructures and

Table 5
Use cases and quotes illustrating increased uncertainty surrounding I4.0 technologies.

Risk	Technology	Case/Application	Quote
Uncertainty of ROI and long-term value	(Stationary actuators) Industrial robots	Automation of manual machining (cutting, grinding)	*Of course, since a lot of parameters need to be adjusted, there are unexpected costs involved during implementation.*
	(Mobile devices) Smartphone (software solutions) app	Parameterisation and reading of machine data	*A lot of people consider it all to be just 'bells and whistles' at the beginning. And if something doesn't work smoothly at first go, it's ignored.*
	(Stationary actuators) Industrial robot	Automation of manual machining (cutting, grinding)	*For us, there's an investment risk. We're spending all this money on this [application], but you never know whether it's going to pay off or not.*
Technology clusters: All, in particular mobile and stationary actuators, wearables, additive manufacturing.			

processes, general legal issues, operational interferences and resistance from employees. The second category includes risks that change their character in conjunction with digital technologies. Based on our analysis, we propose three sources of specific supply chain risks in conjunction with digital technologies in industrial operations: information asymmetries between technology users and vendors, legal uncertainties surrounding data security, privacy and transparency, and digital transformation at the organisation level.

4.2.1. Information asymmetries between users and vendors

The information asymmetries are most pronounced in two main areas: technology-specific knowledge and technology markets. These two types of information asymmetries create risks of direct and indirect dependence in supply chains. Our data show that a lack of internal expertise increases users' dependence on technology vendors, affecting the number of errors during the implementation phase. Table 6 presents several illustrative examples and quotes from our analysis.

Pressure to adopt I4.0 without sufficient technological expertise creates various risks during the implementation phase. This risk applies in particular for software-based technologies in traditional manufacturing industries with decades of focus on non-digital products and related manufacturing processes. The decision-makers at a steel producer, for instance, were aware of the usefulness of QR codes and scanners for tracking materials in production but lacked thorough knowledge of the technology, its features and its constraints. They consequently encountered many initial problems with unscannable QR codes because of poor lighting or with scanners damaged by the high temperatures in a steel plant's harsh environment. Similarly, many practitioners frequently decide to use cloud solutions to handle customer data, for instance, because of the technology's popularity and prevalence. Those in charge often have no knowledge of the technical risks of cyberattacks or the legal obligations attendant to storing external data.

Much akin to insufficient knowledge of the technology itself, we also found a lack of knowledge of the technology market, which is especially relevant for technologies from fast-moving hardware markets, such as sensors, identifiers, mobile devices, wearables and additive manufacturing. Practitioners often do not have enough market transparency or knowledge available to them to be able to evaluate different proposals, such as price or service level agreements. Lacking similar experience, they are simply unable to assess whether services offered will actually meet their needs. The case of one company that had

Table 6
Use cases and quotes illustrating information asymmetries as a major source of supply chain risk from I4.0 applications.

Risk	Technology	Case/Application	Quote
Insufficient knowledge of I4.0 technology	(Mobile actuators) AGVS	AGVS	*We didn't know enough about the requirements that need to be considered besides the technology itself, such as the requirement of having no ramps in the factory.*
	(Stationary actuators) Industrial robot	Automation of manual material processes (cutting, grinding)	*The lighting was good enough for a human eye but too dark for a camera.*
Technology clusters: Mobile and stationary actuators, human-machine interfaces, cloud computing, software solutions, (big) data.			
Insufficient knowledge of technology markets	(Mobile actuators) AGVS	AGVS	*The CEO was unaware of the complexity of the technology selection.*
	(Wearables) Data gloves	Order picking assistance for employees in warehouse processes	*We bought them from a company we met at a trade fair. We thought it was the only relevant company on the market.*
Technology clusters: Mobile actuators, sensors, identifiers, mobile devices, wearables, additive manufacturing.			
Direct and indirect dependence	(Mobile actuators) AGVS	Internal logistics	*The AGV is hard to replace with an alternative product from a different vendor.*
	(Wearables) Data glasses	Order picking assistance for employees	*If the technology failed, I wouldn't be able to maintain my operations.*
	(Identifiers) QR codes	Material identification in steel production	*Of course I'm growing dependent on the system! If it failed at a technological level, I'd immediately need to implement some sort of plan B.*
	(Stationary actuators) Industrial robot	Automation of manual machining (cutting, grinding)	*Hardly any of the software solution are really open. The controls are often quite different. If you've become accustomed to one specific robot and it's then discontinued, you've got a problem.*
Technology clusters: hardware from small, fast-moving markets (mobile actuators, wearables, identifiers) and complex software-based solutions (human-machine interface, cloud computing, software solutions, big data).			

introduced data gloves exemplifies this. Unfamiliar with potential vendors, the company's decision-makers ultimately chose one they had met at a trade fair, only to become aware of other companies with similar products later on.

Insufficient knowledge of both the technology and the technology market can result in direct dependence on a vendor both for hardware from fast-moving hardware markets and complex software-based solutions. While some technologies, such as tablets or routers, are easily replaced with commercial alternatives without much effort or many drawbacks, numerous solutions require vendor-specific hardware, software and know-how. This makes users directly dependent on the vendor when they need to service or replace hardware components or want to upscale or restructure their operations. The vendor's prices, items in stock, product strategy and market success can affect a technology's availability and functionality for users. Many vendors of I4.0 solutions,

for instance, are small, highly innovative and flexible start-ups operating in highly volatile markets. Should a start-up go out of business or discontinue product lines, users most likely have to abandon or replace their technologies. Moreover, users that have outsourced their digitalisation activities to vendors and have not developed extensive internal expertise over time grow dependent on vendors' know-how and innovativeness in many cases.

Based on the evidence and conclusions presented above, the following hypothesis is proposed:

Hypothesis 2a. (H2a): The information asymmetries between technology vendors and users concerning technologies' functionalities and the technology market lead to direct and indirect dependence on technology vendors and an increase in errors and mishandling.

4.2.2. Legal uncertainty surrounding data security, privacy and transparency

Significant legal uncertainty surrounding data security, privacy and transparency as they relate to I4.0 technologies constitutes a major source of supply chain risk for industrial applications (see Table 7). These issues are generally relevant for technologies which collect, process or handle customer/employee data, namely cloud computing, software solutions or big data. The creation of digital twins of human-machine systems is the biggest driver of legal risks and adaptation problems of many applications. Use cases reveal that practitioners frequently have insufficient knowledge of legal issues, such as data security regulations and employee council issues and liability. SMBs in particular lack the financial resources to hire legal experts, rendering them unable to navigate the complex interrelationships and hidden pitfalls of legal issues and regulations. Some companies in our use cases implemented new, connected machines capable of communicating over the company's own WLAN. While the decision-makers examined all the relevant issues related to cyberattacks and other things, they overlooked the fact that the remote maintenance function requiring encrypted employee data needed to comply with the European Union's General Data Protection Regulation (GDPR).

Table 7
Use cases and quotes illustrating legal uncertainty as a major source of new supply chain risks.

Risk	Technology	Case/Application	Quote
General lack of knowledge of legal issues	(Software solutions) Remote maintenance	Remote maintenance	*We didn't realise we were granting access to employee data by using the remote maintenance function.*
Technology clusters: cloud computing, software solutions, big data.			
Workplace law issues	(Wearables) Data glasses	Order picking assistance for employees	*I'm having problems with the employee council. As soon as you start digitalising, you are allowed to track a CNC lathe but not an employee.*
Technology clusters: sensors, mobile devices, wearables, human-machine interfaces.			
Compliance issues	(Wearables) Data glasses	Order picking assistance for employees	*The first question is always 'where's my data being stored?'.*
	–	Consulting	*Especially smaller companies and start-ups aren't capable of signing a complex data protection agreement. […] They just can't handle it.*
Technology clusters: wearables, cloud computing, software solutions, big data.			
Legal issues	(Sensors)	Automated material requisition for Kanban systems	*The main issue is that of monitoring. We monitor our warehouses with this solution and our workplaces too, of course.*
	(Cloud computing)	Remote maintenance	*You have to be aware of which data you're allowed to store, and which not […] Now, you've got all this data. Who's allowed to do what and when with which data? What happens if the customer wants the data deleted? […]Management is liable for this.*
Technology clusters: cloud computing, software solutions, big data, sensors.			

Legal issues frequently arise during the implementation phase and primarily involve aspects of workplace law, data privacy and data protection. The most common risks in this context are impending conflicts with employee councils that are apprehensive about additional workloads and demands, disadvantages for employees and violations of data privacy. Individual employees in companies without employee councils might raise concerns about labour law themselves, thus delaying or averting the implementation. Monitoring solutions in particular are often suspected of exposing employees and their performance to corporate surveillance or, at the least, of being gateways for potential leaks of employees' personal data.

Moreover, the latest developments in legal policies such as the GDPR frequently have implications that are perceived as a major source of risk. Again, these uncertainties often put SMBs at a disadvantage. The complexity of such regulations is simply overwhelming in practice, making them impossible to implement in their entirety. One company, for instance, agreed with a client upon a particular channel of communication about the information technology system. All the data platforms and cloud storage systems for the use case were so well established that the client expected that all their data would be deleted, but the company was unable to name all the locations where client data were stored whenever established procedures were not followed, e.g. when the client sent an email instead of ordering directly through the system.

Several legal conflicts put technology users at risk during the operation phase. The most common risks arise from collecting, storing and processing either supply chain partner or employee data. Since the legal situation of such activities is constantly changing and promises to remain challenging and uncertain in the near future, practitioners view legal issues as an ongoing risk of many technologies. In several cases, companies have had to guarantee certain security measures and that they are able, for instance, to delete certain types of data completely and promptly upon request. Since many companies fail to address and meet these requirements adequately, they are constantly at risk of lawsuits in the event of related incidents.

Based on the evidence and conclusions presented above, the following hypothesis is proposed:

Hypothesis 2b. (H2b): The legal uncertainty surrounding data security, privacy and transparency as they relate to I4.0 technologies can create new types of legal risks at the organisation level and supply chain level, especially for technologies which collect, process and handle data (cloud computing, big data, software solutions) and for technologies which directly or indirectly monitor employee performance (sensors, mobile devices, wearables, human-machine interaction).

4.2.3. Digital transformation at the organisation level

Our findings reveal that the implementation of I4.0 technologies entails digital transformation at the organisation level and supply chain level, causing significant spillover at different levels of analysis (see Table 8). These spillover effects can be either positive or negative and decision-makers face difficulties mapping them. The increased connectivity and linkages inside and outside the organisation heighten vulnerability to cyber risks.

First, I4.0 technologies require making organisational adjustments to

Table 8
Use cases and quotes illustrating digital organisational transformation as a major source of new supply chain risks.

Risk	Technology	Case/Application	Quote
Organisational transformation	(Stationary actuators) Industrial robot	Automation of manual machining (cutting, grinding)	*You have to take care that the robot doesn't damage its environment during the first runs.*
	(Cloud computing)	Remote maintenance	*The biggest problem is the modification of business processes. You're changing the way your operations work. This is one of the threats. […] We underestimated this back then.*
Technology clusters: software solutions, big data, cloud computing, mobile devices.			
Organisational and supply chain interdependencies	Software solutions	Software for evaluating and ordering transportation services	*Of course they became dependent on you as a company. We contractually obliged our suppliers to use our software.*
	Software solutions	Supplier portal	*You have to be careful about what data is relevant to your business and needs to be hosted by your company to keep your business running. […] It's important for our production planning that we have our article master data in our own system rather than spread across several vendor portals by our clients*
	(Big data) Supply chain data	I4.0 solutions consulting	*I had an interesting project: An OEM and a first-tier supplier were both offering each other a cloud solution for storing all their supply chain data and both of them wanted the other one to subscribe to it. It's normal in supply chains for only one party to dominate and for the other one to become dependent.*
Technology clusters: cloud computing, software solutions, big data.			
Cyber risks	(Sensors)	Automated material requisition for Kanban systems	*The IT department is scared that someone will access the process from outside and that data will be stolen or tampered with in some way.*
	(Mobile devices) Smartphone	Parameterisation and reading of machine data	*Anything wireless is not allowed in the production area. They're afraid of someone hacking the system.*
	(Cloud computing)	Remote maintenance	*Every gateway you open increases your risk of an attack. We use all the available state-of-the-art encryption technologies. But if you look at the hacking of that uranium enrichment facility in Iran, there are always going to be ways and means to access our data if someone really wants to do so.*
Technology clusters: cloud computing, mobile devices, sensors.			

the processes involved. A company that automated its reordering process for C-parts, for instance, had to change the process steps themselves so that the process conformed to the technology's functionalities and requirements. Changing the entry process ultimately caused errors in the subprocesses. Since the numerous interdependences characterising the information technology landscape and the process landscape make them sensitive to external changes and newly introduced elements, the initial introduction of such technologies can compromise the stability and reliability of day-to-day operations. In addition, introducing new processes or modifying existing ones to conform to the technologies employed often causes subsequent interferences related to aperiodic or unexpected events, such as special orders or vendor changes. In several cases, technologies have resulted in an ossification of processes and diminished flexibility – since desired process changes inevitably entail changes in the technology solution too. This increases costs and/or requires technological knowledge that users often do not possess. Organisational transformation and increased supply chain interdependences are driven by technologies which impact the whole organisation (e.g. mobile devices) and collaboration-based software (e.g. big data, cloud computing).

Second, cyber risks emerge as an omnipresent theme from the experts' statements. The most relevant threat identified by the practitioners in the interviews that we conducted is that of corporate data espionage and theft over wireless connections such as WLAN or mobile communications. They consider the probability and severity of such events to be quite low in most cases, though, since they assume that their data would be of little interest to attackers. The cyber risks are linked more to the interconnectedness of assets (IoT) than to the connected technologies themselves. Experts with a greater wealth of experience especially warn as well against unauthorised access to physical facilities through digital interfaces, undetected data tampering and malicious encryption of data by ransomware. The use of common and pervasive mature technologies, such as smartphones with Android OS or iOS, exposes applications to such threats in the form of equally common and pervasive mature malware. In addition, many experts consider most technologies to be enticing and rewarding targets of cyberattacks. This is because the range of vulnerable infrastructure grows along with a company's level of digitalisation. Facilities that were completely 'offline' previously become vulnerable to the new threat of cyberattacks as soon as I4.0 technologies link them to the Internet or a corporate intranet. Many experts see a need to address cyber risks in hitherto unaffected areas.

Based on the evidence and conclusions presented above, the following hypothesis is proposed:

Hypothesis 2c. (H2c): Organisational transformation, increased interdependences among supply chain actors, and cyber risks driven by mainly collaboration-based software increase the likelihood of major disruptions that have a significant impact on the entire supply chain.

4.3. Elaborated framework

The empirical qualitative analysis of use cases and interviews with experts reveals that I4.0 technologies are employed in industrial applications in response to certain existing challenges and risks but that they also create new sources of risks. Based on the empirical findings and drawing on insights from NAT, we propose an elaborated theoretical framework that explicates drivers, contingencies and outcomes of digital technologies in industry while focusing on risk management (see Fig. 9). The proposed framework identifies two groups of drivers aligned with the two analytical dimensions of NAT, e.g. complexity and tight coupling of system components, a series of contingencies, and outcomes found in our empirical data. We conceptualise increased complexity in I4.0 technologies as the interaction between a highly dynamic and uncertain external environment (technology market and attributes of technologies), information asymmetries between technology vendors and users, and legal uncertainties surrounding data security, privacy and transparency. The second driver suggested by NAT relates to the interdependence between system components at both the organisation and the supply chain level. In keeping with NAT's underlying logic that high complexity and tight coupling of processes increase the likelihood of accidents, we link the drivers and contingency factors with several outcomes. We identified several outcomes resulting from procurement risks, specifically an increased probability of occurrence of supply chain risks and disruptions, errors and mishandling; and increased dependence on technology vendors.

Several contingency factors emerging from the data affect the identification and management of sources of risk. These include the technology life cycle stage, technology type, and company size and resources. Different risks arise at different stages of the technology life

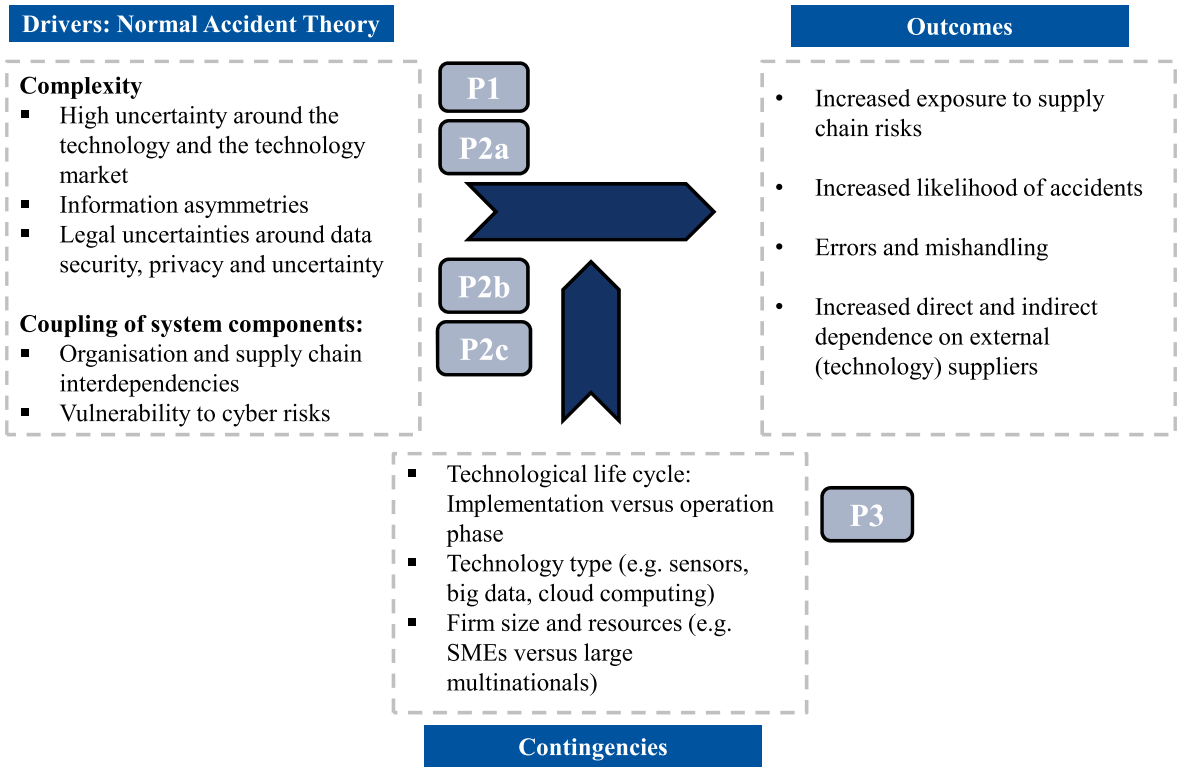


Fig. 9. Elaborated framework: Drivers and contingencies of new sources of supply chain risks of I4.0 digital technologies in industry.

cycle. Our data show that the adverse effects of unaddressed implementation risks grow in the operation phase. We additionally found significant differences between SMBs and larger companies in their perception, identification and management of risks, largely because SMBs' lack of internal resources affect their options significantly. Our analysis of risk factors also shows that sources of risk manifest themselves slightly differently for different types of technologies (see Appendix C). The overview of contingency factors invited the following hypothesis:

Hypothesis 3. (H3): The likelihood of accidents caused by sources of risk from I4.0 technologies is contingent on several factors, specifically company size and resources, technology type and technology life cycle stage.

Fig. 9 presents the elaborated framework with every hypothesis proposed.

5. Discussion and conclusion

The overarching goal of this study is to identify and map risks associated with the implementation and operation of I4.0 technologies. Drawing on NAT and using a unique data set of interviews with experts and 300 case studies, we argue that digital I4.0 technologies are driving the transition to a new external and internal industrial landscape. This landscape is dominated by strong uncertainty about the technology market, the attributes and functionalities of digital technologies and the spillover effects upon organisations and supply chains. Three major risk sources are hypothesised: information asymmetries between technology users and vendors, legal uncertainties and organisational transformation, each predominant for different technology clusters. An elaborated framework is developed and several hypotheses about the drivers and contingencies of risk management in the context of I4.0 technologies are proposed.

5.1. Theoretical contributions

The study makes several important theoretical contributions. First, it provides an exploratory empirical analysis of emerging phenomena. The analysis reveals that the application of I4.0 technologies in industrial operations is unique in several ways and is therefore accompanied by several unique risk sources. Previous studies have demonstrated that the implementation of I4.0 technologies in practice is concomitant with greater connectivity between humans, systems and objects and can create new and modified risks (Tupa et al., 2017). Digital technologies diffuse across entire organisation and their supply chains, triggering organisational changes distinct from earlier changes related to IT (Hanelt et al., 2020). Our study corroborates these findings and expands them with an eye towards supply chain risks linked with technology clusters, showing that greater interdependence at the supply chain level, increased complexity, and digital transformation of organisations and supply chains can create new sources of supply chain risks. This important implication requires further study to gain a more nuanced understanding of the vulnerability at firm and supply chain level brought in by I4.0 adoption, and the required resources and capabilities needed by firms to cope with this. The increased inter-connectedness at both firm and supply chain level needs to be further studied through in-depth investigations and empirical data to evaluate whether the benefits outweigh the risks from the perspective of focal firms and at supply chain level. Moreover, the increased level of complexity, uncertainty around I4.0 technologies as well as increased interconnectivity at firm and supply chain level creates a unique set of challenges for human decision makers. Therefore, an important research direction relates to the incorporation of behavioural theories (Pournader et al., 2020) to understand how this increased complexity impacts the decision-making process (e.g. intuition, use of information, certainty, knowledge) around identifying and assessing supply chain risks for digital technologies.

Second, based on our empirical study, we propose three major risk sources for I4.0 applications: information asymmetries; legal uncertainties surrounding data security and privacy; and interdependences between organisations and supply chains that are relevant for different technology clusters, as shown in the findings. This aligns with earlier literature demonstrating that digital technologies' disruptive effects compel companies to reorganise their internal organisational processes and external supply chains (Porter and Heppelmann, 2014). We also expand on the studies by Guha and Kumar (2017), Fosso et al., (2015), Ivanov et al., (2018) and Rossmann et al., (2017) to start systematically linking supply chain risks with digital technology clusters. The impact as well as suitable mitigation strategies for these novel sources of risks can be further analysed in future studies.

Third, the emerging concept of information asymmetries between technology vendors and technology users as a major source of risk in this context is novel. The underlying idea is in line with Orlikowski's (1992) concept of the duality of technology, i.e. technology development and technology implementation represent distinct processes that therefore require different capabilities to be completed successfully. We demonstrate, however, that the high level of complexity of technology use, functionality and uncertainty about the technology market amplify this duality in the context of I4.0. Understanding the duality of digital technology and the capabilities required by firms to manage technology development and implementation while minimising the gaps and risks between the different stages represents an important avenue for further research.

Lastly, the study has employed Normal Accident Theory (NAT) to conceptualise novel sources of risks triggered by I4.0 technology adoption in industrial operations, thereby expanding the use of this theory in the supply chain risk literature. With this, we contribute to existing literature by employing NAT in a novel context triggered by the use of digital technologies in operations and supply chains. Our findings show that digital technologies aggravate the system complexity through various mechanisms, such as increased uncertainty, information asymmetries, increased direct and indirect dependences on technology suppliers, and emergence of new risks, e.g. cyber risks. Our findings also show that digital technologies, in particular collaborative software solutions, enable tighter integration of value chain processes across functions and company boundaries, but also increase the vulnerability of supply chains by creating stronger interdependences among processes across companies and supply chains. Together, this leads to increasing risk of accidents and therefore dedicated mitigation and prevention strategies need to be developed aligned with the particularities of digital technologies.

5.2. Managerial and public policy implications

Our findings show that companies are facing numerous challenges and are having to deal with a number of risks while they implement current I4.0 technologies. The proposed elaborated framework is intended to help practitioners understand the different types of risks and the ways they arise at the different stages of a technology implementation project. More specifically, our findings present a few implications for managers. First, the study guides managers dealing with I4.0 technologies adoption in industrial operations to distinguish between risks occurring during the development and implementation stages in order to develop nuanced mitigation strategies. Second, managers need to focus on establishing regular knowledge exchange with the technology vendors or to hire internal technology experts in order to reduce the uncertainty and lack of expertise related to I4.0 technologies. Moreover, a better understanding of the technologies can also provide new opportunities for managers. Third, managers need to develop proactive mechanisms to address cyber risks and potential interferences with operations and production processes. For example, there needs to be clear guidelines about what types of devices are allowed for use by employees on the shop-floor or the policy regarding the use of external devices by internal employees. Fourth, managers need to be aware that the adoption of I.40 technologies triggers changes at organisational and supply chain level and specific assessment needs to be performed to evaluate the benefits of increased connectivity versus the risks arising from this new situation.

The study also contains implications for public policy. First, the increased legal uncertainty around the adoption of I.40 creates extra challenges for firms. Governments need to provide extra support regarding the legal aspects related to the implementation of these technologies.

Moreover, our findings show that these risks are especially challenging for SMBs as these often lack a varied set of experts with special know-how for the specific technology. Therefore, our study emphasises the need for governmental programs in order to reduce the market uncertainty for I4.0 products and to facilitate the access to knowledge (e.g. through platforms, educational funding) especially for SMBs.

5.3. Limitations and further research

Even though it makes important contributions, our analysis has its limitations, which open avenues for further research. First, the exploratory nature of our qualitative study limits its generalisability. The foundation for our study is the database of cases launched and maintained by the German government. While this database is valuable for exploratory research, it also presents a bias towards successful cases and towards SMBs. Further research should expand data collection efforts via surveys, Delphi studies and other secondary databases to evaluate the representativeness of this database. Large-scale empirical studies can be employed further to test hypotheses. Moreover, the applicability of our study conducted in an empirical German context to other major industrial contexts, such as the United States or Japan, still has to be established.

Second, the focus of our analysis on a wide range of I4.0 technologies keeps our findings general. Other specific groups of technologies deserve study. Smart products that exchange information independently, trigger actions and control each other may have very different risk profiles, for instance (Pereira and Romero, 2017). Third, our study reveals that humans play a crucial role in the implementation and use of I4.0 technologies. Recent review studies (e.g. Hanelt et al., 2020) have identified the digitalisation of individuals and key decision-makers as an opportunity for further research. Further research could explore the impact the digitalisation of decision-makers has on the identification, management and mitigation of supply chain risks. A growing stream of research drawing on insights from behavioural economics is exploring the impact of human behaviour and cognitive biases on processes and operational performance (Loch and Wu, 2007). Previous studies of supply chain and operations management have examined the role of human factors and cognitive biases in decision-making in inventory management, procurement, forecasting, yield management and resource management. Interest in supply chain risk management is growing as well (Fahimnia et al., 2019). An understanding of risk perception and of decision-making in the event of disruptions to the supply chain is essential for supply chain risk management since such disruptions can have major managerial implications (Fahimnia et al., 2019; Ellis et al., 2010).

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Appendix A. Supplementary data

Supplementary data to this article can be found online at https://doi.org/10.1016/j.ijpe.2021.108323.

References

Alcácer, V., Cruz-Machado, V., 2019. Scanning the industry 4.0: a literature review on technologies for manufacturing systems. Eng. Sci. Technol. Int. J. 22 (3), 899–919. https://doi.org/10.1016/j.jestch.2019.01.006.

Anderson, C.R., Zeithaml, C.P., 1984. Stage of the product life cycle, business strategy, and business performance. Acad. Manag. J. 27 (1), 5–24. https://doi.org/10.5465/255954.

Arlinghaus, J.C., Zimmermann, M., Zahner, M., 2020. The influence of cognitive biases on supply chain risk management in the context of digitalization projects. In: Freitag, M., Haasis, H.D., Kotzab, H., Pannek, J. (Eds.), Dynamics in Logistics. LDIC 2020. Lecture Notes in Logistics. Springer, Cham. https://doi.org/10.1007/978-3-030-44783-0_13.

Barratt, M., Choi, T.Y., Li, M., 2011. Qualitative case studies in operations management: trends, research outcomes, and future research implications. J. Oper. Manag. 29 (4), 329–342. https://doi.org/10.1016/j.jom.2010.06.002.

Bendul, J.C., Knollman, M., 2016. The human factor in production planning and control: considering human needs in computer aided decision-support systems. Int. J. Manuf. Technol. Manag. 30 (5) https://doi.org/10.1504/IJMTM.2016.078921.

Bendul, J.C., Skorna, A.C., 2016. Exploring impact factors of shippers' risk prevention activities: a European survey in transportation. Transport. Res. E Logist. Transport. Rev. 90 (C), 206–223. https://doi.org/10.1016/j.tre.2015.05.008.

Birkel, H., Veile, J., Müller, J., Hartmann, E., Voigt, K.-I., 2019. Development of a risk framework for industry 4.0 in the context of sustainability for established manufacturers. Sustainability 11 (2), 384. https://doi.org/10.3390/su11020384.

Bolić, M., Simplot-Ryl, D., Stojmenović, I., 2010. RFID Systems: Research Trends and Challenges. John Wiley & Sons, Chichester.

Brocal, F., González-Gaya, C., Komljenovic, D., Katina, P., Sebastián, M., 2019. Emerging risk management in industry 4.0: an approach to improve organizational and human performance in the complex systems. Complexity 1–13. https://doi.org/10.1155/2019/2089763, 2019.

Busse, C., Schleper, M., Weilenmann, J., Wagner, S., 2017. Extending the supply chain visibility boundary: utilizing stakeholders for identifying supply chain sustainability risks. Int. J. Phys. Distrib. Logist. Manag. 47 (1), 18–40. https://doi.org/10.1108/IJPDLM-02-2015-0043.

Carter, C.R., Hatton, M.R., Wu, C., Chen, X., 2020. Sustainable supply chain management: continuing evolution and future directions. Int. J. Phys. Distrib. Logist. Manag. 50 (1), 122–146. https://doi.org/10.1108/IJPDLM-02-2019-0056.

Choi, T.Y., Krause, D.R., 2006. The supply Base and its complexity: implications for transaction costs, risks, responsiveness, and innovation. J. Oper. Manag. 24 (5), 637–652. https://doi.org/10.1016/j.jom.2005.07.002.

Chopra, S., Sodhi, M., 2004. Managing risk to avoid supply-chain breakdown. MIT Sloan Manag. Rev. 46 (1), 53–61. Vol. 46 No. 1, pp. 53–62.

Christopher, M., Peck, H., 2004. Building the resilient supply chain. Int. J. Logist. Manag. 15 (2), 1–13. https://doi.org/10.1108/09574090410700275.

Cohen, J., Stewart, I., 1994. The Collapse of Chaos: Discovering Simplicity in a Complex World. Penguin Books, Harmondsworth.

Denzin, N.K., Lincoln, Y.S., 2003. Handbook of Qualitative Research, 2. Sage, Thousand Oaks, California. ISBN: 978-1412974172.

Eisenhardt, K.M., 1989. Building theories from case study research. Acad. Manag. Rev. 14 (4), 532–550. https://doi.org/10.2307/258557.

Ellis, S.C., Henry, R.M., Shockley, J., 2010. Buyer perceptions of supply disruption risk: a behavioral view and empirical assessment. J. Oper. Manag. 28 (1), 34–46. https://doi.org/10.1016/j.jom.2009.07.002.

Fahimnia, B., Pournader, M., Siemsen, E., Bendoly, E., Wang, C., 2019. Behavioral operations and supply chain management–a review and literature mapping. Decis. Sci. J. 50 (6), 1127–1183. https://doi.org/10.1111/deci.12369.

Fan, Y., Stevenson, M., 2018. A review of supply chain risk management: definition, theory, and research agenda. Int. J. Phys. Distrib. Logist. Manag. 48 (3), 205–230. https://doi.org/10.1108/IJPDLM-01-2017-0043.

Federal Ministry for Economic Affairs and Energy and Federal Ministry of Education and Research, 2019. Plattform industrie 4.0. Map of industrie 4.0 use cases. available at: 23 October 2019. https://www.plattform-i40.de/PI40/Navigation/DE/In-der-Praxis/Anwendungsbeispiele/anwendungsbeispiele.html.

Flyverbom, M., Deibert, R., Matten, D., 2019. The governance of digital technology, big data, and the Internet: new roles and responsibilities for business. Bus. Soc. 58 (1), 3–19. https://doi.org/10.1177/0007650317727540.

Fosso Wamba, S., Akter, S., Edwards, A., Chopin, G., Gnanzou, D., 2015. How 'big data' can make big impact: findings from a systematic review and a longitudinal case study. Int. J. Prod. Econ. 165, 234–246. https://doi.org/10.1016/j.ijpe.2014.12.031.

Gibbert, M., Ruigrok, W., Wicki, B., 2008. What passes as a rigorous case study? Strat. Manag. J. 29 (13), 1465–1474. https://doi.org/10.1002/smj.722.

Guha, S., Kumar, S., 2017. Emergence of big data research in operations management, information systems, and healthcare: past contributions and future roadmap. Prod. Oper. Manag.

Guha, S., Kumar, S., 2018. Emergence of big data research in operations management, information systems, and healthcare: past contributions and future roadmap. Prod. Oper. Manag. 27 (9), 1724–1735. https://doi.org/10.1111/poms.12833.

Hahn, G., 2019. Industry 4.0: a supply chain innovation perspective. Int. J. Prod. Res. 58 (5), 1425–1441. https://doi.org/10.1080/00207543.2019.1641642.

Hanelt, A., Bohnsack, R., Marz, D., Antunes Marante, C., 2020. A systematic review of the literature on digital transformation: insights and implications for strategy and organizational change. J. Manag. Stud. https://doi.org/10.1111/joms.12639. https://onlinelibrary.wiley.com.

Hertel, M., 2015. Risiken der Industrie 4.0 – Eine Strukturierung von Bedrohungsszenarien der Smart factory. HMD Prax. Wirtsch. 52 (5), 724–738. https://doi.org/10.1365/s40702-015-0161-1.

Ivanov, D., Dolgui, A., 2020. A digital supply chain twin for managing the disruption risks and resilience in the era of Industry 4.0. Production Planning & Control. https://doi.org/10.1080/09537287.2020.1768450.

Ivanov, D., Dolgui, A., Sokolov, B., 2018. The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. Int. J. Prod. Res.

Ivanov, D., Dolgui, A., Sokolov, B., 2019. The impact of digital technology and Industry 4.0 on the ripple effect and supply chain risk analytics. Int. J. Prod. Res. 57 (3), 829–846. https://doi.org/10.1108/JMTM-10-2019-0368.

Jamnia, A., 2018. Introduction to Product Design and Development for Engineers. London, New York, first ed. CRC Press Taylor & Francis Group, Boca Raton, London, New York.

Kersten, W., Hohrath, P., Böger, M., 2007. An empirical approach to supply chain risk management: development of a strategic framework. In: Proceeding POMS 2007 Conference 2007, Dallas, 4-7 May 2007 available at: pomsmeetings.org. (Accessed 3 August 2020).

Ketokivi, M., Choi, T., 2014. The renaissance of case research as a scientific method. J. Oper. Manag. 32 (5), 232–240. https://doi.org/10.1016/j.jom.2014.03.004.

Levitt, T., 1965. Exploit the product life cycle. Harv. Bus. Rev. 43, 81–94.

Loch, C., Yaozhong, W., 2007. Behavioral operations management. Found. Trends® Technol. Inf. Oper. Manag. 1 (3), 121–232. https://doi.org/10.1561/0200000009.

Marley, K., Ward, P., Hill, J., 2014. Mitigating supply chain disruptions – a normal accident Perspective, Perspective. Supply Chain Manag.: Int. J. 19 (2), 142–152. https://doi.org/10.1108/SCM-03-2013-0083.

McKinsey Digital, 2015. Industry 4.0. How to navigate digitization of the manufacturing sector. available at: . (Accessed 15 July 2020). https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Operations/Our%20Insights/Industry%2040%20How%20to%20navigate%20digitization%20of%20the%20manufacturing%20sector/Industry-40-How-to-navigate-digitization-of-the-manufacturing-sector.ashx.

Miles, M.B., Huberman, A.M., 1994. An Expanded Sourcebook: Qualitative Data Analysis, second ed. Sage Publications Inc, Thousand Oaks, London, New Delhi.

Müller, J.M., Kiel, D., Voigt, K.-I., 2018. What drives the implementation of industry 4.0? The role of opportunities and challenges in the context of sustainability. Sustainability 10 (1), 247. https://doi.org/10.3390/su10010247.

Orlikowski, W.J., 1992. The duality of technology: rethinking the concept of technology in organizations. Organ. Sci. 3 (3), 398–427. https://doi.org/10.1287/orsc.3.3.398.

Oztemel, E., Gursev, S., 2018. Literature review of Industry 4.0 and related technologies. J. Intell. Manuf. 31 (4), 127–182. https://doi.org/10.1007/s10845-018-1433-8.

Pereira, A.C., Romero, F., 2017. A review of the meanings and the implications of the Industry 4.0 concept. Procedia Manufact. 13, 1206–1214. https://doi.org/10.1016/j.promfg.2017.09.032.

Perrow, C., 1999. Organizing to reduce the vulnerabilities of complexity. J. Contingencies Crisis Manag. 7 (3), 150–155. https://doi.org/10.1111/1468-5973.00108.

Porter, M.E., Heppelmann, J.E., 2014. How smart, connected products are transforming competition. Harv. Bus. Rev. 92 (11), 64–88.

Pournader, M., Kach, A., Talluri, S., 2020. A review of the existing and emerging topics in the supply chain risk management literature. Decis. Sci. J. 51 (4), 867–919. https://doi.org/10.1111/deci.12470.

Project management institute, 2017. A Guide to the Project Management Body of Knowledge: PMBOK® Guide, sixth ed. Project Management Institute Inc, Newtown Square.

Ragin, C., 1994. Constructing Social Research: the Unity and Diversity of Method. Pine Forge Press, Sage, Thousand Oaks.

Rao, S., Goldsby, T.J., 2009. Supply chain risks: a review and typology. Int. J. Logist. Manag. 20 (1), 97–123. https://doi.org/10.1108/09574090910954864.

Ries, U., 2015. Cyberattacke in der Keksfabrik. Erpressung durch Hacker. available at: https://www.spiegel.de/netzwelt/web/erpressung-durch-cyberattacken-angriffsziel-industrieanlage-a-1048034.html. (Accessed 1 August 2020).

Ritchie, B., Marshall, D.V., 1993. Business Risk Management. Chapman & Hall, London, Glasgow, New York.

Roßmann, B., Canzaniello, A., von der Gracht, H., Hartmann, E., 2017. The future and social impact of Big Data Analytics in Supply Chain Management: Results from a Delphi study. Technol. Forecast. Soc. Change.

Rossmann, B., Canzaniello, A., von der Gracht, H., Hartmann, E., 2017. The future and social impact of big data analytics in supply chain management: results from a Delphi study. Technol. Forecast. Soc. Change 130 (C), 135–149. https://doi.org/10.1016/j.techfore.2017.10.005.

Rüssmann, M., Lorenz, M., Gerbert, P., 2015. Industry 4.0. The future of productivity and growth in manufacturing industries available at: https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=4&cad=rja&uact=8&ved=2ahUKEwjWwZHit7LlAhVBL1AKHSPaCsEQFjADegQIARAC&url=https %3A %2F %2Fwww.zvw.de %2Fmedia.media.72e472fb-1698-4a15-8858-344351c8902f.original.pdf&usg=AOvVaw2cP2RB4oWqFZniXUiPFNIP. (Accessed 24 August 2020).

Saaksvuori, A., Immonen, A., 2008. Product Lifecycle Management. Springer Verlag, Berlin, Heidelberg.

Scheibe, K.P., Blackhurst, J., 2018. Supply chain disruption propagation: a systemic risk and normal accident theory perspective. Int. J. Prod. Res. 56 (1–2), 43–59. https://doi.org/10.1080/00207543.2017.1355123.

Schlüter, F., Hetterscheid, E., 2017. Supply chain process oriented technology-framework for industry 4.0. In: Kersten, W., Blecker, T., Ringle, C. (Eds.), Digitalization in Supply Chain Management and Logistics: Smart and Digital Solutions for an Industry 4.0 Environment. Proceedings of the Hamburg

International Conference of Logistics (HICL), vol. 23. epubli GmbH, Berlin, pp. 275–299. https://doi.org/10.15480/882.1467.
Schmidt, R., Möhring, M., Härting, R.-C., Reichstein, C., Neumaier, P., Jozinović, P., 2015. Industry 4.0 - potentials for creating smart products: empirical research results. In: Abramowicz, W. (Ed.), Business Information Systems: 18th International Conference, BIS 2015, Poznań, Poland, June 24-26, 2015, Proceedings, Lecture Notes in Business Information Processing, vol. 208, pp. 16–27. https://doi.org/10.1007/978-3-319-19027-3_2.
Skilton, P.F., Robinson, J.L., 2009. Traceability and normal accident theory: how does supply network complexity influence the traceability of adverse events? J. Supply Chain Manag. 45 (3), 40–53. https://doi.org/10.1111/j.1745-493X.2009.03170.x.
Stark, J., 2015. Product Lifecycle Management. Springer International Publishing, Cham.
Tang, C., Tomlin, B., 2008. The power of flexibility for mitigating supply chain risks. Int. J. Prod. Econ. 116 (1), 12–27. https://doi.org/10.1016/j.ijpe.2008.07.008.
Taylor, M., Taylor, A., 2012. The technology life cycle: conceptualization and managerial implications. Int. J. Prod. Econ. 40 (1), 541–553. https://doi.org/10.1016/j.ijpe.2012.07.006.
Tazelaar, F., Snijders, C., 2013. Operational risk assessments by supply chain professionals: process and performance. J. Oper. Manag. 31 (1–2), 37–51.
Tummala, R., Schoenherr, T., 2011. Assessing and managing risks using the supply chain risk management process (SCRMP). Supply Chain Manag.: Int. J. 16 (6), 474–483. https://doi.org/10.1108/13598541111171165.
Tupa, J., Simota, J., Steiner, F., 2017. Aspects of risk management implementation for industry 4.0. Procedia Manufact. 11, 1223–1230. https://doi.org/10.1016/j.promfg.2017.07.248.
Weick, K.E., 1976. Educational organizations as loosely coupled systems. Adm. Sci. Q. 21 (1), 1–19. https://doi.org/10.2307/2391875.
World Economic Forum, 2017. Digital transformation initiative. Unlocking $100 Trillion for business and society from digital transformation. Executive Summary, available at: http://reports.weforum.org/digital-transformation/wp-content/blogs.dir/94/mp/files/pages/files/dti-executive-summary-website-version.pdf. (Accessed 23 October 2019).
Xu, L.D., Xu, E.L., Li, L., 2018. Industry 4.0: state of the art and future trends. Int. J. Prod. Res. 56 (8), 2941–2962. https://doi.org/10.1080/00207543.2018.1444806.
Yin, R.K., 2003. Case Study Research: Design and Methods, Applied Social Research Methods Series, vol. 5. Sage, Thousand Oaks, p. 3.