KNOWLEDGE RISKS IN DIGITAL SUPPLY CHAINS

PROPOSAL OF A DISSERTATION PROJECT AT THE SCHOOL OF BUSINESS, ECONOMICS AND SOCIAL SCIENCES UNIVERSITY OF GRAZ

JOHANNES P. ZEIRINGER

University of Graz, BANDAS-Center, Universitätsstraße 15 F3, 8010 Graz, Austria;
e-mail: johannes.zeiringer@uni-graz.at,

Abstract The digital transformation changes the way how organizations exchange data in supply chains (SC). Data traditionally shared, is enriched by detailed data sets captured by sensors in the production itself. Advanced data analytic approaches make it possible to extract knowledge from such data sets and thus increase the risk that competitive knowledge unintentionally spills over. From a knowledge management perspective, little attention is paid to such knowledge risks arising from data-centric collaborations. Hence, this proposed PhD project aims at investigating this, by using the overall method of Design Science Research. The project focuses on digital SC, as data-centric collaborations play a central role within them. To contribute to knowledge research, a framework is being sought. The elaborated framework should allow an assessment of knowledge risks and support the selection of suitable measures and it should contribute on how to support the management of knowledge risks in digital SC.

Keywords: knowledge risks, knowledge protection, digital supply chain, data-centric collaboration

University of Maribor Press

DOI https://doi.org/10.18690/978-961-286-485-9.54
ISBN 978-961-286-485-9

1 Introduction

The digital transformation offers many new opportunities to improve the operation of supply chains (SC) (Vial, 2019). This has led to innovations and changes in different industry sectors and equally affects knowledge management (KM) and supply chain management (SCM) (Schniederjans et al., 2019). Digitalization means the use of digital technologies to change or improve a business model and provide new revenue and value-producing opportunities (Mäkiö et al., 2018). It is not only penetrating SCM increasingly but also, more and more firms are inter-organizational connected and share data along the SC (Kazantsev et al., 2018), (North et al., 2019). From the perspective of knowledge protection, this increasing exchange of comprehensive data sets needs closer attention, because it is a possible gateway to new knowledge risks (Ilvonen et al., 2018), (Durst & Zieba, 2019).

Digitalization enhances the number of connected devices intensely. Implementation of advanced digital technologies (IoT, blockchain, predictive analytics, etc.) determine the digital SC. This results in each partner generating much more data which is shared with collaborators. Also, due to autonomous systems and affordable sensors, the amount of data which is being generated and shared has exploded in the past decade (Spanaki et al., 2018), (Brettel et al., 2014). Sensors in industrial ecosystems control and monitor processes of industrial production and, as part of it, generate and share data continuously (Chen et al., 2016). As a result digital SC emerge, which does not aim at the difference of physical or digital goods or services, but rather how processes within the SC are innovated and changed by modern technologies (Büyüközkan & Göçer, 2018). A digital SC includes a comprehensive exchange of data and is a multi-layered production network that can be flexibly and quickly optimized and (re)composed (Zeiringer J. P. & Thalmann S., 2020).

Knowledge is a key asset within organizations and a source of an organizations competitive advantage (Grant, 1996; Nonaka, 1994). With digital transformation going on, also knowledge management needs to be reopened as new issues arise. Sharing knowledge outside the company, in data-centric collaborations such as alliances, networks, joint ventures or SC partnerships, companies must take protective measures when transferring knowledge across companies, as knowledge risks arise (Krogh, 2012), (Durst & Zieba, 2017). As knowledge is mobile, it is difficult to protect. Especially in collaborations, different people have access to

valuable knowledge (Elliott et al., 2019). It is important that no unintentional outflow of knowledge should take place. Knowledge protection therefore concentrates on (1) preventing knowledge spill-over, (2) reducing the visibility of knowledge and (3) unwanted knowledge spill-over (Manhart & Thalmann, 2015).

Through the intensive exchange of data in inter-organizational collaborations and especially knowledge-intensive collaborations, companies need to find a suitable trade-off between the benefits and risks of collaborations. Research on this trade-off is rare and more research on inter-organizational knowledge transfer, respectively knowledge protection is urgently needed (Hernandez et al., 2015), (Loebbecke et al., 2016), (Manhart & Thalmann, 2015).

As collaboration involves the exchange of data, knowledge risks emerge, especially in data-centric collaborations. Unless these risks are eliminated or managed, they leave a company fragile. Nevertheless, data is a key asset to partners in SC and a source to support SC activities. The goal of data-centric collaborations is to minimize the manual intervention in production processes in order to improve safety, efficiency and sustainability of production through automation (Vyatkin, 2013). With modern data science approaches comprehensive data sets collected from industrial ecosystems, can be continuously analysed to gain useful knowledge for industrial automation (Chen et al., 2016). Hence, SC processes can be optimized, and quality improvements achieved (Kaiser et al., 2020).

2 Problem definition

Traditionally, data for order management and logistics management are exchanged in clearly specified and controllable ways (Min et al., 2019). Regarding digitalization, not only increasingly more data is being exchanged, but this exchange of data is becoming more important for the core operations areas of companies. Modern data analytics methods make it possible and affordable to analyse such data sets and to extract knowledge about these sensitive areas of operation (Schniederjans et al., 2019), (Birkel & Hartmann, 2019). Besides possible benefits of the increased sharing of comprehensive data sets, also risks of losing competitive advantage could arise. Therefore, the risk of losing competitive knowledge through data-centric collaborations in SC is needed to be researched. Furthermore, organizations should

carefully balance their activities to promote and control knowledge sharing, to protect their competitive knowledge (Ilvonen et al., 2018).
Referring to KM, inter-organizational knowledge sharing has a strategic dimension and requires a careful balancing of knowledge sharing and protection as otherwise a loss of competitive knowledge could arise (Loebbecke et al., 2016). Due to, among other things, digitalization, organizational and national boundaries become more blurred and knowledge can be diffused much easier. Openness and inter-organizational collaboration build the foundation of rich, contextualized and sustainable knowledge sharing activities among networked partners within and beyond organizational boundaries (Ilvonen et al., 2018). Referring to knowledge sharing, corporations increasingly rely on the know-how and expertise of external organizations in order to innovate, to remain competitive and to improve performance within the SC (Zacharia et al., 2019).

So far, research focuses mainly on knowledge sharing and protection between persons (representing organizations) in the form of implicit and explicit knowledge exchange (Loebbecke et al., 2016). Little is known about knowledge risks arising from knowledge discovery of huge and comprehensive data sets shared in the course of their digital SC (Ilvonen et al., 2018), (North et al., 2019). In addition, there are efforts to research data and information security, but knowledge protection received little attention so far (Manhart & Thalmann, 2015).

Based on the following observations within this proposal and the current state of research, the research question (RQ) below results:

How to support the management of knowledge risks in digital SC?

3 Methodology

This project makes use of a mixed methods approach. Design science research (DSR) is used as the overall method (Hevner et al., 2004). In the field of IS, the relevance of research is often directly related to the development of IT artefacts (Peffers et al., 2007). DSR is characterized by behavioural and design science. The basic principle in DSR is that knowledge about a real existing problem is gained through the design and evaluation of a solution (Hevner et al., 2004). The result of the research is not only a design-oriented solution, but also a scientific contribution

in the form of frameworks or models (March & Smith, 1995). In order to ensure this contribution to theory, all phases of design science must be rigorously carried out. This requires that both the design proposals and the cause-effect relationships must be empirically evaluated (Iivari, 1991). The research approach will be iterative, with each iteration having elements of (1) identifying and answering problem formulations from the relevant use case, (2) designing artefacts supporting decision making, and (3) elements of rigor, with behavioural theory, and support from IS to KM, SCM, and decision support systems research (A. R. Hevner, 2007). Referring to the stated research problem, the development of a framework, elaborated based on DSR, would be most suitable.

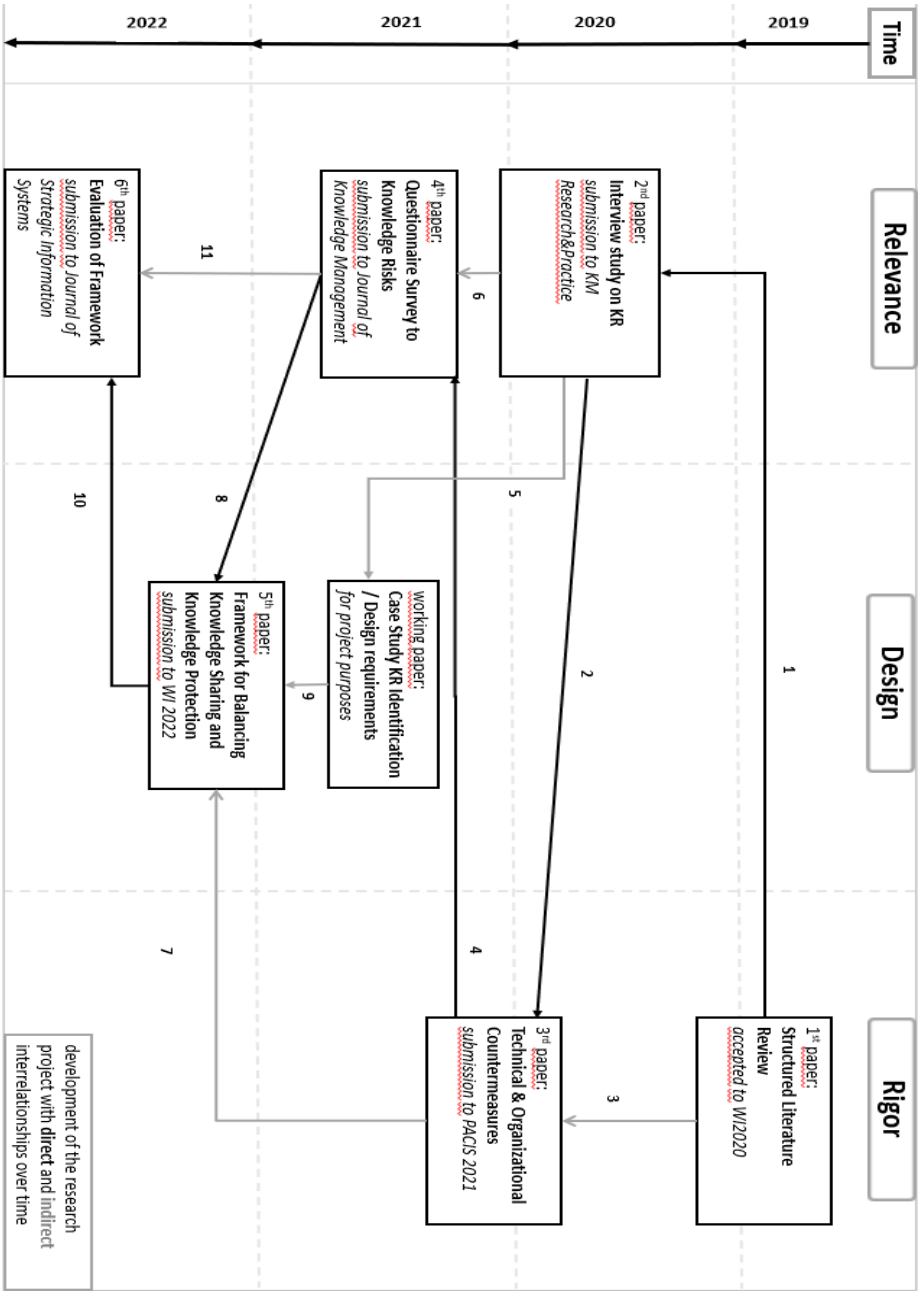

Figure 1: DSR timeline

Figure 1 shows which area the planned papers are assigned to and what their direct and indirect interaction is. The consecutive research papers are listed in the following.

3.1 Paper 1: Structured Literature Review

At first, a structured literature review by Webster and Watson (Webster & Watson, 2002) has been conducted (see chapter 4). In order to elaborate the state of the art in the research field, this is a common process in the information systems (IS) area (Webster & Watson, 2002). Furthermore, a literature review helps to identify the possible research gap. The RQ was regarding which kind of knowledge risks arise from data-centric collaborations and what suitable countermeasures are, see (Zeiringer J. P. & Thalmann S., 2020). The literature review is located at the rigor area within the DSR and an important knowledge base at the beginning of the dissertation project (A. R. Hevner, 2007).

3.2 Paper 2: Interview Study on Knowledge Risk Identification

For this work an interview study by (Patton, 2005) has been conducted (see chapter 4), which is part of the relevance cycle of the DSR (A. R. Hevner, 2007). It is planned to show a detailed requirement analysis for helping to develop the framework. The interview study tried, based on the literature review, to identify different approaches on how to handle knowledge risks in digital SC. Data-centric collaborations were focused, and the balancing of knowledge sharing and protection. There were two staged interviews held with 15 Experts and the elaborated paper has been submitted by now.

Based on the literature review, the risks were theoretically elaborated and analysed; with the interview study, the risks should become more tangible and comprehensible in organizational context. The RQ will be, which knowledge risks arise from data-centric collaborations and which current protection mechanisms are available in order to protect knowledge. Also, it will be shown, if there are already strategies on how to balance sharing and protection and if there are security action plans for what to do after an incident (Thalmann & Ilvonnen, 2020).

3.3 Paper 3: Technical and Organizational Countermeasures

First possible frameworks for technical and organizational countermeasures were deduced from literature and synthesized in a rigor paper. Insights from the first literature review and the interview study were used to develop actionable countermeasures. Also, it is helpful to gather and use theoretical sources to gain creative ideas for the design cycle (A. R. Hevner, 2007).

The RQ is about the possible prevention of unwanted knowledge incidents with help of technical and organizational countermeasures. It also tries to identify measurements that are suitable and easy actionable. The method was the structured literature review, according to (Vom Brocke et al., 2015).

3.4 Paper 4: Questionnaire Survey on Knowledge Risks

Based on the research paper on technical and organizational countermeasures and indirectly the case study, which were carried out in the previous steps, questions for the interviews and online survey can be clearly formulated and the interview study and survey can thus be carried out in a standardised form. The aim of the questionnaire study is to get more details on the problems to be investigated, regarding the identification of them and current protection mechanisms. The target group are experts: SC managers, risk managers or managing directors. After developing first countermeasures, the survey will cover the field of relevance within the DSR again (A. R. Hevner, 2007). The RQ will focus on how organizations are currently deal with arising knowledge risks, if knowledge risks in digital SC represent a barrier to digitalization and to what extent training can help identify knowledge risks in data-centric collaborations. Also, there will be a focus on how to support employees in recognizing knowledge risks in data sets.

Together with the insights of the reviews and the interview study, a first requirement analysis will be conducted. In order to construct a framework, it is necessary to focus on the design cycle after the case study (A. R. Hevner, 2007). It is important to note first intermediated findings and develop a first design concept for needed requirements. This will be processed in an internal working paper and helps to set focus on the fifth paper. The RQ will be to define first requirements for an effective knowledge protection management framework in digital SC. The method will be

user-centred design, according to (Chadia Abras et al., 2004). This will happen simultaneously to the questionnaire study and be a preparation before going into paper 5.

3.5 Paper 5: Framework for Balancing Knowledge Sharing and Knowledge Protection

Based on the findings by then, a framework for balancing knowledge sharing and knowledge protection will be developed. Within this design part of the project, all requirements gathered so far will be processed for this paper (A. R. Hevner, 2007). The main focus will be on the extent to which technical and organizational measures can be used to manage knowledge risks in digital SC.

The RQ will be on which technical or organizational measures can be used to manage knowledge sharing and protection in digital SC and how should a framework be designed to be successfully implemented. The method will be the user-centred design again, according to (Chadia Abras et al., 2004).

3.6 Paper 6: Evaluation of Framework

Finally, the evaluation of the framework will be conducted which, referring to the DSR, is assigned to the relevance circle again (A. R. Hevner, 2007). In DSR, it is important to test the developed artefact in the field, to see if it is appropriate. The results will show, if the artefact is suitable or another iteration is needed (A. R. Hevner, 2007). The evaluation should be executed by an evaluation study which is based directly on the developed framework and the help of the insights gained from the experts. The possible RQ and will potentially be, if the developed framework increases the decision quality of managing knowledge risks within digital SC. The method will be a two staged interview study followed by an (online) survey, according to (Bortz & Döring, 2006).

4 Preliminary/Expected results

As a first step, the state of the art had to be raised. Therefore, a literature review according to (Webster & Watson, 2002) was conducted and processed in a prime paper, see (Zeiringer J. P. & Thalmann S., 2020). In the paper, knowledge risks in data-centric collaborations as part of digital SC were dealt with. Traditional SC risk

management was used to identify causes of risks, risks themselves and potential countermeasures, which were then adapted to digital SC. One of the main insights of this review was that there is little research regarding the field of knowledge risks in data-centric collaborations, which indicated that there is a demand for further research on this main aspect of digital transformation. Furthermore, data-centric collaboration itself is not adequately dealt with so far, as there is still a focus on traditional risks and hardly on intangible risks. It was discovered that there is need for a knowledge risk management and that future research should investigate which kind of measures are meaningful to balance knowledge sharing and protection in data-centric collaborations (Zeiringer J. P. & Thalmann S., 2020). In addition, research shows that the resulting uncertainty creates a barrier to digitalization (North et al., 2019).

The Interview study showed that organizations use different approaches in data-centric collaborations to encounter knowledge risks. It is shown that all three approaches lead to different perspectives of sharing and protection of knowledge within the digital SC. The approaches can be viewed as steps of development, each as one step further in building awareness on knowledge risks and to balance knowledge sharing and protection more holistic. Furthermore, it is shown that minimizing risk can stifle innovation and there is a need for more research [being reviewed].

The second literature review deduced possible actions from literature, to show what is available and what is still missing in order to tackle knowledge risks in data-centric collaborations. In order to build on this and contribute to knowledge research, a framework will be sought after this. The elaborated framework should allow an assessment of knowledge risks and support the selection of suitable measures in practice. It should support the responsible person in the sense of decision support but should not automate the decision (Alter, 2004). With regard to DSR, several cycles of design, evaluation in practice and theoretical reflection should provide a solution to the problem rather than just explore it. Possible developed artefacts could be, e.g., selection lists, visualizations, algorithms or practices. Risks resulting from data exchange can be managed by organizational, technical and/or legal measures. The proposed research project uses this subdivision as a starting point and investigates the simultaneous management of knowledge sharing and knowledge protection in digital SC.

Regarding the theory of knowledge sharing, new categories of knowledge risks that emerge from the growing need to share larger and more comprehensive data sets from which competitive knowledge can be discovered, should be identified and investigated. Also, the data-centric perspective will provide new insights to knowledge sharing theory as well as knowledge risk management. An appropriate strategy to manage knowledge risks, taking data-centric collaborations into account, will be sought (Zeiringer J. P. & Thalmann S., 2020). The expected contribution should be a framework on how to support the management of knowledge risks in digital SC.

5 Future development

The whole project will be split into seven papers. The first paper was a literature review, which has already been accepted to the conference *Wirtschaftsinformatik 2020* (Zeiringer J. P. & Thalmann S., 2020).

The second paper was an interview study (Patton, 2005). Slightly delayed, the third paper, a literature research about technical countermeasures by (Vom Brocke et al., 2015), was written and is submitted in the begin of 2021. At the same time, the planned survey will be conducted and processed in a fourth paper by mid-2021. The elaboration on a working paper starts in Spring 2021, which will help to define design requirements. The final framework is planned to be processed in a paper by spring 2022. Finally, the evaluation of the framework starts in 2022 and ends in June 2022, by submitting the sixth paper.

References

Alter, S. (2004). A work system view of DSS in its fourth decade. Decision Support Systems, 38(3), 319–327. https://doi.org/10.1016/j.dss.2003.04.001

Birkel, H. S., & Hartmann, E. (2019). Impact of IoT challenges and risks for SCM. Supply Chain Management: An International Journal, 24(1), 39–61. https://doi.org/10.1108/SCM-03-2018-0142

Bortz, J., & Döring, N. (2006). Forschungsmethoden und Evaluation. Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-540-33306-7

Brettel, M., Friederichsen, N., Keller, M., & Rosenberg, M. (2014). How Virtualization, Decentralization and Network Building Change the Manufacturing Landscape: An Industry 4.0 Perspective. International Journal of Mechanical, Aerospace, Industrial, Mechatronic and Manufacturing Engineering(8), 37–44.

Büyüközkan, G., & Göçer, F. (2018). Digital Supply Chain: Literature review and a proposed framework for future research. Computers in Industry, 97, 157–177. https://doi.org/10.1016/j.compind.2018.02.010

Chadia Abras, Diane Maloney-krichmar, & Jenny Preece (2004). User-Centered Design. In In Bainbridge, W. Encyclopedia of Human-Computer Interaction. Thousand Oaks: Sage Publications. Publications.

Chen, Y., Lee, G. M., Shu, L., & Crespi, N. (2016). Industrial Internet of Things-Based Collaborative Sensing Intelligence: Framework and Research Challenges. Sensors (Basel, Switzerland), 16(2), 215. https://doi.org/10.3390/s16020215

Durst, S., & Zieba, M. (2017). Knowledge risks - towards a taxonomy. International Journal of Business Environment, 9(1), Article 84705, 51. https://doi.org/10.1504/IJBE.2017.084705

Durst, S., & Zieba, M. (2019). Mapping knowledge risks: towards a better understanding of knowledge management. Knowledge Management Research & Practice, 17(1), 1–13. https://doi.org/10.1080/14778238.2018.1538603

Elliott, K., Patacconi, A., Swierzbinski, J., & Williams, J. (2019). Knowledge Protection in Firms: A Conceptual Framework and Evidence from HP Labs. European Management Review, 16(1), 179–193. https://doi.org/10.1111/emre.12336

Grant, R. M. (1996). Toward a knowledge-based theory of the firm. Strategic Management Journal, 17(S2), 109–122. https://doi.org/10.1002/smj.4250171110

Hernandez, E., Sanders, W. G., & Tuschke, A. (2015). Network Defense: Pruning, Grafting, and Closing to Prevent Leakage of Strategic Knowledge to Rivals. Academy of Management Journal, 58(4), 1233–1260. https://doi.org/10.5465/amj.2012.0773

Hevner, March, Park, & Ram (2004). Design Science in Information Systems Research. MIS Quarterly, 28(1), 75. https://doi.org/10.2307/25148625

Hevner, A. R. (2007). A Three Cycle View of Design Science Research. Scandinavian Journal of Information Systems, 87–92.

Iivari, J. (1991). A paradigmatic analysis of contemporary schools of IS development. European Journal of Information Systems, 1(4), 249–272. https://doi.org/10.1057/ejis.1991.47

Ilvonen, I., Thalmann, S [Stefan], Manhart, M., & Sillaber, C. (2018). Reconciling digital transformation and knowledge protection: a research agenda. Knowledge Management Research & Practice, 16(2), 235–244. https://doi.org/10.1080/14778238.2018.1445427

Kaiser, R., Thalmann, S [Stefan], & Pammer-Schindler, V. (2020). An Investigation of Knowledge Protection Practices in Inter-organisational Collaboration. Protecting Specialised Engineering Knowledge with a Practice Based on Grey-box Modelling. VINE. Advance online publication. https://doi.org/10.1108/VJIKMS-11-2019-0180

Kazantsev, N., Pishchulov, G., Mehandjiev, N., Sampaio, P., & Zolkiewski, J. (2018). Formation of Demand-Driven Collaborations between Suppliers in Industry 4.0 Production Networks. 20th International Working Seminar on Production Economics.

Krogh, G. von (2012). How does social software change knowledge management? Toward a strategic research agenda. The Journal of Strategic Information Systems, 21(2), 154–164. https://doi.org/10.1016/j.jsis.2012.04.003

Loebbecke, C., van Fenema, P. C., & Powell, P. (2016). Managing inter-organizational knowledge sharing. The Journal of Strategic Information Systems, 25(1), 4–14. https://doi.org/10.1016/j.jsis.2015.12.002

Mäkiö, J., Miroliubov, A., & Zhgun, V. (2018). Digitalization – quo vadis? SHS Web of Conferences, 44, 56. https://doi.org/10.1051/shsconf/20184400056

Manhart, M., & Thalmann, S [Stefan] (2015). Protecting organizational knowledge: a structured literature review. Journal of Knowledge Management, 19(2), 190–211. https://doi.org/10.1108/JKM-05-2014-0198

March, S. T., & Smith, G. F. (1995). Design and natural science research on information technology. Decision Support Systems, 15(4), 251–266. https://doi.org/10.1016/0167-9236(94)00041-2

Min, S., Zacharia, Z. G., & Smith, C. D. (2019). Defining Supply Chain Management: In the Past, Present, and Future. Journal of Business Logistics, 40(1), 44–55.

https://doi.org/10.1111/jbl.12201
Nonaka, I. (1994). A Dynamic Theory of Organizational Knowledge Creation. Organization Science, 5(1), 14–37. https://doi.org/10.1287/orsc.5.1.14
North, K., Carvalho, A. de, Braccini, A., Durst, S., Carvalho, J., Gräslund, K., & Thalmann, S [S.] (2019). Information and knowledge risks in supply chain interactions of SMEs: Proceedings of the 10th International Conference on Practical Knowledge Management, Potsdam, Germany. Lecture notes on Informatics.
Patton, M. Q. (2005). Qualitative Research. In B. Everitt & D. C. Howell (Eds.), Encyclopedia of statistics in behavioral science. Wiley. https://doi.org/10.1002/0470013192.bsa514
Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. Journal of Management Information Systems, 24(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302
Schniederjans, D. G., Curado, C., & Khalajhedayati, M. (2019). Supply chain digitisation trends: An integration of knowledge management. International Journal of Production Economics, 107439. https://doi.org/10.1016/j.ijpe.2019.07.012
Spanaki, K., Gürgüç, Z., Adams, R., & Mulligan, C. (2018). Data supply chain (DSC): research synthesis and future directions. International Journal of Production Research, 56(13), 4447–4466. https://doi.org/10.1080/00207543.2017.1399222
Thalmann, S [S.], & Ilvonnen, I. (2020). Why should we investigate knowledge risks incidents? - Lessons from four cases. Proceedings of 53rd Hawaii International Conference on System Sciences.
Vial, G. (2019). Understanding digital transformation: A review and a research agenda. The Journal of Strategic Information Systems, 28(2), 118–144. https://doi.org/10.1016/j.jsis.2019.01.003
Vom Brocke, J., Simons, A., Riemer, K., Niehaves, B., Plattfaut, R., & Cleven, A. (2015). Standing on the Shoulders of Giants: Challenges and Recommendations of Literature Search in Information Systems Research. Communications of the Association for Information Systems, 37. https://doi.org/10.17705/1CAIS.03709
Vyatkin, V. (2013). Software Engineering in Industrial Automation: State-of-the-Art Review. IEEE Transactions on Industrial Informatics, 9(3), 1234–1249. https://doi.org/10.1109/TII.2013.2258165
Webster, J., & Watson, R. (2002). Analyzing the Past to Prepare for the Future: Writing a Literature Review. MIS Quarterly, 26. https://doi.org/10.2307/4132319
Zacharia, Z., Plasch, M., Mohan, U., & Gerschberger, M. (2019). The emerging role of coopetition within inter-firm relationships. The International Journal of Logistics Management, 30(2), 414–437. https://doi.org/10.1108/IJLM-02-2018-0021
Zeiringer J. P., & Thalmann S. (2020). Knowledge Risks in Digital Supply Chains: A Literature Review. In: Proceedings of Wirtschaftsinformatik 2020 (WI 2020).