Proceedings of the 35th European Safety and Reliability & the 33rd Society for Risk Analysis Europe Conference
Edited by Eirik Bjorheim Abrahamsen, Terje Aven, Frederic Bouder, Roger Flage, Marja Ylönen
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-94-3281-3_ESREL-SRA-E2025-P0983-cd

Designing a Systemic Risk and Robustness Assessment for Critical Value Chains

Stefan Schauer, Martin Latzenhofer

AIT Austrian Institute of Technology, Austria.
E-mail: {stefan.schauer; martin.latzenhofer}@ait.ac.at

Sebastian Uhl, Julian Walser, Alexandra Birkmaier

Fraunhofer Austria Research GmbH, Austria.
E-mail: {sebastian.uhl; julian.walser; alexandra.birkmaier}@fraunhofer.at

Supply chains, especially those related to critical goods such as food, hygiene products, and medication, are increasingly vulnerable to disruptions stemming from a wide range of risks and systemic interdependencies. In order to address this challenge, we describe a conceptual approach for a systemic assessment framework that integrates both risk and robustness aspects by design and is tailored to the specific requirements and challenges of critical value chains. This monitoring framework builds on a process model for analyzing vulnerabilities and disturbances within such a critical value chain. The significant stakeholders along with their interconnections and vulnerabilities are identified in a structured manner based on domain information and expert knowledge. Furthermore, the monitoring framework utilizes a cross-sectoral simulation model that builds upon an abstract representation of the supply chain and facilitates the analysis of cascading effects across organizational and sectoral borders. This model enables the assessment and visualization of the complex relations and dependencies within a supply chain in a general manner, particularly capturing orthogonal factors such as transport, maintenance, or legal aspects.

Keywords: Risk and Robustness Assessment, Cross-sector Simulation, Cascading Effects, Vulnerability Analysis, Critical Value Chains

1. Introduction

Recent incidents, such as natural disasters, global pandemics, political turbulence, and armed conflicts, have shown that critical value chains of goods and services can be severely affected by both global and local events. This has become particularly evident due to the armed conflict between Russia and the Ukraine, which had a significant impact on gas and energy market in the European Union Henderson (2024) and on global food supply chains Jagtap et al. (2022); Sheth and Uslay (2023), among others. Also the COVID-19 pandemic had severe impacts on global supply chains due to limited work force Kakaei et al. (2022) or the closure of international ports and other logistics hubs Su (2024); Wang and Su (2025). With regards to natural disasters, there have been extensive studies Ye and Abe (2012) on the consequences of the 2011 earthquake in Japan, which had a devastating impact on the nuclear power plant in Fukushima as well as huge effects on critical infrastructures like dams and roads, and global corporations' value chains. As such value chains represent the backbone of our everyday life, it is crucial to maintain their functionality and improve their robustness and resilience. This requires both the identification of critical goods and the analysis of complex relationships between upstream and downstream players from different industries. Therefore, general factors, such as production locations, preliminary and auxiliary products, refining steps, as well as orthogonal factors like packaging, know-how or transport routes need to be comprehensively considered. Alongside preventive measures to avoid potential bottlenecks, a structured approach is required to minimize the – potentially cascading – effects of any disturbances when they appear.

In this paper, we present a conceptual approach that aims at capturing all the above mentioned relevant information on critical value chains in a structured and easily reproducible way as well as consolidating that information into an integrated assessment model for risk and robustness. This ap-

proach stems from the ongoing national research project MERCURIUS, which deals with the vulnerability of critical value chains in Austria. We introduce a value chain analysis model which is making extensive use of domain information and expert interviews to identify not only the most important stakeholders along a critical value chain but takes a clear focus on the interconnections and dependencies among them. Building on these interdependencies, we further describe a systemic risk and robustness assessment framework. As a core part of this framework, a cross-sectoral simulation approach called CASSANDRA facilitates the analysis of cascading effects along the value chain. Since the underlying dependency graph includes also orthogonal factors in the value chain such as transport, maintenance and legal aspects, the CASSANDRA model enables a holistic overview on the overall impacts an incident might have. As a main advantage of the presented framework, we will show how the results from the simulation can be aligned with common risk indicators of value chains. In this way, the model is able to estimate risk and robustness at the same time, allowing stakeholders to choose their mitigation actions to account for both factors.

The remainder of the paper is structured as follows: Section 2 covers a brief overview on current concepts and models from supply chain management and from risk and resilience management as a starting point for the current model. Section 3 provides a detailed description of the value chain analysis model, including a step-by-step analysis guide. Section 4 covers the main aspects of the cascading effects simulation model. Both parts are then integrated into the combined risk and robustness model in Section 5. Finally, Section 6 concludes the paper and provides an outlook on the next steps in the ongoing research project.

2. Related Work

Risk and resilience have been crucial aspects for companies and organizations, in general, and critical infrastructures, in particular, with specifically the concept of resilience gaining importance over the recent years. This becomes evident when looking at current EU directives such as the Critical Entities' Resilience (CER) directive European Comission (2022a), the Network and Information Systems' security (NIS) directive European Comission (2022b) or the Cyber Resilience Act (CRA) European Comission (2024).

Together with the topic of resilience, all of these directives also have a strong focus on the relations and dependencies among organizations as well as supply chains in general. Accordingly, the analysis of supply chains and Supply Chain Risk Management becomes more important and various methodologies for supply chain analysis have already been described in the literature. These methodologies can be categorized as *empirical* (case studies or statistical surveys Handfield et al. (2020); Gurbuz and Ozkan (2020)), *quantitative* (mathematical models, simulations or multi-criteria decision-making (MCDM) Paul and Chowdhury (2021); Wang and Ip (2009)) and *qualitative* (expert interviews or discussions Ishida (2020); Chowdhury et al. (2021)). Moreover, *hybrid methods* incorporate multiple methodologies of one or multiple categories Kumar et al. (2021); Zhang et al. (2023).

In order to adjust to the higher dynamics and complex interrelations within supply chains, standard risk management processes such as the ISO 31000 International Standardization Organization (2018) or the ISO 27005 International Standardization Organization (2022) are not properly designed but require a clear focus on cascading effects as part of them. Approaches for modeling and simulating cascading effects in specific domains can be found in the literature, e.g., applying Bayesian networks for critical information and communication (ICT) systems Schaberreiter et al. (2013) or Interdependent Markov Chains for the energy sector Rahnamay-Naeini and Hayat (2016) amongst many others. A more generic concept has been introduced by König et al. (2019); Schauer et al. (2020) using probabilistic Mealy automata to connect physical and cyber domains within a critical infrastructure Schauer et al. (2020) or to connect various industry sectors Schauer and Rass (2020).

Although all of these simulation approaches can be used as tools in every risk or resilience process,

an explicit integration of such models has recently be done by Schauer et al. (2021), designing a combined risk and resilience management process.

3. Value Chain Analysis Model

In the following section, we propose a waterfall process model for analyzing intertwined critical value chains. This model builds on multiple methods and incorporates them into a general framework for a complete risk analysis. In short, the process model consists of the steps depicted in Figure 1. In its originality, the process model consists of seven steps resulting in measures for improving robustness. In order to gain an improved systemic risk and robustness assessment, we combine the first three steps of the process model with the combined risk and resilience model described in Section 5. The steps in the systemic risk and robustness assessment framework resemble a detailing of the value chain analysis process in the combined risk and resilience process model in Section 5. Steps (1), (2), and (3) correspond to context establishment and hazard identification. Steps (4) to (7) are a predefinition of the risks which are later assessed quantitatively in the risk assessment process.

Despite proposing certain methodologies for each individual step, the waterfall process model is designed in a way such that the referenced method of any step described in the following Sections 3.1- 3.3 can be exchanged by any method that achieves the same goal.

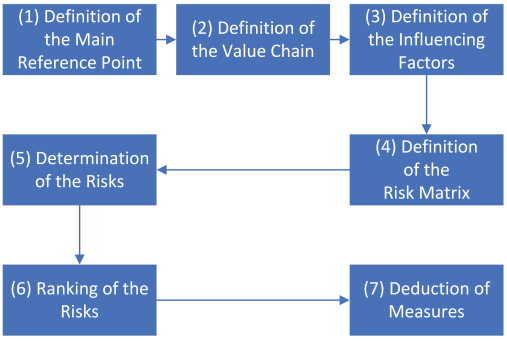

Fig. 1. Value Chain Analysis Model

3.1. *Definition of the Main Reference Point*

Most of the literature on value chain analysis, e.g. Zhang et al. (2023); Kumar et al. (2021); Wang and Ip (2009), assumes the main reference point implicitly. However, defining the main reference point is an essential part of the critical value chain analysis, as it specifies the point of view on the supply network. Different viewpoints on the value chain can result in very different supply networks. For example, considering the milk supply chain of Austria from the point of view of a certain dairy factory results in a rather linear supply chain, whereas from the viewpoint of the complete dairy market, the resulting intertwined supply network Ivanov and Dolgui (2020) contains multiple dairy companies and all their corresponding factories, suppliers, and dependencies that mutually influence each other.

3.2. *Definition of the Value Chain*

In step (2) of the process model, the value chain is defined according to the reference point of step (1). The difficulty of this step is that there is no fixed definition of certain value chains, and depending on the point of view and the level of detail, any value chain can become highly complex and intertwined. Methods for gaining the relevant information can range from expert knowledge or literature reviews Wang and Ip (2009); Paul and Chowdhury (2021), over stakeholder interviews Zhang et al. (2023) to iterative consensus methods like the delphi method Alarabiat and Ramos (2019); Kumar et al. (2021).

For systematically gaining a fine-grained definition of the considered value chain with all relevant actors and dependencies, we propose an iterative search and consensus process inspired by the Delphi method Alarabiat and Ramos (2019), genetic algorithms Holland (1984); Katoch et al. (2021) and by making use of group discussions.

The goal of this process step is to find all relevant and influencing parts of the considered value chain and to represent it as an interdependency graph. Both the Delphi method and genetic algorithms are iterative methods to search for best possible solutions. In every iteration the solution

should improve until a local optimum is found. Genetic algorithms generate new improved solutions by combining previous ones and the best new solutions are selected by a so-called fitness function that defines the quality of the solution. In the Delphi method, experts provide answers and inputs (solutions) and the research comprises those solutions to new questions, thereby allowing the experts to give further and improved feedback (improved solutions).

Furthermore, one aspect that is implemented by genetic algorithms but not considered in the Delphi method, is *mutation* (Katoch et al. (2021)), i.e., integrating randomness or out-of-the-box solutions, to escape local optima. In order to implement this concept in our search process, we propose group discussions and feedback sessions with non-experts to get out-of-the-box views on the value chain under consideration.

Thus, by combining the two search approaches, we propose the following search process:

(1) Definition of the initial value chain by an expert (including a literature review)
(2) Expert interview(s) to improve the current value chain
(3) Group discussion or feedback session with non-experts to get out-of-the-box views
(4) If the supply chain has been improved in steps (2)-(3), then do the next iteration from step (2). Otherwise, the value chain reached a stable point.

3.3. *Definition of Influencing Factors*

The definition of influencing factors is based on the resulting value chain represented as an interdependency graph of step (2). Specifically, the defined value chain allows to systematically derive influencing factors for every given node and edge in the value chain. We propose to use the search process of step (2) (cf. Section 3.2) to generate a best possible list of influencing factors in the value chain.

4. Cascading Effects Analysis

The interdependency graph created as part of the Value Chain Analysis serves as a direct input to a cascading effects simulation approach. This approach aims at integrating the relations between the individual value chain partners and at describing the consequences of an incident happening at one individual organization on the entire value chain. This is done by building on a automaton-based stochastic model that has been developed by König et al. (2019); Schauer et al. (2020) (cf. also Fig. 2). In this model, each partner in the value chain as well as each critical asset within each partner (i.e., each node in the dependency graph) is represented by a probabilistic Mealy automaton; each directed edge represents a dependency among two of these partners.

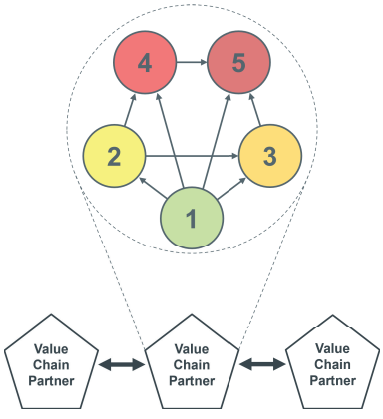

Fig. 2. Illustration of the Mealy automaton model for value chain partners.

In more detail, a Mealy automaton has several different states, which can be used to describe the functionality or operational capacity of the respective value chain partner. The number of states and the interpretation of each state is in general open, which makes the approach highly adaptable to organizations from various domains. These states can be numbered, e.g., from ”1” to ”5”, or labeled, e.g., from ”very low” to ”very high”, to indicate the impact of a specific incident on the respective organization. Additionally, a Mealy automaton operates on input and output signals. The input signals can be interpreted as events or threats acting on the respective organization or asset. According to an event, the state of the automaton can change, e.g., from ”1” to ”2”, to

describe an event with a small impact or from ”1” to ”5” to describe an event with a big impact. Since the effects will in general not be deterministic in a realistic environment, the transitions from one state to another have a specific probability. Accordingly, the state can change from ”1” to ”2” with a high probability and from ”1” to ”5” with a low probability to indicate the fact that small impacts are more likely, but big impacts can occur as well. The output signals can be understood as events that occur after the state change and can depend on the input event as well as on the resulting state. These output signals can then be taken as input events for the depending nodes, i.e., for the organizations or assets that are connected by an edge in the interdependency graph.

This automaton model has been implemented in the tool CASSANDRA [a], which allows to simulate the cascading effects of an incident throughout the entire value chain by following the propagation of signals from one partner in the value chain to another. As a result, CASSANDRA provides an overview on the final state of each partner and thus an estimation on how much the entire value chain is affected by a single incident. Since the effects of an event on a node are probabilistic, a large number of simulation runs will provide an accurate estimation on the worst, best and average case of the consequences on the value chain.

5. Combined Risk and Robustness Model

In order to capture risk and robustness, we are building on an existing framework called the ODYSSEUS Risk and Resilience Framework (ORRF), that previously has been developed as part of the ODYSSEUS project in Schauer et al. (2021). The ORRF builds upon a classical risk management process similar to the ISO 31000 International Standardization Organization (2018) or the ISO 27005 International Standardization Organization (2022) but has some significant changes: first, it has a strong focus on the simulation of threat scenarios making use of the cascading effects simulation from Section 4; second, it integrates two assessment branches, one for risk and one for resilience; and third, it combines the two branches in the end to evaluate the best options to treat risk and resilience at the same time.

Translating the established ORRF to the context of value chains, the first two steps ”Context Establishment” and ”Hazard Identification” are directly covered by the first steps of the Value Chain Analysis described in Section 3 (cf. also Fig. 3). In particular, the ”Definition of the Main Reference Point” is a critical part in the ”Context Establishment” as it frames the entire perspective of the assessment process. Further, the ”Definition of the Value Chain” together with the ”Definition of the Influencing Factors” mainly contribute both to the ”Hazard Identification”. On the one hand, a strong effort is put on identifying the most relevant organizations and parts of the value chain, including not only the direct supplier-consumer relations but also orthogonal factors such as packaging, transport, maintenance or legal aspects. On the other hand, the influences and relations among these relevant organizations and parts in the value chain are captured, in the end providing the interdependency graph that is required for the simulation of the cascading effects. Additionally, also the influences from external hazardous events are identified which then lead to the list of potential threats that will later on be analyzed in the scenarios.

As already mentioned above, a core aspect of the process is the parallel assessment of risk and robustness (cf. Fig. 3). The part of risk assessment follows the classical analysis of the threats that were identified as part of the Value Chain Model (cf. Section 3), i.e., estimating the likelihood and consequences for each individual threat scenario. Whereas the likelihood is usually based on expert opinions or can be deduced from existing statistics and historical data, the consequences are based on the results coming out of CASSANDRA (cf. Section 4). In detail, after a large number of simulation runs for a particular threat scenario, a statistical overview on the expected final state of each individual organization and part of the value chain can be obtained. Where possible, the expected final state can also be weighted with some criticality

[a] Online accessible at https://risk-mgmt.ait.ac.at/cassandra

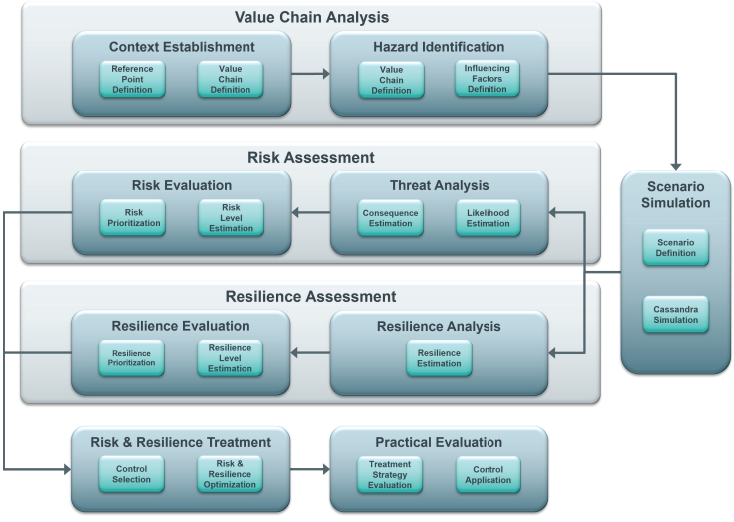

Fig. 3. Illustration of the combined Risk and Resilience Process Model (adapted from Schauer et al. (2021)).

score (i.e., how important the organization or part is for the entire value chain) or some loss (i.e., how much damage a limitation or failure of the organization or part would cost) to get a more tailored estimation of the consequences. By combining the results from all of these organizations or parts, we obtain the overall consequences of the threat scenario for the entire value chain.

The part of the robustness assessment also estimates the robustness level of the entire value chain for each threat scenario. Therefore, the estimation is also based on the outcomes from the cascading effects analysis. However, the final state of each individual organization or part of the value chain is only one aspect of the robustness estimation and is connected to the consequences computed in the risk assessment. The interpretation would be as follows: the more severe the final state of an organization or part of the value chain, the lower the robustness. The second important part is the evolution of the states over the individual steps of the simulation, i.e., over time of the threat scenario. The interpretation would be the following: the longer it takes, i.e., the more steps are required, to bring an organization or part into a worse state, the higher the robustness.

As already mentioned in Section 4 above, the CASSANDRA simulation also provides the best and worst case from the analysis together with the average case. This gives a lower and upper bound on the consequences as well as on the robustness level and thus reconnects with classical risk management at this point. The different assumptions made in the simulation translate to different threat scenarios and the worst, average and best case represent different severity of a threat scenario in the risk assessment. Accordingly, risks could be prioritized based on the average case, worst case or any (weighted) combination of all three values, depending on the operator's needs and requirements. These upper and lower bounds also support and improve the selection of treatment options, as the operator can evaluate all three bounds and thus get a better estimation for the improvement gained by one or a combination of several treatment measures.

6. Conclusion and Outlook

The main complexity drivers for a general formulation of a supply chain security analysis are interdependencies and cascading effects triggered by external influences. These manifest themselves in external threats that affect the vulnerabilities of the system and can subsequently be assessed, i.e., quantified, as risks. In order to address these relationships as efficiently as possible, our approach

presented here combines three approaches - the Value Chain Analysis Model (cf. Fig. 1), the CASSANDRA model (cf. Fig. 2) and the ODYSSEUS Risk and Resilience Process Model - to create a Systemic Assessment Framework (cf. Fig 3).

Particularly through the extensive use of iteration in various phases, this process is successively refined with repeated feedback loops, and the informative value is improved:

- Development of a general image of the value chain that stands up to the assessment of (internal) experts and (external) observers (Value Chain Analysis Model).
- Implicit distillation of the key influencing factors, which in turn represent the determining factor for the robustness analysis (Value Chain Analyses Model).
- Simulation and testing of possible cascading effects via these influencing factors through ongoing repetitions in order to analyze the behavior of the value network under external influence (CASSANDRA simulation model).
- Determination of the average final state (i.e., impact) of the actors involved in the value creation network, which can be understood as a measure of robustness, achieved by repeated threat scenario simulation (ODYSSEUS Risk and Resilience Process).

Based on this process model, targeted measures and controls can then be derived that address and protect the identified influencing factors. For future research activities, we plan to adopt the effect of these measures in a further step and thus - also via the key aspect of iteration - include their effectiveness in the assessment of the entire value chain. Furthermore, the monitoring aspect of the risk and robustness framework is a focus of future research activities. Considering also the efforts and costs for these measures, the most effective ones, both financially and in terms of their application, can be derived.

Acknowledgement

This work was supported by the research project MERCURIUS (Project-Nr. FO999905306), which is funded by the Austrian National Security Research Program KIRAS (http://www.kiras.at/) of the Austrian Federal Ministry of Finance (BMF).

References

Alarabiat, A. and I. Ramos (2019). The delphi method in information systems research (2004-2017). *Electronic Journal of Business Research Methods 17*(2), pp86–99.

Chowdhury, P., S. K. Paul, S. Kaisar, and M. A. Moktadir (2021). Covid-19 pandemic related supply chain studies: A systematic review. *Transportation Research Part E: Logistics and Transportation Review 148*, 102271.

European Comission (2022a, December). CRE Directive (2022/2557). *Official Journal of the European Union* (L 333/164).

European Comission (2022b). NIS 2 Directive (2022/2555). *Official Journal of the European Union* (L 333/80).

European Comission (2024). Cyber Resilience Act (2024/2847). *Official Journal of the European Union 2024/2847*.

Gurbuz, I. B. and G. Ozkan (2020). Transform or perish: Preparing the business for a postpandemic future. *IEEE Engineering Management Review 48*(3), 139–145.

Handfield, R. B., G. Graham, and L. Burns (2020). Corona virus, tariffs, trade wars and supply chain evolutionary design. *International Journal of Operations & Production Management 40*(10), 1649–1660.

Henderson, J. (2024, March). The Impact of the Russia-Ukraine War on Global Gas Markets. *Current Sustainable/Renewable Energy Reports 11*(1), 1–9.

Holland, J. H. (1984). Genetic algorithms and adaptation. In O. G. Selfridge, E. L. Rissland, and M. A. Arbib (Eds.), *Adaptive Control of Ill-Defined Systems*, pp. 317–333. Boston, MA: Springer US.

International Standardization Organization (2018). ISO 31000:2018 Risk management. Technical report, International Standardization Organization (ISO), Geneva, Switzerland.

International Standardization Organization (2022). ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection. Technical report, International Standardization Organization (ISO), Geneva, Switzerland.

Ishida, S. (2020). Perspectives on supply chain management in a pandemic and the post-covid-19 era. *IEEE Engineering Management Review 48*(3), 146–152.

Ivanov, D. and A. Dolgui (2020). Viability of intertwined supply networks: extending the supply chain resilience angles towards survivability. a position paper motivated by covid-19 outbreak. *International Journal of Production Research 58*(10), 2904–2915.

Jagtap, S., H. Trollman, F. Trollman, G. Garcia-Garcia,

C. Parra-López, L. Duong, W. Martindale, P. E. S. Munekata, J. M. Lorenzo, A. Hdaifeh, A. Hassoun, K. Salonitis, and M. Afy-Shararah (2022, January). The Russia-Ukraine Conflict: Its Implications for the Global Food Supply Chains. *Foods 11*(14), 2098. Number: 14 Publisher: Multidisciplinary Digital Publishing Institute.

Kakaei, H., H. Nourmoradi, S. Bakhtiyari, M. Jalilian, and A. Mirzaei (2022). Effect of COVID-19 on food security, hunger, and food crisis. *COVID-19 and the Sustainable Development Goals*, 3–29.

Katoch, S., S. S. Chauhan, and V. Kumar (2021). A review on genetic algorithm: past, present, and future. *Multimedia Tools and Applications 80*(5), 8091–8126.

Kumar, P., R. K. Singh, J. Paul, and O. Sinha (2021). Analyzing challenges for sustainable supply chain of electric vehicle batteries using a hybrid approach of delphi and best-worst method. *Resources, Conservation and Recycling 175*, 105879.

König, S., S. Rass, B. Rainer, and S. Schauer (2019). Hybrid Dependencies Between Cyber and Physical Systems. In K. Arai, R. Bhatia, and S. Kapoor (Eds.), *Intelligent Computing*, Volume 998, pp. 550–565. Cham: Springer International Publishing.

Paul, S. K. and P. Chowdhury (2021). A production recovery plan in manufacturing supply chains for a high-demand item during covid-19. *International Journal of Physical Distribution & Logistics Management 51*(2), 104–125.

Rahnamay-Naeini, M. and M. M. Hayat (2016, July). Cascading Failures in Interdependent Infrastructures: An Interdependent Markov-Chain Approach. *IEEE Transactions on Smart Grid 7*(4), 1997–2006.

Schaberreiter, T., P. Bouvry, J. Röning, and D. Khadraoui (2013). A Bayesian Network Based Critical Infrastructure Risk Model. In O. Schütze, C. A. Coello Coello, A.-A. Tantar, E. Tantar, P. Bouvry, P. Del Moral, and P. Legrand (Eds.), *EVOLVE - A Bridge between Probability, Set Oriented Numerics, and Evolutionary Computation II*, Volume 175, pp. 207–218. Berlin, Heidelberg: Springer Berlin Heidelberg.

Schauer, S., T. Grafenauer, S. König, M. Warum, S. Rass, and S. Rass (2020). Estimating Cascading Effects in Cyber-Physical Critical Infrastructures. In *Critical Information Infrastructures Security*, Lecture Notes in Computer Science, Linköping, Sweden, pp. 43–56. Springer International Publishing.

Schauer, S., M. Latzenhofer, S. König, and S. Rass (2021). Conceptual Approach Towards a Combined Risk and Resilience Framework for Interdependent Infrastructures. In *Proceedings of the 31st European Safety and Reliability Conference (ESREL 2021)*, Angers, France, pp. 2161–2171.

Schauer, S. and S. Rass (2020). Creating a Cross-Domain Simulation Framework for Risk Analyses of Cities. In J. Staggs and S. Shenoi (Eds.), *Critical Infrastructure Protection XIV*, IFIP Advances in Information and Communication Technology, Cham, pp. 307–323. Springer International Publishing.

Sheth, J. N. and C. Uslay (2023, November). The geopolitics of supply chains: Assessing the consequences of the Russo-Ukrainian war for B2B relationships. *Journal of Business Research 166*, 114120.

Su, Z. (2024, January). Impact of COVID-19 lockdown on vessel traffic in Shanghai Port: a spatial-temporal analysis and implications for shipping and transport logistics. *International Journal of Shipping and Transport Logistics 19*(1), 57–81. Publisher: Inderscience Publishers.

Wang, D. and W. H. Ip (2009). Evaluation and analysis of logistic network resilience with application to aircraft servicing. *IEEE Systems Journal 3*(2), 166–173.

Wang, L. and C. Su (2025, February). Port congestion and resilience in Shanghai during the Citywide lockdown. *Ocean & Coastal Management 261*, 107501.

Ye, L. and M. Abe (2012). The impacts of natural disasters on global supply chains. Working Paper 115, ARTNeT Working Paper Series.

Zhang, Z., P. R. Srivastava, P. Eachempati, and Y. Yu (2023). An intelligent framework for analyzing supply chain resilience of firms in china: a hybrid multicriteria approach. *The international journal of logistics management 34*(2), 443–472.