Control of Systemic Risks in Global Networks – A Grand Challenge to Information Systems Research

Fabian Lorig[1], Ingo J. Timm[1], and Peter Mertens[2]

[1] Trier University, Center for Informatics Research and Technology, Trier, Germany
{lorigf,itimm}@uni-trier.de
[2] Friedrich-Alexander-University Erlangen-Nürnberg,
Wirtschaftsinformatik I, Nürnberg, Germany
peter.mertens@fau.de

Abstract. The emergence of global networks also results in the occurrence of systemic risks that might affect the stability of the overall system. To cope with these risks, this workshop on the "Control of Systemic Risks in Global Networks" provides a platform for the collection and discussion of innovative approaches, methods, and theories but also of practical problems from the areas of simulation, artificial intelligence, operations research, and statistics. This enables the exchange of experiences and methods between scientists and practitioners.

Keywords: Grand Challenge, Systemic Risk, Reference Framework.

1 Introduction

Modern communication networks lead to a stronger coupling of and interdependency between social and economic areas. Examples are electronic marketplaces, which enable ever faster transactions, worldwide production networks, which allow for higher specialization with increasing efficiency, and *smart grids*, which facilitate the provision of energy in the European Single Market by means of flexible control. The resulting worldwide and interconnected networks increasingly decide on the competitiveness of enterprises.

On the one hand, this development is promoted by a strong **demand pull** for innovative technologies that emanates from companies. This results from the companies' endeavor to take advantage of environmental differences in a "globalized world". Examples are increasing sales opportunities in emerging countries, low labor costs, special competences in the development and production of electronic components or software products, discoveries of raw materials, and tax conditions.

On the other hand, there is an increasing **technology pressure**. This is due to an increasing performance-cost ratio of data management as well as from the fact that modern multi and manycore systems accelerate or initially enable the solving of sophisticated planning, disposition, and control algorithms. Moreover, the advancement of traditional methods, e.g., artificial neural networks and deep learning,

14th International Conference on Wirtschaftsinformatik,
February 24-27, 2019, Siegen, Germany

allows for the discovery of patterns and the investigation of systems that remained hidden or were inaccessible before.

Along with these worldwide networks, *systemic risks* emerge which affect the stability of the overall system [1]. Examples of potential failures are flash crashes in high-frequency trading, production downtime due to delivery delays, or blackouts in energy networks. For instance, on September 28th, 2003, power plant failures in Italy lead to disruptions of the Internet infrastructure, which relied on energy supply and at the same time was required to control other power plants. This resulted in a cascade of failures and has nearly caused the collapse of the entire Italian energy supply [2,3].

Obviously, not all risks are equivalent with respect to their probability of occurrence and of the consequences. Thus, those *systemic risks* must be identified, which – as illustrated by the example – affect the stability of the overall system and are not considered as part of the risk assessment of the independent subsystems. Here, the extent of the risk must be considered as well as the probability of finding an adequate countermeasure with reasonable effort.

In a joint initiative, which is steered by the *German Informatics Society* (Gesellschaft für Informatik; GI), Information Systems Research and Computer Science have selected the *control of systemic risks in global networks* as one of the five most important Grand Challenges for the future [4]. From an information system research perspective, two major interests can be identified: On the one hand, the availability as well as the situational aggregation and interpretation of decision-relevant information and on the other hand the autonomous identification, quantitative estimation, and flexible reaction to risks.

2 Current Technology Pressure

In information system as well as computer science research, there are ongoing discussions whether networks can be designed or dynamically emerge from the interaction of devices with network technologies: Worldwide networks are not designed as part of an "engineering process", they are created through the interaction of interconnected systems as emergent phenomenon and must be described and understood [5].

The need for a development of methods for the design of such networks can be identified when investigating the current technology pressures. Developments that can contribute to the control of systemic risks include but are not limited to:

1. **Communication Networks**: Advances in communication networks, e.g., an increasing performance-cost ratio of communication channels (hardware) and greater flexibility in routing (software), which allow for prioritized communication in case of emergency.
2. **Simulation**: Recent developments in simulation from a tool for planning support to a real-time assistance for decision support through the development of innovative formalisms, e.g., system dynamics or agent-based simulation, and due to the immediate availability of current data.

3. **Machine Learning**: Revolutionary progress in machine learning that is facilitated by the increasing availability and amount of (training) data as well as shift from multi to multi and manycore computing. This allows for the use of deep learning, convolutional neural networks as well as data, text, and opinion mining techniques.
4. **Decentralized Control**: The availability of approaches for decentralized and adaptive control with autonomous software agents, multiagent systems, and organic computing promotes the high-tech strategy "Industry 4.0".
5. **Transaction Processing Systems (Blockchain)**: New forms of transaction processing systems, e.g., blockchain, allow for the tamper-resistant and decentralized organization and logging of safety-critical operations in processes such as access or updates of sensitive data.
6. **Multilayer and Multiplex Networks**: A shift from the analysis of isolated and homogenous networks to the investigation of multilayer and multiplex networks (interdependent networks).
7. **Convergence**: The convergence of technical systems and processes leads to the unification of business models and technologies across sectors. Through this, technical and economic success of one domain might dominate another domain, e.g., successful business models of internet giants can compete with stationary trade in the physical world even though the horizon of experience is considerably lower.

Due to disciplinary barriers, the aforementioned technology areas are not yet sufficiently developed, applied, or transferred for controlling systemic risks. This limits the opportunities for action that can be undertaken to prevent the potentially dramatic consequences of systemic risks. Still, these technologies have a high potential to contribute as component of a solution for controlling systemic risks.

Considering disaster management strategies, for instance, it can be illustrated how disciplines can learn from each other and benefit from the experiences of other disciplines. Insurance companies make use of reinsurances to handle major claims which could result in their insolvency. Such approaches are also applicable to supply chain management as protection against supply shortages that might result in disruptions of the own production of goods. In this regard, supply chain management can also learn from insurances as systemic risks emerge from networks of reinsurances which can potentially result in uncontrollable chain effects that lead to global crises.

3 Reference Framework

Suitable technologies and methods for controlling systemic risks are diverse. Thus, to classify and distinguish different approaches, we suggest the use of a morphological box. It serves as a reference framework for discussion within the workshop as approaches can be classified and assessed according to different dimensions. In Figure 1, the morphological box is illustrated that is used for the assessment of the approaches

that are presented as part of this workshop. For each approach, the aspects of *networks*, *risks*, and *decision situation* are focused.

To this end, the domain focus of the workshop lies on *logistics*, *finance & insurances*, and *public services*, yet, also contributions from other domains are welcome. With respect to the type of risk that is addressed by the approaches, it can be differentiated into five types, according to the domain the risk is related to: *production*, *market*, *finance*, *institution*, and *nature*. In addition, also the occurrence of the risk is classified as *regularly*, *periodically*, or *rarely*. Finally, the decision situation of the risk can be specified according to the risk's predictability as well as by the authority which is the decision maker.

Network	***Domain***	Logistics			Finance & Insurances			Public services	
	Network model	Available and fixed		Available and ongoing change		Situation-dependent change		Ad-hoc	
Risk	***Type of risk***	Production	Market		Finance		Institutional		Nature
	Occurrence	Regularly			Periodically			Rarely	
Decision situation	***Predictability***	Predictable and plannable		Predictable and not plannable		Not predictable but plannable		Not predictable and not plannable	
	Authority	Single person		Committee		Automated, with intervention of persons		Fully automated	
	Horizon	Enterprise			Network			Society	

Figure 1: Reference framework for the classification and discussion of approaches.

4 Discussion

To address the Grand Challenge of controlling systemic risks in global networks, this workshop aims at both the collection and discussion of innovative approaches, methods, and theories but also practical problems from the areas of simulation, artificial intelligence, operations research, and statistics. To this end, the goal of the workshop is to provide a platform for the exchange of experiences and methods between scientists and practitioners. Moreover, the development of a medium-term research agenda shall be promoted for targeting this Grand Challenge.

5 Acknowledgements

We would like to thank all those that contributed to the initiative on "Control of Systemic Risks in Global Networks" for their fruitful comments and innovative ideas.

References

1. Buldyrev, S. V., Parshani, R., Paul, G., Stanley, H. E., & Havlin, S. (2010). Catastrophic cascade of failures in interdependent networks. In: Nature, 464 (p. 15).

2. UCTE (2004). FINAL REPORT of the Investigation Committee on the 28 September 2003 Blackout in Italy. UCTE Report – April 2004.
3. Johnson, C. W. (2007). Analysing the causes of the Italian and Swiss blackout, 28th September 2003. In *Proceedings of the twelfth Australian workshop on Safety critical systems and software and safety-related programmable systems. Volume 86* (pp. 21-30). Australian Computer Society, Inc.
4. Mertens, P. & Barbian, D. Business & Information Systems Engineering (2015) 57: 391.
5. Gkantsidis, C., Mihail, M., & Saberi, A. (2003). Conductance and congestion in power law graphs. In: ACM SIGMET-RICS Performance Evaluation Review Vol. 31, No. 1 (pp. 148-159), ACM.