Springer Series in Reliability Engineering

Per Hokstad
Ingrid B. Utne
Jørn Vatn *Editors*

Risk and Interdependencies in Critical Infrastructures

A Guideline for Analysis

Springer

Springer Series in Reliability Engineering

Series Editor

Hoang Pham

For further volumes:
http://www.springer.com/series/6917

Per Hokstad · Ingrid B. Utne
Jørn Vatn
Editors

Risk and Interdependencies in Critical Infrastructures

A Guideline for Analysis

Springer

Editors
Per Hokstad
Safety Research
SINTEF
Trondheim
Norway

Ingrid B. Utne
Department of Marine Technology
Norwegian University of Science
and Technology
Trondheim
Norway

Jørn Vatn
Department of Production and Quality
Engineering
Norwegian University of Science
and Technology
Trondheim
Norway

ISSN 1614-7839
ISBN 978-1-4471-4660-5 ISBN 978-1-4471-4661-2 (eBook)
DOI 10.1007/978-1-4471-4661-2
Springer London Heidelberg New York Dordrecht

Library of Congress Control Number: 2012953014

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

Technology comprises much more than the products and systems that shape our environment. Today our living, working, transportation, and communication are based on large coupled networks. The functioning of our society is completely dependent on these networks or critical infrastructures, such as electricity supply, water supply, oil and gas production, transportation, banking and finance, and information and communication technologies (ICT). Risk and vulnerability analyses are needed to grasp the impact of threats and hazards. However, these become quite complex, as there are strong interdependencies both within and between the infrastructure systems. The interdependencies can cause redundant systems to fail simultaneously due to common cause failures; one system can fail due to failure of another system and thereby increased load; and finally, if the service of one infrastructure is depending on another (say electricity) there can be a direct cascading effect of a failure.

This book provides a theoretical basis and a practical guideline for analyzing interdependencies and risks in critical infrastructures. Examples and case studies for several infrastructures are included for illustrating the areas of application. Various risk and vulnerability analysis techniques are adapted to different infrastructures. The book describes the identification of hazards that are threatening infrastructures, and enhances the understanding of how these threats can propagate throughout the system and affect other infrastructures. It is mainly aimed at users with limited experience in risk analysis of critical infrastructures, to enable use of the methods in real world problems. The methods are presented describing the inputs needed for the analysis, the type expertise to draw upon, and expected results from doing these kinds of analyses.

The book provides essential reading for municipalities and infrastructure owners who need knowledge about the risks and vulnerabilities of their critical infrastructures, to avoid hazardous events and plan for emergency preparedness. It should also be a valuable reading for consultants and researchers in the area, and could serve as a supplementary curriculum and reading for master students in risk analysis.

The book starts out with a couple of introductory chapters. Chapter 1 gives an overview of some methods and approaches for investigating interdependencies in critical infrastructures, and some literature is briefly reviewed. Main concepts—like risk, vulnerability, critical infrastructure, and different types of interdependencies—are further elaborated in Chap. 2. Chapter 3 outlines a generic "risk and vulnerability analysis" that could serve as a basis for investigating the hazards and risks of an infrastructure system. This analysis should conclude with suggesting risk reducing measures and identification of needs for more detailed analysis through the use of more advanced methods.

Chapter 4 presents a generic method for identifying and analyzing interdependencies, and provides an example applied to railway, electricity supply, and ICT (based on an actual event at the Central station (railway/bus) of Oslo, Norway). The modeling of interdependencies is also the topic of Chaps. 5 and 6. A modeling framework for interdependent technical infrastructures and types of vulnerability analyses, distinguishing between global vulnerability analysis, critical component analysis, and geographic vulnerability analysis, is described in Chap. 5. Chapter 6 utilizes the framework and types of analyses from Chap. 5 and presents two case studies on an interdependent electric distribution and water distribution system in a city and on an interdependent railway system in southern Sweden.

Chapters 7 and 8 treat risk analyses of electricity supply systems. Chapter 7 describes an analytical approach for the analysis of electricity supply, investigating the consequences of supply interruptions, and Chap. 8 presents three case studies using results of previous chapters in the book. The topic of Chap. 9 is the integrated urban water supply. Challenges faced by the water utilities to provide safe, secure, and reliable service are discussed, and risk analysis models are presented.

The analysis of ICT is treated in Chap. 10. In particular, the dependencies between ICT and other critical infrastructures are addressed. Further, main threats toward ICT systems are explained, and various risk analysis techniques are presented. Chapter 11 discusses risk in maritime transport systems and interdependencies within the transport system, as well as to other infrastructure systems. An example on LNG (liquefied natural gas) transport is presented in Chap. 12.

The last two chapters treat challenges for management. Chapter 13 presents human reliability management and the importance of infrastructure resilience, illustrated by an empirical study of joint stressful conditions for control room operators in electricity supply and water supply systems in California. Chapter 14 concludes the book by discussing organizational challenges regarding risk management in critical infrastructures.

Several chapters of the book are to a large extent based on results from the research project DECRIS (Risk and Decision Systems for Critical Infrastructures), which was funded by the Norwegian Research Council and carried out in close cooperation with the municipality of Oslo.

Trondheim, 2012

Per Hokstad
Ingrid Bouwer Utne
Jørn Vatn

Contents

Chapter 1
A Brief Overview of Some Methods and Approaches for Investigating Interdependencies in Critical Infrastructures

Ingrid Bouwer Utne, Henrik Hassel and Jonas Johansson

Abstract This chapter presents methods for analysing interdependencies in critical infrastructures. In general, there are three groups of methods for analysing interdependencies; (1) conceptual, (2) model and simulation and (3) empirical and knowledge-based approaches. Examples of methods belonging to these groups are presented. The latter part of the chapter discusses challenges related to modelling, focusing on how to deal with complexity, trade-offs between abstraction and fidelity, choice of consequence measures and obtaining information.

1.1 Introduction

In recent years, several different types of methods for analysing interdependencies in critical infrastructures have been published; see, for example, Pederson et al. [1] for an overview. Some of these analyses have been used as input to the approaches presented in this book, whereas others represent alternatives. Still, researchers (e.g. Kröger [2]) emphasize the need for more extended analyses of interdependencies, and pinpoint challenges related to the use of traditional risk analysis methods in the analysis of large and complex infrastructures.

I. B. Utne (✉)
Department of Marine Technology, Norwegian University of Science and Technology (NTNU), Trondheim, Norway
e-mail: ingrid.b.utne@ntnu.no

H. Hassel
Department of Fire Safety Engineering and Systems Safety, Lund University, Lund, Sweden

J. Johansson
Department of Measurement Technology and Industrial Electrical Engineering, Lund University, Lund, Sweden

P. Hokstad et al. (eds.), *Risk and Interdependencies in Critical Infrastructures*, Springer Series in Reliability Engineering, DOI: 10.1007/978-1-4471-4661-2_1,

In general, the work related to failures and interdependencies in critical infrastructures can be divided into three groups:

1. Conceptual approaches, mainly providing definitions and classifications of important concepts related to critical infrastructure and interdependencies, also presenting categories of interdependencies and factors affecting these.
2. Model and simulation approaches, using (advanced) quantitative techniques to investigate interdependencies and visualize effects of failure.
3. Empirical and knowledge-based approaches, providing models and results based on empirical data and real events in the past.

Most of the chapters in this book belong to the group two types of approaches. Chapter 13 by Roe and Schulman is one exception and can be classified as an empirical approach. Below some literature related to each of these groups are reviewed.

1.2 Group 1: Conceptual Approaches: Definitions and Classifications

There are several publications that treat the subject of defining and classifying what constitutes *critical infrastructures* and the concept of *interdependencies*. Below an overview of some of the most influential work within this area is given.

Rinaldi et al. [3] refer to the following definition of critical infrastructure:

> The framework of interdependent networks and systems comprising identifiable industries, institutions (including people and procedures) and distribution capabilities that provide a reliable flow of products and services essential to the defence and economic security of the United States, the smooth functioning of governments at all levels, and society as a whole.

Luiijf and Klaver [4] refer to the EU communication on critical infrastructure protection (2004), which defines critical infrastructures as "those physical and information technology facilities, networks, services and assets which, if disrupted or destroyed, have a serious impact on the health, safety, security or economic well-being of citizens or the effective functioning of governments". The EU Green Paper [5] includes the sectors; energy, ICT, water, food, health, financial, public and legal order and safety, civil administration, transport, chemical and nuclear industry and space and research, as critical infrastructures.

There are various types of interdependencies discussed in the literature. Some papers distinguish between *dependencies* and *interdependencies*. Rinaldi et al. [3] define interdependencies between infrastructures as a bidirectional relationship and dependencies as unidirectional. Bidirectional relationships means that the state of one infrastructure affects or is correlated according to the state of another infrastructure. The infrastructure characteristics focus on the system hierarchy, timescales, operating procedures, training and redundancy, as well as ownership and regulations. Failures can be cascading, escalating and common cause and state of operation may vary from optimal operation to total failure.

Rinaldi et al. [3] present a framework of six dimensions to describe and analyse interdependencies: (1) type of interdependencies, (2) surroundings, (3) coupling and response behaviour, (4) infrastructure characteristics, (5) type of failures and (6) state of operation.

They also define four categories of interdependencies:

1. *Physical* interdependency—physical coupling between inputs and outputs, for example, a commodity produced/modified by an infrastructure is required by another infrastructure to function.
2. *Cyber* interdependency—the state of the infrastructure depends on the information transmitted through the information infrastructure.
3. *Geographical* interdependency—one or several elements of infrastructures are in close proximity so that one event (e.g. fire) creates disturbances to the infrastructures.
4. *Logical* interdependency—two or more infrastructures have reciprocal effects without any physical, geographical or cyber interdependency.

Zimmerman [6, 7] distinguishes between *spatial* and *functional* interconnectedness and dependency. Spatial interconnectedness refers to proximity between infrastructures as the most important relationship between the systems. Functional interconnectedness refers to a situation in which an infrastructure is necessary for operation of another infrastructure, for example, the pumps in a water treatment systems needing electricity in order to function. There are also commonly situations with both types of interconnectedness, for example, wireless communication.

Zimmerman [7] describes three important *factors* related to interdependency between infrastructures:

1. Interconnectedness/couplings, which affect how failures propagate through the systems.
2. Redundancy, affecting alternative ways of restoring system functioning.
3. System knowledge, which, for example, enables identification of threats.

Bagheri and Ghorbani [8] present a framework which attempts to unify and consolidate current research on analysis of interdependencies. The framework is five-dimensional, consisting of system analysis (e.g. risk management), behaviour analysis (e.g. simulation models), knowledge discovery (e.g. hypothesis testing), visualization (e.g. visualization of analysis data) and information sharing (e.g. rules and regulations).

1.3 Group 2: Model and Simulation Approaches

Several advanced approaches model or simulate the behaviour of a group of coupled infrastructures in order to evaluate how disturbances cascade through the systems and impact the different infrastructures involved.

A risk-based interdependency assessment process for infrastructures is presented in Brown et al. [9]. The iterative process can be supported by different

simulation tools, such as system dynamics and agent-based modelling. System dynamics modelling is used to simulate connections between the infrastructures, track commodities and identify vulnerabilities. Existing data and projections of system operation and supply requirements under different events and performance variations at various locations and environmental conditions are simulated and quantified. In agent-based modelling, an agent is used as a model of a real-world decision maker. According to Brown, an agent is a "self-contained piece of code that uses a genetic algorithm to learn how to interact with other agents in order to maximize its utility". The actions of each agent depend upon the actions of other agents, and the overall performance of the system depends on the competition and coordination under defined constraints.

Haimes et al. [10] present inoperability input–output model (IIM) for interdependent infrastructures, based on the Leontief economic model. There are several different applications of the IIM in the research literature. In Crowther [11], an IIM focuses on economic interdependencies due to transactions of goods and services between different operational sectors and economic regions. IIM is in Crowther used to calculate the direct trade-offs between preparedness costs and economic resilience of different regions.

Vulnerable locations to terrorist attacks in critical infrastructures and how to identify and prioritize such vulnerabilities are the focus in Apostolakis and Lemon [12]. The identification process uses network modelling, which often results in a large number of vulnerabilities to be screened and prioritized which is done in the paper by multiattribute utility theory (MAUT) and expected disutilities. Patterson and Apostolakis [13] use parts of this methodology, but analyse many more infrastructures and different types of users. Findings are presented in a graphical display showing the criticality of geographical areas, conditional on a given threat.

Ezell [14] presents the infrastructure vulnerability assessment model (I-VAM), which quantifies vulnerability. The model is based on MAUT and structured as a value model. It aggregates vulnerability scores for each component into values for each sub-system and finally for the total system.

A proactive method for risk management that focuses on interdependencies in critical infrastructures and cascading effects from failures is presented in Robert et al. [15]. They discuss different tools, such as a dependency matrix for assessing resources needed for a given system provided by other systems, and consequence curves to model impacts of degradation in a resource (e.g. water or electricity) on different infrastructures.

Vulnerabilities at a regional level are analysed by Myers and Sorrentino [16] by use of a geospatial mapping and visualization tool. Then, they apply network analysis to investigate the identified vulnerabilities of the infrastructures and their criticalities across sectors.

Nan et al. [17] address the need for advanced modelling and simulation methods to understand the interdependencies and complexities in critical infrastructures. They present a hybrid simulation approach which tries to prevent extensive use of computational resources by dividing the overall simulation

platform into different simulation models at first and then integrating them in the architecture of distributed networks.

Johansson and Hassel [18] present a modelling framework for understanding and analysing interdependent critical infrastructures. The framework is applied in Johansson et al. [19] for an interdependent system, namely the railway infrastructure in the southern parts of Sweden. Chapter 5 of the present book gives an overview of this method, and in Chap. 6, the framework is used for vulnerability analysis of two different interdependent systems.

1.4 Group 3: Empirical and Knowledge-Based Approaches

An alternative approach to the simulation methods is to study statistical data and actual events and to define measures which summarize characteristic features of these. Such approaches may reveal patterns with respect to political decisions, consequences for society or on the failure propagation between various infrastructures. Some of these approaches can be used as a basis for the simulation and modelling approaches.

Zimmerman and Restrepo [20] discuss the use of quantitative metrics for measurements of interdependencies, and cascading effects between critical infrastructures are suggested, for example, the number of times infrastructure i caused damage to other infrastructures j, k,…,n divided by the number of times infrastructure j, k,…,n damaged infrastructure i.

Major electrical power outages are investigated to understand how extreme events may lead to failures of other infrastructure systems in McDaniels et al. [21]. They present a framework that (1) defines the context and conditions in which an initial infrastructure failure has occurred, (2) describes the type of interaction and context leading to an infrastructure failure interdependencies (IFI) event and (3) assesses type of societal consequences and severities related to the IFI event. In order to produce probabilities for an IFI event, data from databases, expert opinions and/or simulations are needed. The framework aims at providing a basis for future probabilistic risk analyses.

Cox [22] sets priorities for protecting US infrastructures against terrorist attacks. Use of methods like decision tree, project planning models of terrorist attacks and hierarchical optimization are suggested.

Kröger [2] describes couplings between electricity supply, gas, railways, ICT and urban water by using an assessment matrix. Colours illustrate the strength of the dependencies, for example, electric-powered railway is dependent on continuous electricity, and thus, these cells are marked red. Regarding other infrastructures, the dependency is moderate, so these cells are marked yellow. Green indicates a low dependency.

Rahman et al. [23] have investigated 347 infrastructure failure cases from 1994 to 2005 to determine their causes and impact on critical infrastructures, including propagating effects. They also discuss the limitations of public reports, which often are too brief to really find out the specific failures.

Li et al. [24] provide an overall framework including probabilistic risk assessment (PRA), decision analysis and expert judgment, involving stakeholders and decision makers in every step. The framework develops scenarios described by event trees, and probabilities are assigned based on statistics, expert interviews and stakeholder inputs. MAUT is used to evaluate the impact of failures and their consequences for stakeholders, and use of performance indices.

Zio et al. [25] present an all-hazard analysis which considers intentional man-made acts, as well as natural and accidental hazards. The analysis uses tables for identifying characteristics, operational modes and failure modes relevant for assessing vulnerability of critical infrastructures. An example, using the IEEE96 reliability test system, is used for demonstrating the analysis.

There exist a lot of data about infrastructure performance in the past, but it may be hard to utilize such data for determining future situations. In addition, the growing use of computer systems leads to increased amounts of data. Guikema [26] focuses on natural disaster risk analysis, using statistical theory, for example, regression methods, to deal with the large amounts of data and to provide a basis for risk analysis of critical infrastructures.

1.5 Challenges in the Modelling of Critical Infrastructures: Implications for this Book

The three approaches described above can clearly provide important information to decision-making about risks. The conceptual approaches (group 1) can provide concepts and frameworks that can be used in the other two approaches. The empirical/knowledge-based approaches (group 3) can reveal patterns of infrastructure breakdowns that have been observed in the past. A limitation of the empirical/knowledge-based approaches is of course that their reactive nature makes it difficult to address new situations and capture events that have not yet occurred; something which the model/simulation approaches (group 2) can address. At the same time, the empirical/knowledge-based approaches can provide important input to the model/simulation approaches regarding the characteristics of interdependencies between infrastructure systems.

Some of the most important challenges that one has to face when modelling and simulating critical technical infrastructures are how to:

- Deal with complexity,
- Deal with the trade-off between abstraction and fidelity,
- Measure consequences of undesired events,
- Obtain information.

1.5.1 Complexity

The largest challenge when it comes to modelling and simulating interdependent infrastructures is the vast complexity. Even if we only consider a single infrastructure, the complexity is significant. Extrapolating this to the system of systems, a set of interdependent critical infrastructures, the complexity manifolds. This complexity comes from several different sources:

1. **The size of the problem at hand**, that is, multiple large-scale systems interacting in multiple ways. The sheer size of the modelling problem is one source. The number of components that need to be addressed is large, and the appropriate level of detail is not obvious, that is a component can always be broken down into "sub-components" or aggregated with other components into "super-components". In addition, the interactions among components and infrastructures are extensive. This, of course, is the main reason why it is important to approach the modelling of critical infrastructures in a holistic way rather than looking at individual infrastructures in isolation. The holistic perspective makes it possible to identify higher-order effects, something that would otherwise be very difficult.
2. **The large variety of elements that need to be addressed**. The character of the components varies greatly, some being mainly technical, whereas some are human or organizational, that is, related to the operation or restoration of the critical infrastructures.
3. **The large variety in the timescales**. For example, some interactions between infrastructure systems enable disruptions to spread immediately, that is, there is a so-called tight coupling (using the terminology from Perrow [27]). This is the case, for example, when electric power disruptions instantaneously spread to disruptions in telecommunication components (given no back-up supply exist). Other interactions, however, act on an entirely different timescale—that is, they are "looser". For example, interrupted power supply to water pumping stations for a water tower will not give rise to negative effects in the water distribution system until the water tower is empty (typically in the order of hours), and interrupted delivery of fuel to combined heat and power plants will not spread until the fuel stocks are empty (in the order of days or weeks).

There is no straightforward answer to the question of how to deal with the large complexity. The first step, however, is realizing that a single approach will never cover everything of interest. As a consequence, it becomes very important to clearly state what the purpose and limitations of a particular approach actually are, so that potential users can determine whether an approach is useful or not.

1.5.2 Trade-off Between Abstraction and Fidelity

There are many ways of describing and modelling complex systems, for instance, concerning level of detail and to what extent physical and dynamical aspects are captured. On one hand, it is possible to use extremely detailed and advanced models, for example, sophisticated engineering models. Such an approach is likely to provide a simulation model of high fidelity, which means high correspondence between the model and actual system performance. The downside is that this requires very large resources to develop the model, to gather and process the vast amount of the required input data, and a considerable simulation time. On the other hand, it is possible to use very simplified and abstract models with the benefit of less data required as input and simulation times are very short. Examples of the latter approaches are, for example, Albert et al. [28] and Holmgren [29]. In these approaches, the system performance is generally approximated as the degree of "network connectedness". Such an approach would, for example, not make a difference between different types of components, but for many types of networks, the type of component matters significantly (i.e. which functions the components have). In an electric power distribution system, for example, there is a crucial difference between generators and stations supplying customers. If a station fails, only the customers connected to that station will lose power supply, whereas the loss of a generator can lead to many more customers without power supply. As such, the downside of too simplified and abstract models is that they do not capture enough of the relevant characteristics and behaviour of the systems.

It is clear that there exists a very difficult trade-off between fidelity and abstraction, and there is not much research performed when it comes to exploring such trade-offs. Among the exceptions are the papers by Hines et al. [30], Overbye et al. [31], Simonsen et al. [32]. However, these have only addressed electric power systems (with different points of departure) and are far away from providing clear-cut guidance. There is a need for at least including the basic physical and functional characteristics of the infrastructures in the modelling framework. Finding the appropriate trade-offs is something that always needs to be tailored to the particular context.

1.5.3 Consequence Measures

Another challenge when it comes to modelling critical interdependent infrastructures in the context of risk and vulnerability analysis is to choose an appropriate measure for characterizing the negative consequences of failure scenarios. This issue is largely interlinked with choosing a functional model, since the functional models to a large degree depicts the consequence measures. An example is if one uses simple functional models that only takes into account the topology of a power system, that is, only considering how nodes and edges are interconnected and not

their heterogeneity in terms of, for example, generation or load. It is then impossible to define the loss of load (MW) as the consequence measure.

Another example is if the analysis is related to improving the technical robustness of a water distribution system. Then it may be sufficient to choose a consequence measure (or several) that reflects direct consequences in the water distribution, such as the number of customers affected, and cubic metres of water not supplied. In some cases, it may be relevant to consider a larger societal context and to differentiate between what types of customers (industry, residential and hospitals) are impacted and to what extent society can continue to function without water supply. As such, choosing consequence measures must be done in conjunction with choosing functional models and the context in which the analysis is performed.

1.5.4 Obtaining Information

There are many challenges related to obtaining the information necessary to model critical infrastructures. The first challenge simply concerns the fact that large amounts of information are needed to perform simulations. The more advanced and detailed the model is the more information is needed. The second challenge concerns the high degree of confidentiality restrictions related to attaining the desired information. This issue is exacerbated by the fact that the responsibility and operation of infrastructures is fragmented across many actors and institutions in society (e.g. Amin [33], de Bruijne and van Eeten [34]). This is also discussed in Chap. 14 of the present book.

There is no simple answer to this challenge; however, generally it can be said that a precondition for analysing interconnected systems is that joint efforts by several actors must be initiated, or there must at least be a broad agreement among the infrastructure owners. In addition, due to possible limitations in collecting and getting access to relevant information, one may have to simplify the models used.

1.6 Conclusion

The vast complexity of large infrastructure systems implies that we will never end up with a single best perspective or approach when it comes to risk modelling in critical infrastructures. Different approaches are simply needed to address different aspects of the issues at hand. The present book provides a selection of approaches and perspectives for analysing the risk and vulnerability of critical interdependent infrastructures; and these approaches are differently suited depending on the needs and interests of the users.

References

1. Pederson, P., Dudenhoeffer, D. D., Hartley, S., & Permann, M. (2006). *Critical infrastructure modeling: A survey of U.S. and International Research*. Idaho National Laboratory, Idaho Falls.
2. Kröger, W. (2008). Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools. *Reliability Engineering and System Safety*, *93*, 1781–1787.
3. Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, *21*, 11–25.
4. Luiijf, E., & Klaver, M. H. A. (2005). *Critical infrastructure awareness required by civil emergency planning. Proceedings of the 2005 first IEEE International Workshop on Critical Infrastructure Protection* (*IWCIP*'05), IEEE Computer Society.
5. European Commission (2005). Green paper on a European programme for critical infrastructure protection 576 final. Brussels.
6. Zimmerman, R. (2004). *Decision-making and the vulnerability of interdependent critical infrastructure*. *Proceedings of IEEE International Conference on Systems, Man and Cybernetics*.
7. Zimmerman, R. (2007). Social implications of infrastructure network interactions. *Journal of Urban Technology*, *8*, 97–119.
8. Bagheri, E., & Ghorbani, A. A. (2008). The state of the art in critical infrastructure protection: A framework for convergence. *International Journal of Critical Infrastructures*, *4*, 215–244.
9. Brown, T., Beyeler, W., & Barton, D. (2004). Assessing infrastructure interdependencies: The challenge of risk analysis for complex adaptive system. *International Journal of Critical Infrastructures*, *1*, 108–117.
10. Haimes, Y., Horowitz, M., Lambert, J., Santos, J., Lian, C., & Crowther, K. (2005). Inoperability input-output model for interdependent infrastructure sectors. I: Theory and methodology. *Journal of Infrastructure Systems*, *11*(2), 80–82.
11. Crowther, K. G. (2008). Decentralized risk management for strategic preparedness of critical infrastructure through decomposition of the inoperability input-output model. *International Journal of Critical Infrastructure Protection*, *1*, 53–67.
12. Apostolakis, G. E., & Lemon, D. M. (2005). A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism. *Risk Analysis*, *25*(2), 361–376.
13. Patterson, S. A., & Apostolakis, G. E. (2007). Identification of critical locations across multiple infrastructures for terrorist actions. *Reliability Engineering and System Safety*, *92*, 1183–1203.
14. Ezell, B. C. (2007). Infrastructure vulnerability assessment model (I-VAM). *Risk Analysis*, *27*, 571–583.
15. Robert, B., Morabito, L., & Quenneville, O. (2007). The preventive approach to risks related to interdependent infrastructures. *International Journal of Emergency Management*, *4*(2), 166–182.
16. Myers, J. D., & Sorrentino, M. A., Jr. (2011). Regional critical infrastructure assessment: Kansas city. *International Journal of Critical Infrastructures*, *7*(1), 58–72.
17. Nan, C., Kröger, W., & Probst, P. (2012). Exploring critical infrastructure interdependency by hybrid simulation approach. In G. Berenguer & S. Guedes (Eds.), *Advances in safety, reliability and risk management*. London: Tayor & Francis Group.
18. Johansson, J., & Hassel, H. (2010). An approach for modeling interdependent infrastructures in the context of vulnerability analysis. *Reliability Engineering and System Safety*, *95*(12), 1335–1344.
19. Johansson, J., Hassel, H., & Cedergren, A. (2011). Vulnerability analysis of interdependent critical infrastructures: Case study of the Swedish railway system. *International Journal of Critical Infrastructures*, *7*(4), 289–315.

20. Zimmerman, R., & Restrepo, C. E. (2006). The next step: Quantifying infrastructure interdependencies to improve security. *International Journal of Critical Infrastructures*, *2*, 215–230.
21. McDaniels, T., Chang, S., Peterson, K., Mikawoz, J., & Reed, D. (2007). Empirical framework for characterizing infrastructure failure interdependencies. *Journal of Infrastructure Systems*, *13*, 175–184.
22. Cox, L. A., Jr. (2008). Some limitations of risk = threat × vulnerability × consequence for risk analysis of terrorist attacks. *Risk Analysis*, *28*, 1749–1761.
23. Rahman, H. A., Beznosov, K., & Marti, J. R. (2009). Identification of sources of failures and their propagation in critical infrastructures from 12 years of public failure reports. *International Journal of Critical Infrastructures*, *5*(3), 220–244.
24. Li, H., Apostolakis, G. E., Gifun, J., VanSchalkwyk, W., Leite, S., & Barber, D. (2009). Ranking the risks from multiple hazards in a small community. *Risk Analysis*, *29*, 438–456.
25. Zio, E., Piccinelli, R., & Sansavini, G. (2012). An all-hazard approach for the vulnerability analysis of critical infrastructures. In G. Berenguer & S. Guedes (Eds.), *Advances in safety, reliability and risk management*. London: Tayor & Francis Group.
26. Guikema, S. D. (2009). Natural disaster risk analysis for critical infrastructure systems: An approach based on statistical learning theory. *Reliability Engineering and System Safety*, *94*, 855–860.
27. Perrow, C. (1999). *Normal accidents: Living with high-risk technology*. Princeton: Princeton University Press.
28. Albert, R., Jeong, H., & Barabási, A.-L. (2000). Error and attack tolerance of complex networks. *Nature*, *406*(6794), 378–382.
29. Holmgren, Å. (2006). Using graph models to analyze the vulnerability of electric power networks. *Risk Analysis*, *26*(4), 955–969.
30. Hines, P., Cotilla-Sanchez, E., & Blumsack, S. (2010). Do topological models provide good information about electricity infrastructure vulnerability. *Chaos*, *20*, 1–5.
31. Overbye, T. J., Cheng, X., & Sun, Y. (2004). *Comparison of the AC and DC power flow models for LMP calculations. Proceedings of the* 37*th Hawaii International Conference on System Sciences*. Hawaii.
32. Simonsen, I., Buzna, L., Peters, K., Bornholdt, S., & Helbing, D. (2008). Transient dynamics increasing network vulnerability to cascading failures. *Physical Review Letters*, *100*, 1–4.
33. Amin, M. (2000). National infrastructures as complex interactive networks. In T. Samad & J. Wayrauch (Eds.), *Automation, control, and complexity: An integrated approach*. New York: Wiley.
34. de Bruijne, M., & van Eeten, M. (2007). Systems that should have failed: Critical infrastructure protection in an institutionally fragmented environment. *Journal of Contingencies and Crisis Management*, *15*(1), 18–29.

Chapter 2
Defining Concepts and Categorizing Interdependencies

Jørn Vatn, Per Hokstad and Ingrid Bouwer Utne

Abstract This chapter defines and discusses important concepts like risk, uncertainty, vulnerability and interdependency. In the literature, these concepts are used in various ways and there exists no common accepted terminology. Therefore, these terms are defined to provide a basis for consistent use throughout this book.

2.1 Observables and Uncertainty

Uncertainty is the fundamental concept when defining risk. Uncertainty is here used to describe the lack of certainty regarding events, conditions, magnitudes, etc. Especially, we are uncertain regarding so-called observables. Observables are quantities or events which in principle are observable at some point in time. At the analysis point in time, the observables are not known, but they will become known at a later stage; hence, they are treated as random quantities in the analysis. For example, the number of electricity users affected by a major outage is uncertain at the time of analysis, but will be known in principle after an outage has occurred. In order to express uncertainty in quantitative terms, probability statements are used. For observables directly related to the decision(s) to be made with support from the

J. Vatn (✉)
Department of Production and Quality Engineering,
Norwegian University of Science and Technology, Trondheim, Norway
e-mail: jorn.vatn@ntnu.no

P. Hokstad
SINTEF Safety Research, Trondheim, Norway

I. B. Utne
Department of Marine Technology, NTNU, Trondheim, Norway

P. Hokstad et al. (eds.), *Risk and Interdependencies in Critical Infrastructures*,
Springer Series in Reliability Engineering, DOI: 10.1007/978-1-4471-4661-2_2,

risk analysis, a main objective is to quantify the uncertainty and presents the corresponding risk picture.

2.2 Risk

A variety of definitions of risk exist in the literature ranging from "probability times consequence" to "uncertainty related to issues valued by humans". When it comes to expressing risk in a risk analysis, there are two important ways of thoughts: The traditional interpretation is that risk is a property of the system being analysed where risk comprises two dimensions; probability addressing whether undesired events will occur or not, and the consequences indicating the severity of the undesired events. A more recent interpretation (see e.g. [1]) takes uncertainty as a basis when risk is to be defined. In this interpretation, there are no inherent probabilities describing the system. The performance of the system in terms of whether events occur or not, and their severity is uncertain. This uncertainty is then expressed by probabilities reflecting the state of knowledge the risk analysis group has regarding the system being analysed. This interpretation is therefore often referred to as an epistemic risk definition and to quantify risk, three elements are introduced: $<e, p, \boldsymbol{S}>$. p is used as a probability measure of the occurrence of an event, say e. $\boldsymbol{S}$ represents the severity of the event. Note that $\boldsymbol{S}$ is a multidimensional random quantity, covering several dimensions like personnel safety, environmental impacts, material damages, loss of service, etc. Since there is more than one event to treat, i is used as an index to run through all relevant events. An operational definition of risk is now the set of all relevant triplets:

$$R = \{ < e_i, p_i, S_i > \} \tag{2.1}$$

In Eq. (2.1), p_i is used to quantify uncertainty regarding the occurrence of an event e_i for a given time period. Rather than focusing on a given time period, it is often more convenient to consider a time unit, and the probability term is then replaced by a frequency. A frequency (f_i) is then to be interpreted as the expected number of occurrences per unit time.

When risk is expressed in terms of Eq. (2.1), this is always done conditionally on a set of aspects which here is denoted as $\boldsymbol{\mathcal{D}}$, $\boldsymbol{\mathcal{U}}$ and $\boldsymbol{\mathcal{V}}$. $\boldsymbol{\mathcal{D}}$ represents the result of dialogue processes and risk communication among stakeholders that elaborate on the values and preferences domain, such as who are exposed to threats, and whose needs in the society should be focused on. Further, $\boldsymbol{\mathcal{U}}$ represents the relevant information, the theories, the understanding and the assumptions which are the basis for the risk assessor, and finally, $\boldsymbol{\mathcal{V}}$ represents the result of any verification processes, for example, third party verification. See [2] for further discussion of this operationalization of the risk concept.

In the traditional or classical definition of risk, the probabilities in Eq. (2.1) are interpreted as true properties of the system being analysed. Since we have limited data and information regarding the system, it is impossible to reveal the exact values of these probabilities. It is then common to present uncertainty intervals for the risk measure.

In the epistemic interpretation, it is the other way around. Then, the basis is that there is uncertainty regarding whether the undesired events will occur, and the corresponding severity. Probabilities are used to express this uncertainty, and there is no additional uncertainty in the probability statements. However, as part of the documentation of the risk analysis, uncertainty is qualitatively stated in terms of discussion of assumptions and simplifications. In relation to Eq. (2.1), such arguments are stated as part of $\boldsymbol{\mathcal{U}}$.

Methods and models used in risk analysis are often not affected by the interpretation of risk in Eq. (2.1). However, the way uncertainty is interpreted and presented will vary between the classical and the epistemic interpretations of risk.

2.3 Risk Register and Risk Matrices

A risk register is a formal document used to document the result of risk assessment exercises. The risk register is a table where each undesired event is listed in a separate row. The column headings may vary from analysis to analysis, but typical headings are (1) hazard/threat, (2) possible corresponding event, (3) probability of the event to occur and (4) consequence given that the event occurs. Since a risk register also serves as a follow-up tool as part of the risk management process, more headings are introduced that cover risk-reducing measures, responsibilities and due dates. The use of risk matrices in risk management is outside the scope of this book, but some challenges in documenting hazards and threats in a risk register are discussed in the following.

When documenting events in a risk register, it is common to specify probability and consequence in semi-quantitative terms, that is, by use of intervals. For example, P1 is used to represent a probability less than one per 1000 years, P2 is used to represent a probability between one per 100 years to one per 1000 years, and so on. Similar categories are used for the consequence dimension.

Each event in the risk register may then be plotted in a risk matrix illustrated in Fig. 2.1. The red-yellow-green colour regime indicates the magnitude of the risk and is a result of a calibration process. Typically, the red area represents a situation where we normally cannot proceed without implementing risk-reducing measures. The yellow area represents a situation where risk-reducing measures should be evaluated and implemented unless they are unreasonable costly or impractical. This is often referred to as the ALARP principle (as low as reasonably

Fig. 2.1 Example of risk matrix

practicable). In the green area, one usually proceeds without any risk-reducing measures unless there are some obvious efficient measures available.

Regarding the severity of an undesired event, a challenge is encountered when the probability distribution over **S** is to be mapped into one single consequence number, since one often is dealing with several dimensions like safety, costs and outage of service. One way of tackling this is to specify one consequence number for each of these dimensions and then plot the events in separate risk matrices. What becomes trickier then is to map the probability distribution over each consequence dimension. If five consequence classes ranging from low to high were used, one could present five symbols in the risk matrix for each event and for each consequence dimension. The probability of each *symbol* is then found by multiplying the probability of the undesired event with the corresponding probability of the consequence. A more simplified approach is to insert only one symbol for each event using the worst-case consequence. A reasonable worst case means a situation where the probability of the consequence class is in the order of 5–10 %. Note that the probability statement must then also reflect the worst-case situation.

2.4 Reliability

Whereas risk is a term used to pinpoint what can go wrong the term reliability points to a system or a components ability to perform the predefined required functions. Reliability is measured in terms of the probability that a system or a component is able to perform its required function at a given point of time, or over a given period of time for a given set of conditions. For example, the reliability of a backup generator is the probability that it will start upon a demand and that it will function for eight hours.

2.5 Vulnerability

While the term risk primarily is used to express uncertainty regarding adverse events, the concept of vulnerability is more directly related to the characteristics of a system. In daily speech, a child is vulnerable since its ability to resist threats and dangers is low. Therefore, the focus in a vulnerability analysis moves away from the *possibility* that adverse events occur, to system properties determining how easy it is to eliminate major system functions. For example, a vulnerability analysis of power supply intends to examine how the system is able to withstand adverse events and threats, such as line breaks, sabotage and ageing. Often, a vulnerability analysis extends the regular system limits, that is, it does not only focus on the number of affected end users, but also the impacts, such as who is affected (e.g. a hospital or a key company in the region), and measures implemented to mitigate the consequences (e.g. mobile gasworks).

It is often valuable to use a checklist with vulnerability factors to assist the consequence assessments when using a risk register. Examples of such factors are as follows:

- Area
- Chain effects
- Culture
- Degree of coupling
- Dependency with other societal critical functions
- Duration
- Geographical scope
- Level of maintenance and renewal
- Mental preparedness
- Outdoor temperature
- Population density per 1 km^2
- Quality of operational procedure and knowledge
- Substitution opportunities for infrastructure
- Time of day.

Scores may be defined reflecting a possible qualitative state of each factor. For example, the vulnerability factor "time of day" may include the states *Night*, *Evening*, *Working hours*, *Early morning* and *Rush hours*.

2.6 Resilience

In recent years, the term resilience has been introduced in relation to risk and safety. In general, resilience is the ability of a system to react and recover from unanticipated disturbances and events (see e.g. [3]) in contrast to reliability which is the ability of a system to have an acceptable low failure probability with respect

to a defined function and a given operational conditions [4]. Since reliability at least implicitly restricts focus to a *given* set of stress, the term resilience is therefore preferred in situations where any kind of stresses and disturbances are to be considered. McDaniels et al. [5] point out two key properties of resilience, namely robustness and rapidity. *Robustness* refers to a system's ability to withstand a certain amount of stress with respect to the loss of function of the system, or as Hansson and Helgesson [6] define it: "the tendency of a system to remain unchanged, or nearly unchanged, when exposed to perturbations". *Rapidity* on the other hand refers to a system's ability to recover from an undesired event with respect to the speed of recovery. Vulnerability as defined above may thus be seen as the antonym to resilience, capturing both the robustness and the rapidity aspects of a system.

2.7 Bow Tie Diagram

Figure 2.2 shows a so-called bow tie diagram often used as a conceptual model to assist the risk modelling. The starting point for the analysis is the undesired event shown in the middle of the diagram. To the left, possible causes behind the undesired event are illustrated, and the consequences that might follow are included to the right. Several barriers and safety functions are implemented to prevent the undesired event from occurring and to mitigate the consequences given that the event has occurred. Vulnerabilities are conditions related to the system being analysed which may have a negative impact on either the possibility of the undesired event to occur or consequences given that the event has occurred. For example, given a bad state of the vulnerability factor *maintenance and renewal,* an electrical grid is more prone to blackout events, that is, on the causal side. On the other hand, a bad state of the vulnerability factor *quality of operational procedure*

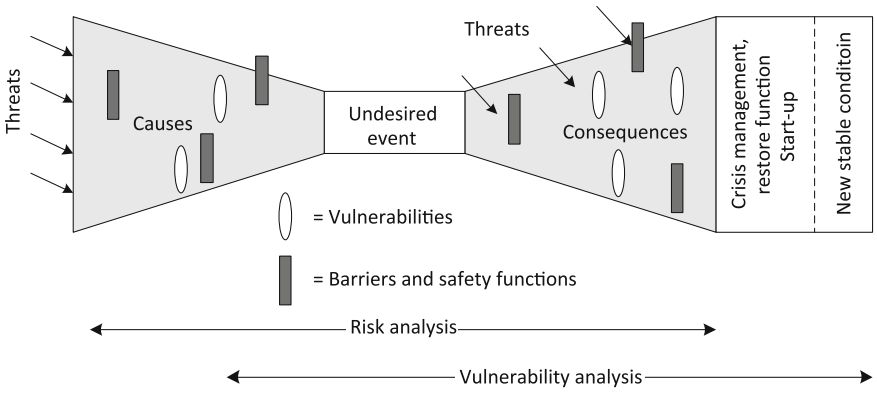

Fig. 2.2 Bow tie diagram with related terms

and knowledge will lead to longer restoration time, and hence, more severe consequences.

Figure 2.2 also indicates that a traditional risk analysis starts early in the course of events that may lead to the undesired event, and that typically stops at the immediate consequence(s) of that event. The vulnerability analysis has less focus on the causes behind disturbances in the system, but focuses more on the vulnerabilities that may cause such disturbances to result in the undesired event. The vulnerability analysis also has a more comprehensive view on the recovering process that follows after the immediate consequences of the event.

2.8 Basic Needs, Societal Critical Functions and Infrastructure

Critical infrastructure is a term used by governments to describe assets that are essential for the functioning of a society and the economy. Since the word *infrastructure* points to physical assets, other terms are often introduced focusing on what to achieve, such as *life lines* and *societal critical functions*. Societal critical functions can be defined as functions that are essential to ensure the basic needs of a society. DSB [7] has made a systematization of needs, functions, infrastructures, and inputs, described below.

2.8.1 Basic Needs

The basic needs point to what is considered essential in a society, and in this context, this means as follows:

- Food
- Water
- Heating and cooling
- Safety and security.

2.8.2 Societal Critical Functions

A variety of societal critical functions are required to ensure that the basic needs of a society are fulfilled. It is not always obvious which societal functions are to be considered as critical. DSB [7] proposes to limit critical functions to those functions where (1) a loss of the function in seven days or more will threaten basic

needs and (2) such a loss occurs under disadvantageous conditions and/or in combination with coincidence of other events. Based on such an argument, the societal critical functions are as follows:

- Water supply
- Food supply
- Heat supply
- Financial security
- National security
- Life and health
- Crisis management
- Law and order.

2.8.3 Infrastructure

The societal critical functions depend on infrastructure components. To some extent, infrastructure components may be replaced by other substitutes; hence, their criticality depends on the organization of infrastructure components in the society. The following basic infrastructure components are often considered:

- Telecommunication network
- ICT-network
- Network of roads
- Railway network
- Water and sewage network
- Fuel supply and logistics
- Power grid
- Harbours.

2.8.4 Input Factors

Finally, several input factors are required to provide the infrastructure elements and/or the societal critical functions. These are as follows:

- Labour
- Other services
- Transportations
- ICT-services
- Telecommunication
- Goods and products
- Energy.

2.9 Dependency and Interdependency

In classical risk analysis, the concept of *stochastic dependency* is crucial since various types of dependencies may compromise the effect of the "defence in depth" principle emphasizing the importance of multiple barriers to control hazards. Two events A and B are said to be stochastic independent if information regarding the occurrence of one of the event will not alter the probability of the other one. Mathematically, this is expressed by:

$$\Pr(A|B) = \Pr(A) \tag{2.2}$$

Stochastic dependency then means that information regarding the occurrence of one of the events will change the probability of the other. Our main concern is *positive dependency* where the occurrence of an event typically represents a barrier failure, and positive dependency then means that the probability of failure of one of the barrier increases if it is known that the other barrier has failed. Although stochastic dependency is accounted for in risk analysis, it does not indicate the type of dependency or causes behind.

In risk modelling of critical infrastructures, there are several types of dependencies to take into account: Various regimes exist in order to classify types of dependencies, and it is common to use the term *interdependency* between infrastructures, rather than the term dependency. Rinaldi et al. [8] propose a categorization regime with 6 dimensions to understand various aspects of interdependency. Three types of interdependencies and failures are applied in this book, motivated by Rinaldi et al. [8]:

a. *Cascading failures*, where a failure in one infrastructure causes disturbances in another infrastructure. In this situation, there is a functional relationship between two or more infrastructures. For example, water supply is dependent on electricity for water treatment.
b. *Escalating failures* where failure in one infrastructure worsens an independent disturbance in another infrastructure. For example, a breakdown in the metro is significantly worse if a main road is unavailable due to a fire in a tunnel.
c. *Common cause failures* where two or more infrastructures are disrupted at the same time due to a common cause. For example, a fire in a culvert may cause interruption of electricity, water and telecommunication at the same time. Often, the term geographical dependency is used to explain such failures because one or several elements of the infrastructures are in *close proximity* so that external threats may knock out several infrastructures at the same time.

When categorizing dependency and interdependency, the term *functional interdependency* is used in situations where there are cascading failures, the term *impact interdependency* is used in situations where there are escalating failures and the term *geographical dependency* is used in situations where there are common cause failures.

The term escalating failures is used to describe that the impact of a failure in one system is worsened by a failure of another system reflecting the overall system demand, for example, transportation needs. Such escalating effects may be evident even if the performances of the two systems are *independent*. The structure of the overall system demand will often cause higher load on one system in case of a failure of another system which may increase the probability of failure or reduced performance. The two systems are therefore stochastically dependent, but it cannot be categorized as a common cause failure since there is no common cause that causes the failure of the two systems, and the term escalating failures is also used to express such load dependency between systems.

References

1. Aven, T. (2003). *Foundations of risk analysis. A knowledge and decision-oriented perspective*. New York: Wiley.
2. Vatn, J. (2012). Can we understand complex systems in terms of risk analysis? *Journal of Risk and Reliability, 226*(3), 346–358.
3. Hollnagel, E., Woods, D. D., & Leveson, N. (Eds.). (2006). *Resilience engineering: Concepts and precepts*. Aldershot: Ashgate Publishing Limited.
4. Zio, E. (2009). Reliability engineering: Old problems and new challenges. *Reliability Engineering and System Safety, 94*, 125–141.
5. McDaniels, T., Chang, S., Cole, D., Mikawoz, J., & Longstaff, H. (2008). Fostering resilience to extreme events within infrastructure systems: Characterizing decision contexts for mitigation and adaptation. *Global Environmental Change, 18*(2), 310–318.
6. Hansson, S. O., & Helgesson, G. (2003). What is stability? *Synthese, 136*, 219–235.
7. DSB (2011). Nasjonal sårbarhets og beredskapsrapport (NSBR) (2011). ISBN: 978-82-7768-246-4. http://dsb.no/Global/Publikasjoner/2011/Rapport/NSBR2011.pdf Last visited 2011-10-18.
8. Rinaldi, SM., Peerenboom, JP., Kelly, TK. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine, 21*(6), 11–25.

Chapter 3
Risk and Vulnerability Analysis of Critical Infrastructures

Per Hokstad, Ingrid Bouwer Utne and Jørn Vatn

Abstract This chapter presents an approach for a cross-sector risk and vulnerability analysis (RVA) of critical infrastructures. The RVA is an extended version of a preliminary hazard analysis (PHA) and can be applied to any complex system with only minor adaptations. The analysis has three phases described below: (1) analysis preparation, (2) preliminary risk analysis and (3) detailed risk analyses. The objective of the RVA is to identify hazardous events related to the activity/system as thorough as reasonably practicable. In phase 2, risk is assessed by the analysis group from direct assessments of probabilities and consequences on a semi-quantitative scale, such as low (L), medium (M) and high (H). This is in line with a standard PHA, which aims to identify and assess all major risks, and provide risk-reducing measures, without including detailed risk calculations or analyses. The preliminary risk analysis is then used for screening, and the most critical events are investigated further for various detailed analyses and quantifications. The RVA described here intends to give a complete overview of all risks elements related to the systems under investigation.

P. Hokstad (✉)
SINTEF Safety Research, Trondheim, Norway
e-mail: per.hokstad@sintef.no

I. B. Utne
Department of Marine Technology, NTNU, Trondheim, Norway

J. Vatn
Department of Production and Quality Engineering,
Norwegian University of Science and Technology, Trondheim, Norway

P. Hokstad et al. (eds.), *Risk and Interdependencies in Critical Infrastructures*,
Springer Series in Reliability Engineering, DOI: 10.1007/978-1-4471-4661-2_3,

3.1 Phases of Analysis

The first phase is to clarify analysis objectives. The main purpose of a cross-sector risk and vulnerability analysis (RVA) is to provide authorities with decision support regarding identification of risks and vulnerabilities, prioritization of risk-reducing measures and planning of emergency preparedness related to a number of infrastructures for which they are responsible.

Phase 2 of the RVA is to provide a preliminary risk analysis similar to a preliminary hazard analysis (PHA), which includes identification and risk assessment of undesired events (UEs). The bow-tie diagram introduced in Chap. 2 constitutes a useful conceptual framework for the analysis, where the undesired (hazardous) events are in focus, investigating both causes and various (undesired) consequences. However, the RVA includes an evaluation of a wider set of consequences, for example, also looking into consequences of other infrastructures. Finally, the third phase allows for more detailed analyses.

The main phases of the RVA are outlined below and are further elaborated in the next sections:

1. *Risk analysis preparation*
   - Clarify objectives and stakeholders
   - Determine system boundaries and consequence categories
   - Establish forum/meeting place for relevant stakeholders.
2. *Preliminary risk analysis*
   - Identify undesired/hazardous events and societal critical functions (SCFs) affected
   - Analyse causes and vulnerabilities
   - Assess risk and suggest risk-reducing measures.
3. *Detailed risk analyses*
   - Select UE for detailed analyses, based on the results of phase 2
   - Describe the accident scenario and system subject to detailed analyses
   - Carry out detailed analyses, *for example*,
     - Causal analysis
     - Consequence analysis
     - Interdependency analysis.

3.2 Phase 1: Analysis Preparation

Phase 1 follows the start-up of a traditional risk analysis and is therefore only briefly described here. For a thorough introduction to risk analysis, [1] is recommended for further reading.

3.2.1 Clarify Objectives and Stakeholders

First, the objectives of the RVA have to be clearly stated; if not—the analysis may give irrelevant results. The objectives will usually depend on who the stakeholders are, *that is*, who will use the results and who will be affected by the loss of infrastructure. Thus, identifying stakeholders is part of the initial planning process, since stakeholders may have different objectives and motivations for carrying out a risk analysis:

- Authorities, such as municipalities and counties, may be concerned about getting a total overview of vulnerabilities and threats within their fields of responsibility. Then, they need to assess several sectors as a whole to enable planning of emergency preparedness.
- Infrastructure owners, *for example*, of the water supply system, electricity production plant, may be more interested in the analyses of production.
- Users of the infrastructures, *for example*, large hospitals or transportation companies, may be preoccupied with analyses of own vulnerabilities and dependencies to critical infrastructures, to assess their need for backup solutions.

3.2.2 Determine System Boundaries; Specify Types of Causes and Consequences

The scope of the analysis and the level of detailing are other important issues. Relevant questions are as follows:

- Is the assessment of the infrastructures to be carried out at an overall system level, or are subsystems or single components also of interest?
- To what extent should the analysis include human and organizational contributions to hazardous events?
- Which types of causes are considered? For instance, are natural disasters and malicious acts included?
- Which types of consequences should be considered: those related to the system functions, to the infrastructure owners, specific users, or to societal functions?
- As a result of this, it is specified which consequence dimensions should be assessed: for example, regularity/availability of infrastructure, loss of lives, personal injuries, economic losses, etc.?
- Specify the frequency and consequence categories to use (e.g. 1–5); see Sect. 3.3.4.

3.2.3 Establish Forum for Stakeholders

Most often many stakeholders are involved in risk analyses of critical infrastructures. As seen above, they can have varying motives for the analysis, and it is important to establish a forum to facilitate discussions of stakeholder

perspectives, risk perceptions, fields of responsibilities, communication and exchange of knowledge. The forum must also include experts on the various infrastructures.

Also note that risk assessments of societal risks may require use of classified information, either company specific or national. Security grading limits the possibility for releasing information to the public, and there could also be a need for security clearance of the participants in the analysis.

3.3 Phase 2: Preliminary Risk Analysis

The objective of phase 2 is to identify UE and analyse the risks in a rather coarse way to be able to select the most critical events for further detailed analysis. The following is based on [2, 3].

Figure 3.1 shows a conceptual bow-tie model used for entering information related to each event in the risk register (RR) of the RVA, *cf.* Chap. 2. Every information unit to be specified is discussed in the following subsections. Rectangles with a dark grey background represent the information specified by the user, or the analysis group.

3.3.1 Identification of Undesired/Hazardous Events and Societal Critical Functions

For the identification of the undesired/hazardous events, it is useful to develop a generic hierarchy of these. The following categories are used at the top level [3]:

1. Natural events,
2. Medical/Biological events,
3. Technological events,
4. Human behaviour (Malicious/dysfunctional).

Such a hierarchy makes the analyses more structured and traceable. For example, in relation to Fig. 3.1, the first level is *Natural event*, the second level is *Meteorological* and the third level is *Flooding*. A complete list UE of up to level 3 is provided in Appendix A.

The UE can be either *generic* or site specific. A generic event can refer to an event at an unspecified railway station, whereas a site-specific event may concern a specified transformer station in a specific area.

The UE are not directly pointing towards the SCF. A part of the analysis is to connect relevant SCF to the UE. For each SCF, both the actual function and the physical implementation ("system") are identified, for example, both "passenger transportation" and "railway lines" when we consider train transport. Similar to

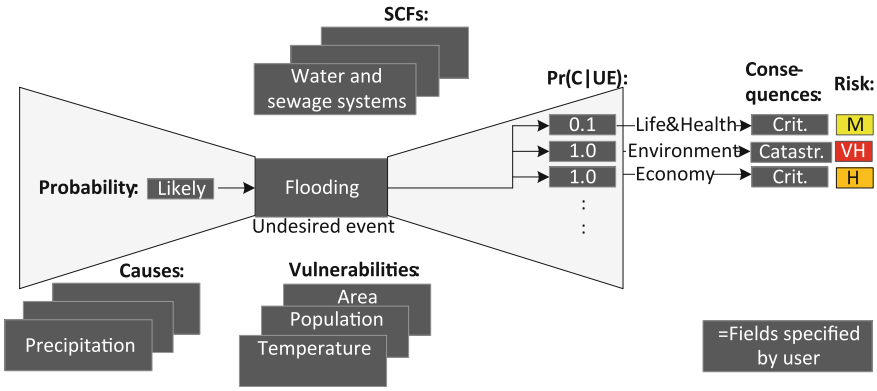

Fig. 3.1 Conceptual specification model for the undesired hazardous event, example. (*SCF* societal critical function; *C* event of certain critical consequence; *UE* undesired event; *M* medium; *H* high; *VH* very high)

the UE, the SCF are structured in a hierarchy. The complete list is shown in Appendix B. To get an impression of SCF included, the level one SCF are shown below. They may be used as a "checklist":

- Electricity supply
- Electronic communication (ICT)
- Water and sewage systems
- Oil and gas supply
- Transport (road, railway,…)
- Banking and finance
- Food supply
- Sanitation
- Health, social and social security services
- Police, emergency and rescue services
- Public management
- Media and news communication
- Important industries
- National symbols.

Figure 3.1 shows an example of a level 2 element in the SCF list, *that is*, *water and sewage systems*. In order to structure the analysis, it is recommended to describe the relation between each SCF and the corresponding UE. Referring to the bow-tie diagram in Fig. 3.1, three principal situations exist regarding a SCF:

1. The SCF itself *affects* the causal chain of events (before the UE occurs), *for example*, it can be a cause of the event. This SCF is labelled "*before* the UE". An example could be a significant breakage in a water pipeline in the water and sewage system that causes flooding in a traffic junction.

2. The SCF is *part* of the systems put in place to mitigate the effect of the UE. This is denoted "*after* the UE". For example, the water and sewage system is part of the entire firefighting system in relation to an event with *fire*.
3. There is a possibility that the occurrence of the UE will *result* in a deficiency of the SCF. Then, the SCF is "*threatened* by the UE". For example, a flooding due to heavy rainfall may cause excavation leading to damage to the water and sewage system.

3.3.2 Causal Analysis

In order to gain a better understanding of why the hazardous events occur, the RVA may elaborate on the causes leading up to the event. Figure 3.1 illustrates that there are one or more failure causes that precede the undesired (hazardous) event. Rather than performing a causal analysis by means of, *for example* fault tree analysis (FTA), the failure causes are only listed at this stage in the analysis. For example, one may list heavy rain and lack of buffer capacity in the waterways as causes behind a flooding. In a later detailed analysis, these causes may be included in hydrological and hydraulic models. A good understanding of failure causes will be a basis for assessment of the probability that the hazardous event occurs later in the analysis.

3.3.3 Vulnerability Analysis

Several vulnerability factors will affect the probability of the event, and/or the consequences if the event occurs. Figure 3.1 indicates that temperature, population and area are vulnerability factors that should be taken into account when assessing probability as well as consequence. The vulnerability factors are only listed at this stage of the analysis without any explicit modelling with respect to probability and consequence. Obviously, the knowledge of a highly populated area will increase the consequence compared to a less dense population, but such information is only documented as arguments for the assessments. To help structuring, it is valuable to categorize vulnerability factors either to be relevant *before* the hazardous event, *that is*, left-hand side in Fig. 3.1, or *after* the hazardous event. In some situations, the factors may influence both "sides" of the undesired event in the bow-tie diagram.

3.3.4 Risk Assessment

It is necessary to establish categories both for probabilities and for the chosen consequence dimensions; for example, using categories 1–5, 1 being the "best" and 5 the "worst". Whether to use a 3-, 4-, or 5-point scale has to be clarified as

Table 3.1 Example of consequence categories for three dimensions (life, economy, unavailability)

Category	Life and health/injury	Economy (mill. €)	Unavailability[a]
1	Up to 5 injured/seriously ill	<0,1	Delimited
2	6–40 injured/seriously ill	0,1–1	Some damages
3	1–2 fatalities, 40–100 injured/seriously ill	1–10	Serious
4	3–10 fatalities, 100–500 injured/seriously ill	10–100	Critical
5	More than 10 fatalities, more than 500 injured/seriously ill	>100	Catastrophic

[a] Unavailability is constituted by extent and duration, see Fig. 3.2

	0 - 6 hours	6 - 24 hours	1 - 7 days	1 - 4 weeks	1 - 6 months	More than 6 months
1 – 10 persons	Delimited	Delimited	Some damages	Some damages	Serious	Serious
10 - 100 persons	Delimited	Some Damages	Some damages	Serious	Serious	Critical
100 - 1 000 persons	Some damages	Some Damages	Serious	Serious	Critical	Critical
1 000 – 10 000 persons	Some damages	Serious	Serious	Critical	Critical	Catastrophic
10 000 - 100 000 persons	Serious	Serious	Critical	Critical	Catastrophic	Catastrophic
> 100 000 persons	Serious	Critical	Critical	Catastrophic	Catastrophic	Catastrophic

Fig. 3.2 Matrix defining categories of infrastructure *unavailability,* (using five consequence categories), based on *duration* (*horizontal axis*) and *extent* (*vertical axis*)

part of the analysis preparations. An example of 5 consequence categories is shown in Table 3.1 for three consequence dimensions: life and Health/Injury, economy and unavailability (of infrastructure service).

Note that the consequence dimension *unavailability* may be further differentiated by means of *duration* and *extent (number of exposed persons),* as illustrated in Fig. 3.2.

A discussion between stakeholders is needed to calibrate the categories of various dimensions and thus provide resulting risk matrices. In particular, when the risks of several infrastructures are assessed, it must be assured that categories are consistent. Such calibration is part of the analysis preparation.

The assessed frequency or probability of the UE is required for plotting the events in a risk matrix, see Chap. 2. When assessing the consequences resulting

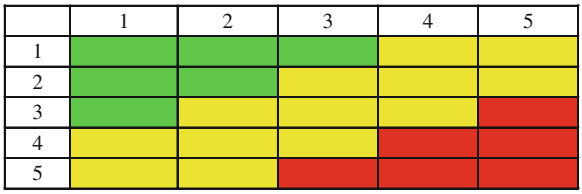

Fig. 3.3 Risk matrix with five frequency/probability categories (*vertical axis*) and five consequence/severity categories (*horizontal axis*). Three risk areas (*green, yellow, red*) according to the ALARP principle

from a hazardous event, it is necessary to reflect on the stochastic nature of the course of events in the right-hand part of the bow-tie diagram in Fig. 3.1. As discussed in Chap. 2, it is common to consider some worst-case scenarios. By worst-case, one often does not consider the absolute extreme, but situations that are reasonable under bad conditions. A conditional probability Pr(*C*|*UE*) is introduced in Fig. 3.1 to denote the conditional probability that a certain (worst-case) consequence will be the result, given that the undesired hazardous event occurs. This conditional probability is taken into account when the frequency (probability) of the UE is assessed, by reducing the frequency.

As discussed in Sects. 3.3.2 and 3.3.3, causes leading up to the hazardous event and the identified vulnerability factors are used as a basis when assessing both frequencies and consequences, although no formal method is provided for this purpose.

When the frequency and consequence categories of the UE are estimated, the identification number of the UE is plotted in the risk matrix, see Fig. 3.3, presenting an example with five frequency and five consequence categories (*cf.* Fig. 2.1). This is used as a basis for the risk evaluation (see below).

3.3.5 Additional Specifications of Undesired/Hazardous Events

Some of the above specifications are somewhat specific to the RVA for critical infrastructures meaning that they represent an extension of a standard PHA. The RVA also provides additional information to support the risk assessment related to the undesired hazardous events, since the following questions are considered:

- Does the event have a major accident potential?
- Are there relevant interdependencies (in the SCFs), if the event is site specific?
- Are there communication challenges to the public related to crisis management?

This information is for instance relevant when selecting events for further detailed risk analyses (phase 3).

3.3.6 *Risk Evaluation and Risk-Reducing Measures (Risk Control)*

The hazardous events are assigned a risk priority number (RPN), *cf.* Chap. 2. This is based on the probability (frequency) and consequence categories. The RPN can be obtained by just adding the probability and consequence categories, which means that a probability category 2 and a consequence category 3 for a specific event add up to a RPN of 5. The RPNs should be placed into the risk matrices for each consequence dimension.

The risk matrix is typically divided into coloured areas. Broadly speaking, this corresponds to the as low as reasonably practicable (ALARP) principle. With a green, yellow and red colouring regime, events in the "red area" will require risk-reducing measures and/or additional, more detailed analyses to be carried out. Also for events in the "yellow area", risk-reducing measures will typically be considered based on their efficiency. This partition of the risk matrix in red, yellow and green areas is subject to discussions among the stakeholders.

The present book does not go into detail on advanced decision models and management tools (*cf.* Chap. 1.)

It is essential to assign responsibilities to specific persons for implementing the risk-reducing measures (and further required actions), *cf.* forum for stakeholders (Sect. 3.2).

3.4 Phase 3: Detailed Risk Analyses

Based on the results from phase 2 of the RVA, some undesired hazardous events are selected for further detailed risk analysis. This selection may be based on different criteria, but often events with high risks or serious consequences are selected, giving input, *for example* to cross-sector emergency preparedness planning. It is also possible to select events with strong interdependencies, events related to malicious acts or special types of consequence dimensions. Before selecting events, it is important to clarify the purpose of the detailed analyses.

The detailed analyses may consist of:

1. *Causal analyses*: The purpose of casual analysis is to identify and assess all possible causes to the accident scenario. Often FTA is used, because then it is possible to assess the different combinations of events leading to the TOP event, as well as failures in barriers, see below.
2. *Interdependency analyses*: The purpose of interdependency analysis is to investigate interdependencies (within and across infrastructures) and to assess how failures propagate if a critical hazardous event occurs. Various types of analyses are described in subsequent chapters, for example see Chaps. 4 and 5.

3. *Consequence analyses*: The purpose of the consequence analysis is to gain more knowledge about what may happen after the event has occurred. Often an event tree analysis (ETA) is applied, see below.
4. *Network analyses:* see below.

Below some of the commonly used methods are briefly described, in order to demonstrate the diversity of these methods. More on the standard analyses, FTA and ETA, can be found, for example in Rausand [1], also see Appendix C.

3.4.1 Fault Tree Analysis

An FTA is typically conducted to structure the knowledge regarding causes of a hazardous event. The hazardous event corresponds to the so-called TOP event in the fault tree diagram. An FTA analysis uses logical gates to investigate combination of causes. The AND gate is used in situations where two or more causes (or more precisely events) are required for an event higher up in the diagram, whereas an OR gate is used when only a single cause is necessary for an event to occur on a higher level. The aim of the analysis is to find combination of causes that lead to the TOP event, and the probability that the TOP event occurs. FTA is primarily a method for analysing binary static systems. For dynamic and/or multistate systems, use of FTA will often give limited value.

3.4.2 Dose–Response Models

For many infrastructure systems, so-called dose–response models are used both on the left- and right-hand side in the bow-tie diagram in Fig. 3.1. For example, in a flooding scenario, the dose may be the amount of precipitation and the response the capacity in the drainage system. Both precipitation and capacity are treated as stochastic variables, and by combining the stochastic behaviour of these variables with physical hydrological and hydraulic models, it is possible to derive the probability of various critical situations.

3.4.3 Event Tree Analysis

ETA is typically used to describe the right-hand side of the bow-tie diagram in Fig. 3.1. The analysis starts with the hazardous event and aims at structuring the course of events that follows. A set of branching points are developed from left to right until typical end consequences are reached. A branching point may either be a barrier or safety function intended to mitigate the course of events, or it may be

the outcome of a critical situation/condition like *night* or *day*. The objective of the analysis is to structure knowledge regarding the course of events in order to identify possible mitigating measures and to calculate the conditional probabilities of each end consequence.

3.4.4 Network Analyses

Several network models exist. For instance, a flow line network analysis (FNA) aims at describing the flow in a distribution network, such as an electricity grid, a water distribution network or a network of roads. The network comprises nodes and arcs. Nodes are branching or meeting points, and the arcs represent flow between the nodes. The flow depends both on the physical capacity of the infrastructure and on the dimension of a water pipe. But the flow also depends on parameters, such as water pressure, roughness, slope, etc. Next, the physical capacity may be compromised due to failures and defects in the system. Probabilistic models exist for calculating the stochastic performance at critical nodes in the network. Other network models exist, for example see Chap. 5.

References

1. Rausand, M. (2011). *Risk assessment: Theory, methods, and applications* (2nd ed.). Hoboken, NJ: Wiley.
2. Utne, I. B., Hokstad, P., Kjølle, G., Vatn, J., Tøndel, I. A., Bertelsen, D., Fridheim, H., & Røstum, J. (2008). Risk and vulnerability analysis of critical infrastructures—The DECRIS approach. www.sintef.no/project/SAMRISK/DECRIS/Documents/DECRIS_paper_SAMRISK_final%20080808.pdf. Last visited 02 May 2012.
3. Henriksen, S., Sørli, K., & Bogen, L. (2007). Method for identification and ranking of critical societal functions (in Norwegian). Norwegian Defence Research Establishment. ISBN 978-82-464-1192-7. http://rapporter.ffi.no/rapporter/2007/00874.pdf. Last visited 02 May 2012.

Chapter 4
Interdependency Modelling in Risk Analysis

Per Hokstad, Ingrid Bouwer Utne and Jørn Vatn

Abstract Failures of critical infrastructures can represent a threat both to people, economy and societal functions and to national security. So, thorough risk analyses of infrastructures are required to reduce the probability and mitigate the consequences of failures. The interdependencies between infrastructures can be strong, but are seldom accounted for in current analyses. This chapter presents a method for assessing these interdependencies and also provides an example. The analysis is part of an overall cross-sector risk and vulnerability analysis (RVA), see Chap. 3.

4.1 Steps of the Interdependency Analysis

The total risk and vulnerability analysis (RVA) consists of three *main* phases (*cf.* Chap. 3). Phase 1 consists of analysis preparations. In phase 2, hazardous events are identified and analysed in a coarse way, as in a preliminary hazard analysis (PHA). Also, a screening is carried out to identify the hazardous events for which more detailed analyses are required. The detailed analyses (phase 3) may include an analysis of interdependencies, which is described in this chapter. A detailed interdependency analysis includes the following steps:

P. Hokstad (✉)
SINTEF Safety Research, Trondheim, Norway
e-mail: per.hokstad@sintef.no

I. B. Utne
Department of Marine Technology, NTNU, Trondheim, Norway

J. Vatn
Department of Production and Quality Engineering,
Norwegian University of Science and Technology, Trondheim, Norway

P. Hokstad et al. (eds.), *Risk and Interdependencies in Critical Infrastructures*,
Springer Series in Reliability Engineering, DOI: 10.1007/978-1-4471-4661-2_4,

(1) Describe the undesired hazardous event, specify a corresponding scenario and identify relevant societal critical functions (SCFs), *cf.* Chap. 3.
(2) Identify interdependencies.
(3) Perform a semi-quantitative risk assessment of the scenario.
(4) If needed, perform additional detailed quantitative analyses (optional).
(5) Evaluate risk and suggest measures to reduce interdependencies and risk.
(6) Analyse costs and benefits (optional).

The above approach is based on having thorough system knowledge, but detailed skills in probability or statistics are not required (perhaps with an exception for steps (4) and (6)). These six steps are described below, and the approach will be illustrated by a case involving railway, electricity supply and ICT.

4.2 Step (1): Description of the Undesired Hazardous Event

In step (1), the selected hazardous/undesired events are described more in detail than done in phase 2 (*cf.* RVA in Chap. 3). This means that physical location, environmental conditions and constraints, time and operational factors should be described. In addition, technical and organizational systems with physical objects that are directly affected need to be included. When these details of the hazardous event are specified, it is referred to as an (accident) *scenario*.

Next, the SCFs that are relevant for the scenario must be identified and described. One can start from the generic list of SCFs given in Appendix B. Note that some relevant SCFs may not be identified until the qualitative analysis is carried out (*cf.* step (2), above).

4.3 Step (2): Identification of Interdependencies and Qualitative Analysis

In step (2), the interdependencies between the affected SCFs are analysed qualitatively.

4.3.1 Identification of Interdependencies

Interdependencies can be categorized in different ways. Here, three categories are used (*cf.* Chap. 2):

1. Geographical (giving common cause failures)
2. Functional (resulting in cascading failures)
3. Impact (causing escalating failures).

Geographical interdependencies are caused by systems being geographically close/adjacent (physical proximity) and can result in common cause failures, *functional* interdependencies are related to *cascading failures* (the functioning of one system depends on the functioning of another), and *impact* interdependencies are used in situations with *escalating failures*.

The infrastructures and corresponding SCFs which *in the given scenario* are exposed to *geographical interdependencies* are revealed by asking:

- Is the SCF immediately threatened by the undesired event due to the proximity of its systems/equipment?
- Are there other systems/functions that can be threatened, for example, by spreading of a fire/smoke (or flooding) caused by the event?

The *functional interdependencies* between the "geographical SCFs" identified above and other SCFs are identified stepwise by asking:

- Which SCFs are directly depending on the above geographical SCFs? These represent the *first-order functional interdependencies*.
- Which SCFs are affected by the loss of the SCFs identified as first-order functional interdependencies? These represent the *second-order functional interdependencies*.

The *impact* type of interdependencies can be identified by assessing whether the loss of more than one SCF can cause a more serious situation than by just adding the losses of the two SCFs (considering separate failures).

For all interdependencies, one should identify the relevant barriers to protect a SCF or at least those reducing the impact of the event. The barriers can be both physical (i.e. a separation between SCFs or between SCFs and threats) and organizational (e.g. access control).

4.3.2 Construction of the Cascade Diagram

The outcome of the geographical and functional interdependency identification can be visualized in a *cascade diagram*, as shown in Fig. 4.1 [1]. A cascade diagram gives an overview of the interdependencies in a structured manner. The cascade diagram resembles an event tree, but there are some differences: in an event tree, only one of the paths from the hazardous event to the end consequence can occur, so the branches are mutually exclusive. In the cascade diagram, the branches are not mutually exclusive and an undesired hazardous event can give rise to a number of affected SCF. The risk quantification differs for these two types of modelling as well.

Impact interdependencies can be taken into account in the calculations of risk, but do not have any direct influence on the cascade diagram.

The construction of a cascade diagram (Fig. 4.1) starts with the hazardous event to the left, and the SCFs that are directly affected due to their geographical location are placed to the right of the event (see "nodes" SCF1–SCF3). Then, the SCFs

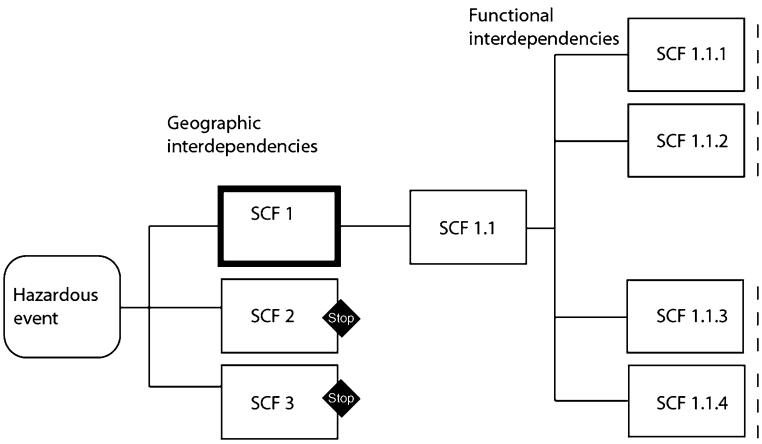

Fig. 4.1 Example of a cascade diagram, adapted from [1]

having functional interdependencies are introduced to the right in the figure. It is seen that four SCFs are depending on SCF 1.1. The interdependencies are visualized by lines and the SCFs by boxes; dependency going "from left to right". A SCF which for any reason is not investigated any further is marked with a stop symbol (e.g. SCF2 and SCF3). The boxes where no subsequent SCFs (to the right) have been identified are marked with a dashed line, and these are called *leaf nodes*. The cascade diagram supports both qualitative and quantitative analyses of consequences and risk.

When the interdependencies are identified to a feasible level of detail, the cascade diagram is analysed *qualitatively*:

- Can an interdependency cause total or partial malfunction of an affected SCF?
- What are the likely direct consequences due to the loss of a SCF?
- Do barriers exist which can prevent the occurrence of common cause failures or cascading failures?
- Does any loss have a potential for causing a major accident?
- How could interdependencies be reduced in terms of risk-reducing measures (and what is the benefit)?

In some cases, it can be relevant to investigate only those interdependencies with the most serious probabilities and consequences and thus simplify the diagram.

4.3.3 An Example: The Culvert Case

As an example, the following scenario is specified [1–3]:

> Loss or damage to electricity supply and/or ICT systems close to a culvert at Oslo Central Station (railway station), also resulting in failures to other SCFs.

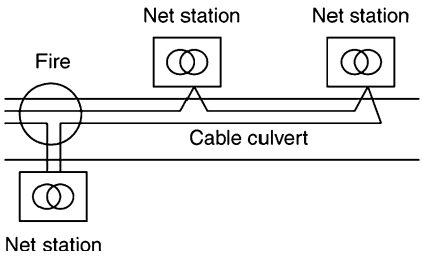

Fig. 4.2 Schematic illustration of the electric cables in the culvert, adapted from [3]

The basis for this scenario is an actual event that occurred close to Oslo S (railway station) in November 2007, when an entrepreneur unwarily broke a cable when digging a ditch. The cable breakage led to a short circuit and fire affecting Oslo S, actually paralysing the region's rail traffic and transportation systems for 20 h, and also shutting down the local Internet systems for about 10 h, [3]. Note that this culvert example here is not used for accident investigation ("what did actually happened that day?"), but as the starting point for analysing interdependencies and consequences in the possible chains of events of this scenario.

Figure 4.2 shows the layout of the electric cables in the culvert at Oslo S. There were two high-voltage cables which served three net stations. The redundant cables were placed in the same culvert. In the actual fire, both cables were destroyed. The physical objects, systems and infrastructures immediately affected were the electricity supply cables and ICT cables (telephone, Internet, railway communication). The culvert is in close proximity to the railway station, Oslo S, major road trafficking intersections and highways, a subway station and a bus station. Further, the traffic control centre (TCC) for a large part of the Norwegian railway traffic is located in the buildings of Oslo S, and this TCC receives electricity supply from one of the three net stations that was affected.

In general, it is important to consider contents of culvert and possible traffic junctions, traffic control centres and transportation means in the proximity of the culvert. Three geographical SCFs/objects are immediately identified (*cf.* SCF1–SCF3 of Fig. 4.1):

- Electricity supply cables in the culvert
- ICT cables in the culvert
- The departure/arrival (D/A) hall at the railway station, that is, SCF could be defined as railway traffic at Oslo S (during the actual event at Oslo S, smoke from the culvert fire spread to the departure/arrival hall, causing the station to shut down).

Next, consequences of failure in the electricity supply cables are assessed. Examples of relevant first-order functional interdependencies (systems depending on relevant electricity supply) are as follows:

- ICT providers
- Railway traffic centre
- Shops.

Examples of SCF depending on ICT providers are (second-order functional interdependencies):

- Internet
- Emergency/police
- Train communication
- Electronic payment transfer (EPT).

Finally, observe some relevant *barriers* in this example case:

- Physical protection of cables
- Access control (with respect to sabotage)
- Redundancy of electricity supply, for example, more than one electricity cable
- Physical separation of the affected SCFs.

4.4 Step (3): Semi-Quantitative Risk Assessment

After a qualitative evaluation, risk quantification based on the cascade diagram can be performed. The approach is exemplified by the culvert case described above.

4.4.1 Quantification of Probability and Consequence

Risk is here to be quantified as the product of probability (frequency) and consequence. A semi-quantitative approach is now applied by introducing categories 1–5 (*cf.* Chap. 3). Only the consequence dimension *loss of service* is considered in this example. In total, the following parameters are assessed in order to estimate the risk related to a scenario:

- Frequency (F) of the accident scenario
- Conditional probability (P) that a specific SCF will be affected, given that a "previous event" has occurred (another SCF has failed)
- Extent (E), that is, the number of people affected by the loss of a SCF
- Duration (D), that is, the time period that a SCF is unavailable.

Here F, P, E and D are categorical variables, taking values 1, 2, 3, 4 or 5. The extent, E, and duration, D, for an event are used as measures of the direct consequence of the loss of a SCF. These assessed values of E and D are next used as a basis for assessing the conditional probability P that another ("subsequent") SCF is affected. For example, a long duration of electricity outage will cause a redundant unit (such as an uninterrupted power supply (UPS)) to run out of power.

Table 4.1 gives an example of how five categories can be defined for each of the parameters, F, P, E and D (in terms of the "actual" parameters f, p, e and d). This is the specification used in the example, but the categories have to be adapted to the actual analysis.

Table 4.1 Categories 1–5 for parameters *F*, *P*, *E* and *D* used in the example case

Category	Frequency (*f*)	Probability (*p*)	Extent (*e*)	Duration (*d*)
1	Less than once every 1,000 years	10^{-4}–10^{-3}	≈10	<1 h
2	Once every 100–1,000 years	10^{-3}–10^{-2}	≈100	1–6 h
3	Once every 10–100 years	10^{-2}–10^{-1}	≈1,000	6–48 h
4	Once every 1–10 years	10^{-1}–1	≈10,000	48 h–1 week
5	Once or more every year	1	≈100,000	>1 week

Category 1 represents the "least serious" outcomes: those with a frequency *f* less than once every 1,000 years, a probability *p* of 10^{-4}–10^{-3}, the extent *e* being in the order of 10 persons and finally, the duration *d* of the event being less than 1 h. Similarly, category 5 represents the most serious outcomes. Observe that the categories are defined in terms of *intervals* for the parameters *f, p* and *d*, while the order of magnitude is given for the extent *e*. Both types of categories can be feasible depending on the type of analysis, but it is important to adapt the formulas used for calculating the risk (below).

The first step of the semi-quantitative analysis is to estimate the risk triplet <*F, E, D*> of the hazardous event and then <*P, E, D*> for each subsequent event (i.e. node in the cascade diagram). When all these parameters are assessed, the next step is to carry out the actual risk calculations. These are carried out from right to left in the cascade diagram, starting with the leaf nodes and ending with the total risk for the accident scenario.

Before describing the actual risk quantification, it should be noted that the category values in Table 4.1 are given in logarithmic scale and should be transformed into "true values" to give the actual risk. These transformations are given in Eqs. (4.1)–(4.4) below. First, the actual frequency of the initiating event is given by:

$$f = 10^{F-4.5} \tag{4.1}$$

Here, for instance, $F = 2$ gives $f = 10^{-2.5}$, which is a frequency in "the middle of" the interval $(10^{-3}, 10^{-2})$, for category 2. This is based on the geometric mean of the category. So, when $F = 2$, the frequency equals $f = 10^{-2.5} = 0.00316$, being the geometric mean of the category 2 interval for *f*.

Similarly, the conditional probability of a subsequent event (loss of SFC) equals

$$p = 10^{P-4.5} \text{ for } P = 1,\ 2,\ 3,\ 4, \text{ and } p = 1 \text{ for } P = 5 \tag{4.2}$$

The extent, *e*, is given as

$$e = 10^{E} \tag{4.3}$$

Thus, category $E = 1$ in Table 4.1 corresponds to approximately $e \approx 10$ persons being affected, whereas category $E = 4$ means that in the order of 10,000 persons are affected by the loss of the SCF.

Finally, the duration is given as

$$d = 6^{D-1.5} \tag{4.4}$$

which is also based on the categories in Table 4.1. For example, $D = 4$ gives $d \approx 88.2$ h, which is quite close to the geometric mean of that category (≈ 90 h).

The present description is restricted to consider the consequence dimension "loss of service", where consequence of a lost SCF is defined in terms of E and D, and the total risk can be defined in terms of all relevant F, P, E and D. However, this type of categorization can be defined for any consequence dimension, for example, also for number of persons injured/killed and economic losses.

4.4.2 Risk Calculation

Now, returning to the cascade diagram, each node corresponds to the loss of service for a SCF. In order to calculate the mean consequence and thus the risk of the hazardous event, the calculation procedure starts with the leaf nodes, see Fig. 4.3. Consider a leaf node, j, having probability p_j to occur, and loss of SCF having extent e_j and duration d_j. The mean consequence C_j related to this leaf node is then given by:

$$C_j = p_j \cdot e_j \cdot d_j = 10^{P_j - 4.5} \cdot 10^{E_j} \cdot 6^{D_j - 1.5} j = 1, 2, \ldots \tag{4.5}$$

These consequences correspond to, $C_{1.1.1}$, $C_{1.1.2}$, $C_{1.1.3}$ and $C_{1.1.4}$, respectively, in Fig. 4.3.

When the mean consequence for each leaf node has been calculated, all consequences of a branch are combined into the merging node to the left (here SCF 1.1 in Fig. 4.3). When the risk related to this merging node is calculated, it is based on the consequences C_j for all nodes of the branch (as given for leaf nodes above) and the probability p_i for the merging node, i (here SCF 1.1). In other words, the mean consequences for nodes of a branch are summed and then multiplied with the probability of its merging node, to give the overall mean consequence for that branch, i:

$$C_i = p_i \cdot \sum\nolimits_j C_j = 10^{P_i - 4.5} \cdot \sum\nolimits_j C_j \tag{4.6}$$

Note that for convenience double indexing as C_{ij} is not used (implying that C_i and C_j have different interpretations). This process is repeated, following all branches to the left, and finally, the mean consequence of the hazardous event can be calculated, giving the total risk of the accident scenario:

$$R = 10^{F - 4.5} \cdot \sum\nolimits_k C_k = f \cdot C \tag{4.7}$$

Here, the summation is over all k, corresponding to the *geographical interdependencies*, that is, the SCFs *immediately to the right of the hazardous event* (i.e. $k = 1, 2, 3$ in Fig. 4.3), and f is the frequency of the hazardous event.

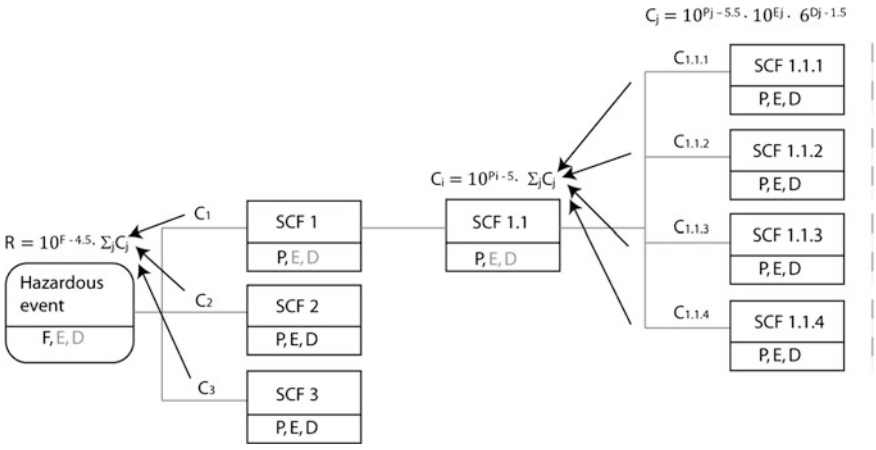

Fig. 4.3 The calculation procedure for the cascade diagram, from [1]

Observe that, except for leaf nodes and stop nodes, the *E* and *D* are in grey (see Fig. 4.3). This means that *E* and *D* are not used for consequence assessment of that node (and thus not during risk assessment). However, the *E* and *D* values are relevant for assessing the *P*s of the nodes directly to the right.

In short, the risk quantification procedure implies that one moves from left to right when parameters are assessed (as probabilities of SCFs can depend on the extent and duration of the node to the left). Further, relevant barriers are evaluated, and their effects on the *E* and *D* of a node are assessed. Next, when the mean consequences of all nodes are calculated, one moves from right to left to assess mean consequences. At last, the total risk $R = f \cdot C$ is calculated, from the frequency, f (Eq. 4.1) and the consequence, $C = \Sigma_k C_k$ In the above approach, *R* represents the mean number of person hours of lost services per year, due to the scenario being investigated.

4.4.3 Numerical Example: The Culvert Case

The estimated category values of *F, P, E* and *D* related to the loss of SCF ("loss of service") are now applied to the culvert case. Figure 4.4 shows the cascade diagram, inserted values for these parameters at the various SCF (nodes). The relevant location-specific (geographical) SCFs are electricity supply cables, ICT cables and the nearby railway D/A hall. The example only considers functional interdependencies related to the first of these, showing SCFs depending on electricity supply through the cables in the culvert. The relevant SCFs of the cascade diagram are identified through their physical objects, for example, cables and D/A hall, being the objects that are immediately affected.

In the diagram, the electricity supply cables are the physical components in the culvert, whereas the electricity supply represents the SCF. The probability

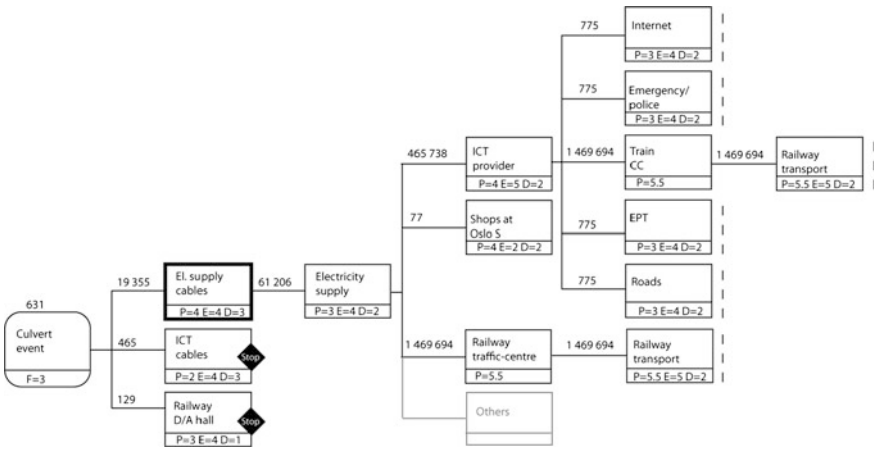

Fig. 4.4 Cascade diagram for the culvert scenario, showing interdependencies with values for <*P*, *E*, *D*>. *Black frame* indicates redundancy. EPT = electronic payment transfer. D/A = departure/arrival. From [1]

category of loss of electricity supply is $P = 3$. This is determined due to any redundancy that may be available, for example standby power units.

Observe that some nodes are allocated the probability category $P = 5$, which means $p = 1$. Such a strong coupling between the nodes can occur, for example between train communication and railway transport. If the train communication fails, then the railway transport is affected, regardless of extent and duration of the communication outage.

The calculations can be visualized, for example, by considering the leaf node "Internet" with $P = 3$, $E = 4$, $D = 2$. The contribution to risk of the scenario from this node can be calculated from Eq. (4.5):

$$C_{internet} = p \cdot e \cdot d = 10^{3-4.5} \cdot 10^4 \cdot 6^{2-1.5} = 775$$

The Internet node is combined with the other leaf nodes into the merging node "ICT provider" with $P = 4$, $E = 5$, $D = 2$ by using Eq. (4.6):

$$C_i = p_i \cdot \sum_j C_j = 10^{P_i - 4.5} \cdot \sum_j C_j = 10^{4-4.5} \cdot 1472792 = 465738$$

In this last calculation, E and D are not used, as discussed previously.

Further, the "ICT provider" node is merged into the node "electricity supply" which again is merged into "electricity supply cables". The calculations use the P values given in Fig. 4.4 and Eq. (4.6). The final calculation of risk for the scenario with $F = 3$ is calculated by using Eq. (4.7):

$$R = 10^{F-4.5} \cdot \sum_k C_k = 10^{3-4.5} \cdot 19949 = 631$$

The *F, P, E* and *D* values given in Fig. 4.4 show that the calculated risk for this scenario is equal to 631 person hours lost per year. In this case, the loss of railway transport contributes most to the total risk of the scenario.

4.5 Step (4): Generalizations and Additional Analyses (Optional)

The above approach is referred to as semi-quantitative since category values are used for the relevant risk parameters. This is often preferred, as exact values are very uncertain, and it can be more feasible to assess a category. However, if more exact values (e.g. of *f* or *p*) are available, a fully quantitative risk analysis can easily be carried out by directly using values of *f, p, e* and *d* instead of the categories used in the semi-quantitative approach. The relevant formulas are given above.

Further, the procedure described above treats all SCFs as equally important, that is, a duration of 10 h for $e \approx 10{,}000$ persons is equally important irrespective of which SCF is lost. This is hardly the case. However, it is straight forward to emphasize some SCFs as being more important than others by using weighting factors, see [2].

The above calculations have not treated *impact* interdependencies. One way to treat these is to increase the "extent" measure, *E*. A rough approach would be to increase all extent measures, *Ej*, with one unit for events with escalating failures or impact interdependencies. If these effects are strong, *Ej* could even be increased by two units and so on. A numerical measure for the impact interdependencies can then be established by calculating the risk for the hazardous event with and without treating impact interdependencies. The ratio between these two risk measures will give a quantitative expression of the strength of the nonlinear escalating failures.

4.6 Step (5): Risk Evaluation and Risk-Reducing Measures

The objective of a cross-sector RVA is often to get insight into a general class of hazardous events. Therefore, the analysis of a site-specific scenario (*cf.* the above culvert event) should be evaluated with respect to a corresponding generic event, by asking whether a similar event can occur in other places/locations of the geographical area that is investigated. If this is the case, one should assess whether these other events typically have higher or lower risks than the analysed scenario. In the culvert case, this means that one should consider the total number of similar objects (culverts) in Oslo and ask whether the culvert being analysed is more or less interconnected with other infrastructures than similar culverts. Such

evaluations are important to an overall assessment of risk, to consider whether overall risk is tolerable, and decide on risk-reducing measures.

The cascade diagram can be used during the process to suggest risk-reducing measures, in particular, by reducing interdependencies between the SCFs. The introduction/modification of barriers (organizational, human and physical) is important, for example, the separation of various SCF. Also, redundancy and emergency preparedness are typical measures. The effects of risk-reducing measures can be evaluated in the cascade diagram by changing frequency and/or consequence categories and then perform a re-calculation.

The assessments and evaluation of risk-reducing measures should of course be carried out in close cooperation with the stakeholders. The areas of responsibilities for private enterprises and public authorities can be unclear. So, when a plan for risk reduction is formulated, the responsibilities for implementing various measures must be clearly stated.

4.7 Step (6): Costs Caused by Loss of Service (Optional)

It can be useful to formalize the trade-offs between different consequence dimensions (e.g. when there are huge costs associated with implementing a risk-reducing measure). A first attempt to develop a normative guideline for trade-offs between different types of consequences is suggested as follows:

1. For *loss of service*, the consequence is described by extent e and duration d, as shown in Table 4.1. A first-order approximation for the total consequence is to take the product of e and d, which represents the total person hour of loss of service.
2. Also for other consequence dimensions, such as *safety* (loss of life), *economy* and *environment*, categories similar to those presented in Table 4.1 are established (see Table 3.1).
3. Category 1 for economy is assumed to correspond to category 1 for loss of service; category 2 for economy corresponds to a category 2 for loss of service and so on. Thus, a trade-off between economy and loss of service is implicitly given.
4. By systematically utilizing this trade-off between consequence categories, a regression line can be fitted in order to relate economy to loss of service. If y represents the economic impact (in million EUR) and $x = e \cdot d$ represents the total person hour in terms of loss of service, a log–log equation can be established between these (using values in Table 3.1 and Fig. 3.2).

The estimated log–log equation between y = economic impact and x = person hours lost becomes

$$\ln y = 0.57 \ln x - 6.4 \tag{4.8}$$

Considering the culvert case, we have that the extreme event that actually happened at Oslo S caused approximately 1.5 million person hours lack of service. The economic impact of this is by Eq. (4.8) equal to:

$$y = \exp(0.57 \ln 1\,500\,000 - 6.4) \approx 5.5 \text{ million EURs} \tag{4.9}$$

The cost of risk-reducing measures can now be assessed by a formal approach; keeping in mind that Eq. (4.8) is just a first-order assessment of the trade-offs.

The nonlinear relation (4.8) can be applied for the consequences ($x = e \cdot d$) for all SCFs in the cascade diagram. Next, the cost figures are propagated to the left in the cascade diagram by multiplying with probabilities and adding contributions from each branch. The expected "cost" given that the scenario occurs is then found to be approximately 250,000 EURs, and by multiplying with the frequency of the scenario, we are left with an expected yearly cost of approximately 8,000 EURs (without any risk-reducing measures being implemented).

A redundant electricity cable will almost eliminate the expected cost; hence, such a measure may be defended if the yearly capital cost is in the order of magnitude of 8,000 EUR or less.

In railway transportation, a delay is often valued in the range of 0.25 EURs per passenger minutes (averaged over various categories of travellers). A linear cost function of passenger minutes delay coincides with Eq. (4.8) for $x \approx 60{,}000$ person hours. For smaller values of x, Eq. (4.8) gives a higher value compared to railway transportation, and for larger values, the result is turned the other way around due to the nonlinearity of Eq. (4.8). Therefore, a proposed measure more in line with what is used in transportation would be

$$\ln y = 0.8 \ln x - 9 \tag{4.10}$$

where y still is the cost equivalent in million EURs and x is person hours. Note that a calibration of such a transformation usually is required, and in most cases, it is necessary to differentiate depending on type of critical infrastructure.

4.8 Conclusions

This chapter has described an approach to interdependencies, which can be performed as a simple qualitative analysis using a cascade diagram, but which may be extended with more complicated semi-quantitative or quantitative analyses, if needed. The cascade diagram is introduced as an important tool for performing the analyses. In the semi-quantitative approach, the total risk across the relevant sectors and SCF are assessed, defining probabilities and consequences in terms of categories. An example scenario is considered, involving electricity supply and ICT, as well as railway transportation: defining risk as person hours with loss of service. Additional, more detailed analyses are also considered, for example, to assess costs related to the likely losses of the scenario.

References

1. Utne, I. B., Hokstad, P., & Vatn, J. (2011). A method for risk modelling of interdependencies in critical infrastructures. *Reliability Engineering and System Safety, 96*, 671–678.
2. Utne, I. B., Hokstad, P., & Vatn, J. (2009). *A method to modeling interdependencies in risk analysis of critical infrastructures. Reliability, Risk and Safety: Theory and Applications*. Florida: CRC Press.
3. DSB (2008) Fire in cable culvert. Oslo central station (In Norwegian: Brann i kabelkulvert. Oslo Sentralstasjon 27.11.2007). Directorate for civil protection and emergency planning (DSB), Tønsberg, Norway.

Chapter 5
Modelling, Simulation and Vulnerability Analysis of Interdependent Technical Infrastructures

Jonas Johansson and Henrik Hassel

Abstract In this chapter, a modelling framework for interdependent technical infrastructures is presented. As input to the framework, characteristics of interdependencies and the objectives of the modelling framework are discussed. The overall approach is to divide the modelling of technical infrastructures into two parts, a topological part and a functional part. The topological part describes the structure and how components are connected. The functional part describes the flow of the infrastructure and how the system reacts when strains affect it. This generic approach of how to model individual infrastructures then enables the inclusion of dependencies in and analyses of a "system-of-system" model. Three perspectives of vulnerability analyses are also presented: global vulnerability, critical components and geographical vulnerability. The presented framework is utilized in, but not limited to, the context of vulnerability analyses in Chap. 6 for two different types of interdependent technical infrastructures.

5.1 Introduction

As discussed in Chap. 1, modelling and simulation approaches generally aim to assist an analyst in understanding how disturbances cascade through a set of interconnected infrastructures. Chapter 4 presented one way of analysing

J. Johansson (✉)
Department of Industrial Engineering and Automation, Lund University, Lund, Sweden
e-mail: jonas.johansson@iea.lth.se

J. Johansson · H. Hassel
Lund University Centre for Risk Assessment and Management (LUCRAM), Lund, Sweden
e-mail: henrik.hassel@lucram.lu.se

H. Hassel
Department of Fire Safety Engineering and Systems Safety, Lund University, Lund, Sweden

P. Hokstad et al. (eds.), *Risk and Interdependencies in Critical Infrastructures*, Springer Series in Reliability Engineering, DOI: 10.1007/978-1-4471-4661-2_5,

interdependencies between critical infrastructures, where scenarios are analysed "manually" using cascade diagrams. The present chapter addresses the task of modelling and simulating interdependent infrastructure systems from a different perspective. Here, the task is to model infrastructure systems and their interdependencies, in order to run computer simulations to assess the behaviour of the infrastructures when subjected to strains. In order to identify and understand the effects of interdependencies and the consequences that can arise, an approach for vulnerability analysis is also presented. It should be noted that the framework presented here is of a general character rather than being a specific tool which can be straightforwardly applied in a specific situation. Instead, the framework should be seen as providing a platform for modelling interdependent infrastructures, but it must be complemented with expert knowledge, specific tools and models which are adapted to the particular modelling task and analysis of interest. In Chap. 6, the use of the framework for modelling and vulnerability analysis of specific interdependent infrastructures is exemplified. Although the framework is only exemplified in a vulnerability analysis context, the framework could also be utilized in reliability analysis approach, as, for example, the one described in Chap. 7.

In the development of the framework, several guiding criteria were formulated. They are briefly described here to guide the reader with respect to the purpose and limitations of the framework. Firstly, the modelling framework enables analyses that are looking beyond "N−1" contingencies. "N−1" is a design criterion extensively used in the context of critical infrastructures [1, 2], which says that a system should be able to tolerate the loss of any *single* component and still maintain full function. Looking beyond N−1 means that the aim is to systematically generate a large number of scenarios (simulating failures) involving more than a single failure, to find out what will happen in the systems given the failures and to assess their negative consequences. With a more "manual" approach, it would not be possible to do that in the same systematic and comprehensive way. Secondly, since the goal is to be able to analyse a large number of scenarios, the simulation times (i.e. how computational burdensome the model is) become critical. A concern with limiting simulation times often leads to approaches that are limited in scope in terms of only considering single failures (N−1), for example the one performed by Koonce et al. [3], or not performing an exhaustive search but rather a partial assessment [1]. However, only addressing single failures or conducting partial analyses is likely to fail to capture many important insights—especially unexpected or non-intuitive aspects. Thirdly, the proposed framework is only applicable to those critical infrastructure systems that can feasibly be described as networks. This is, in reality, a rather limited constraint since a wide range of systems can be described in the form of networks (*cf.* [4]), such as social networks (e.g. celebrity networks), technical networks (e.g. the Internet, transport, water supply and electrical power systems), cellular networks and the studies of the written human language.

In Chap. 1, a number of challenges for modelling and simulating critical infrastructures were given. In Sect. 5.1, we add to these challenges in terms of a way of how to characterize and model interdependencies. A framework for modelling interdependent infrastructures, presenting features and the purpose of the framework, is given in Sect. 5.2. This framework is useful for developing infrastructure models that take interdependencies into account and for demonstrating how expert knowledge from various infrastructure domains can be integrated into a system-of-systems model. Sections 5.3 and 5.4 present the frameworks for single and interdependent infrastructures, respectively. In Sect. 5.5, the concept of vulnerability analysis is introduced, discussing how this type of analysis can be used to inform decision-makers and giving three perspectives of this type of analysis approach.

The modelling framework and analysis approach presented here is utilized in Chap. 6 in two case studies of interdependent infrastructures. Chapter 6 more clearly exemplifies issues such as how to model infrastructures by using the framework, generate potential failure scenarios, assess what will happen in the infrastructures given the occurrence of the failure scenario and estimate the severity of the negative consequences.

5.2 Characterization of Interdependencies

In Chap. 1, a general description of interdependencies and how to characterize them was given. Here, we formalize and operationalize these concepts in order to fit the presented modelling framework. There are some different interpretations of what constitutes an interdependency. Rinaldi et al. [5] argue that interdependency is a bidirectional relationship between two infrastructures. Interdependency can also be interpreted as a unidirectional relationship between two infrastructures (e.g. Ref. [6]). In the present section, we define interdependency to be a bidirectional relationship, and dependency is defined as a unidirectional relationship. In general, interdependencies are macro-properties of coupled systems that stem from dependencies between different components of the systems.

Dependencies can be direct or indirect. *Direct dependencies*, denoted as first-order dependencies, are direct couplings between two systems, system i is dependent on system j. *Indirect dependencies*, denoted as higher-order dependencies, are dependencies between systems through other systems. For example, if system i is dependent on system j and system j is dependent on system k, then a second-order dependency exists between systems i and k. Considering more than two systems simultaneously, which have direct dependencies between them, enables the possibility to capture higher-order dependencies.

Several suggestions of categorizations of interdependencies and dependencies exist in the literature. In Chap. 1, the classification proposed by Rinaldi et al. [5] was described where four types of interdependencies are distinguished (physical, information/cyber, logical and geographical). Zimmerman [7], on the other hand, only differs between functional and spatial interdependencies. Zimmerman's use of spatial interdependencies corresponds to how Rinaldi et al. use the term geographical interdependency. Finally, Lee et al. [8] differ between four types of functional interdependencies and use the term collocated dependency to denote what Rinaldi et al. refer to as geographical interdependency. On a more general level, these categorizations can be divided into two main types of dependencies, namely *functional* and *geographical*. These two classes of dependencies were described in Chap. 2 and note that the third class described in Chap. 2, impact dependencies, is seen as a subset of functional dependency in the present modelling approach.

A *functional dependency* exists when the function of a component in one infrastructure depends on the function of a component in another infrastructure. An example can be that a fresh water pumping station is dependent on electricity provided by a certain node in the electric power network; and if the node is no longer able to provide its services, the pumping station no longer functions. Several of the categorizations, referred to above, distinguish between different types of functional dependencies, for example, physical and informational. However, in a modelling context, they can often be treated similarly. The other category, *geographical dependency*, exists when two (or more) components are located proximate to each other—enabling an external event (e.g. weather phenomena, explosion, etc.) to negatively affect the functioning of both.

Vulnerabilities due to functional and geographical dependencies have been exploited in several past events, for example, the 2005 storm Gudrun [9] in Sweden and the 1998 Ice Storm in Canada [10]. This has also been the case with respect to geographical dependencies, such as in the Kista power disruption [11] and Hurricane Katrina [12]. Furthermore, in many cases, it is actually a combined effect of functional and geographical dependencies that determine the severity of the negative consequences due to strains. As such, this points to a need for including them both simultaneously in analyses of critical infrastructures.

5.3 Objectives of the Modelling Framework

The authors of the present chapter have developed a modelling framework that is particular useful for the analysis of individual as well as interdependent technical infrastructures. The goal is to better understand the infrastructures, with a special focus on what can go wrong (in a risk management context), and what the implications of interdependencies are for the functioning of the systems. The framework can be seen as complementing the approach described in Chap. 4 in that it tries to capture those interdependencies which may be difficult to capture

using more "manual" approaches. Of course, this is at the expense of a higher level of modelling detail and that computers must be used as a support. Below, the framework is presented first for a single infrastructure system and then for interdependent infrastructures.

There will never be a single best approach to the complex issue of modelling interdependent infrastructures, but rather different approaches adapted for different aspects of the problem at hand is advocated for. The objective of the presented modelling framework is to assist an analyst in:

1. Modelling technical infrastructures.
2. Representing functional and geographical dependencies between infrastructures.
3. Describing threats, hazards and unwanted events as either structural or functional strains.

A benefit of the modelling framework is that it gives a common platform for modelling different technical infrastructures, that is, in terms of a structural and a functional model. Each model of the infrastructures can be developed relatively independent, which facilitates the practical work of developing the models since several different competencies are usually necessary to develop the models.

5.4 Modelling Framework for Individual Infrastructure Systems

All technical infrastructures, and also many other types of systems, can be divided into two main parts, the first is the *structural part* of the system with the interconnections of system components and the second is the *functional part* that governs flow in the network. For an electrical power system, the first part describes busbars, breakers, switches, fuses, lines and cables and how they are connected and for a road transportation system it describes intersections, roundabouts and roads. The functional part describes, respectively, the flow of electricity and the flow of cars, busses and bicycles. The structural properties of a system is often governed by geographical constraints, such as the number of possible roads an intersection can have or the number of power lines that can occupy a limited geographical area. The functional properties are governed by physical constrains, such as the number of cars that can traverse a street or the amount of power that can be transferred through a cable. For both parts of the system, disturbances and unwanted events, henceforth termed by the general term *strains*, can affect either the structural properties or the functional properties, for example, a landslide that renders a road unusable (i.e. affecting the structural properties) or a slow moving car on the road (i.e. affecting the functional properties). Example of strains to a water system could be the caving in of a water pipe line (i.e. a structural strain) or the contamination of water supply systems by an antagonistic attack (i.e. a functional strain). Hence, we argue for a system model that differentiates and takes both these properties of the system into account [13].

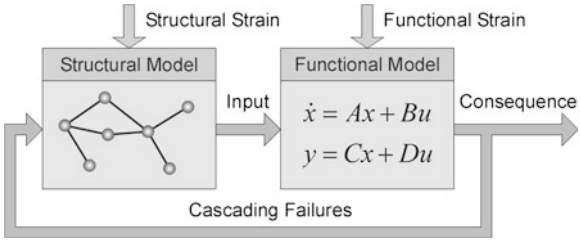

Fig. 5.1 Modelling framework for a single infrastructure. The structural model is exemplified with a network consisting of nodes and edges. The functional model is here exemplified with—but not restricted to—a first-order linear differential equation

The proposed representation of a system is to separate it into a structural model and a functional model, see Fig. 5.1. In the structural model, the system's physical components are represented as *nodes* (e.g. bus bar in a power system and a junction in a road transportation system) and *edges* (e.g. power lines and roads), the collection of nodes and edges are henceforth simply called components. This is similar to how a system is represented in the field of network theory (e.g. Ref. [14]). The geographical location of the components is kept track of in order to accommodate geographically constrained strains.

In the functional model, the system performance is evaluated taking into account both the topological constraints (e.g. all roads in operation) and the functional constraints (e.g. the number of cars from A to B and the capacity of the roads to accommodate the movement of cars). The functional model can range from simple topological models to advanced dynamical models which will affect how computational burdensome the model becomes. It is hence possible to utilize existing engineering models in the modelling framework, for example, for a power system, the power flow model as described in Chap. 7 could be used. However, these may be too computationally burdensome depending on the aim of the analysis (e.g. for a comprehensive vulnerability analyses of multiple interdependent infrastructures) and a more simplified functional model have to be developed. Essentially, this dwells down to a trade-off between the fidelity of the results and number of scenarios that can be analysed.

It should be noted that the division in structural and functional model is *implicitly* also normally done in existing engineering models for technical infrastructure systems. Here, however, we argue that by *explicitly* separating the structural and functional models, it enables the modelling of different types of technical infrastructures with the same modelling approach and in addition also enables the modelling of interdependent infrastructures as described in the next section. The benefits of explicitly dividing the modelling of technical infrastructures into a structural and a functional part are as follows:

1. It simplifies the modelling process and the description of modelling limitations with respect to the topological representation (structural model) and the flow properties of the system (functional model).
2. It is easier to contrast different types of analyses and the validity of the results from the analyses in terms of what types of strains that has been taken into consideration.
3. It can provide a structure to a management scheme, where mitigation actions to improve the system can be divided into improving the structure (e.g. having redundant components) and improving the function of the system (e.g. increasing the generation capacity in a power system or building a second lane for a road section in order to increase the throughput).
4. The modelling framework of individual infrastructures facilitates the modelling of interdependent infrastructures, as will be discussed in the next section.

External strains to the model of the system can be represented in two ways: as a structural strain or as a functional strain. *Structural strains* correspond to the removal of components in the system. *Functional strains* affect, in a general term, the function of the system, for example, change in demand, generation or the capacity of the system. An example of a structural strain could be the flooding of a river that makes one or several roads impassable, which is represented in the structural model by the removal of the affected edges. A structural strain is thus always binary in the modelling framework; either the component is in function or out of function. An example of a functional strain is the partial flooding of the road, hence affecting the capacity of the road or a sudden increase in the demand of an infrastructure service—for example, more cars want to use the road system than "normal". Functional strains are thus continuously represented in the modelling framework.

Another important aspect to consider in a modelling framework for technical infrastructures is so-called internal cascading failures. Internal cascading failures are introduced by the physical limitations of a system. An example of internal cascading failures is the following with respect to an electric power transmission system; an external structural strain renders a power line out of function (e.g. an airplane flying into the power line), the flow of the network thus directly changes, as given by the functional model, and more power is transferred on remaining power lines, one of the power lines gets overloaded (i.e. carries a greater load than its designed capacity), and the protection system trips the overloaded line. The tripping of the overloaded line is represented as a strain to the structural model (i.e. removal of the overloaded line). This continues until either no more lines are overloaded (and consequently tripped) or there is no more line to trip. In more general terms, an internal cascading failure corresponds to a strain (functional or structural) that causes other elements of the system to be overloaded, as determined by the functional model. These overloaded elements in turn cause a structural strain through a feedback loop, that is, the removal of one or several elements in the structural model. Depending on the system and the aim of the analysis, internal cascading failures are in some cases necessary to account for but in other cases less so.

5.5 Modelling Framework for Interdependent Technical Infrastructures

The modelling framework for individual infrastructures, described in the previous section, provides a common platform for modelling interdependent technical infrastructures, since all infrastructures are modelled in the same fundamental way, see Fig. 5.2. The modelling framework for interdependent technical infrastructures takes its point of departure from the individual infrastructures. Each system is initially mapped and modelled from the viewpoint of the single infrastructure and its direct dependencies to other infrastructures. These individual models are then merged into a "system-of-systems" representation. There are several benefits with such an approach. Firstly, expert knowledge regarding each type of infrastructure can be utilized for the construction of the individual models. Secondly, it can also solve some practical difficulties when it comes to confidentiality issues regarding studies of real-life systems—since it is only one party that has the whole picture and there is little or no need to share all of the information to all involved stakeholders.

When the individual system models are merged together, it is possible to study the effects of interdependencies between the systems. Of course, there is an upper limit regarding how many infrastructures that feasibly can be included in the same modelling task. This means that higher-order interdependencies between the infrastructures of interest which goes though infrastructures not included in the modelling task will not be captured. Hence, the choice of which infrastructures to include in a modelling task is a very important one.

In order to evaluate an individual system's performance, the functional model is used together with the structural model, as described in the previous section. But in addition, the status of the system's dependencies to other systems is also taken into account. The two types of dependencies introduced in Sect. 5.1, functional and geographical, are distinguished here. The geographical dependencies are modelled by defining the spatial location of each component in a three-dimensional Cartesian coordinate system.

The functional dependencies between the systems are modelled as *dependency edges* between components (nodes and/or edges) in different systems. For example, if a telecommunication router is dependent on power supply, it is modelled as a dependency edge from the telecommunication node to the node in the power system that supplies the router. If a component in a system no longer functions (e.g. can no longer supply power), the incoming dependency edges (if there exist any) from other systems are removed. The effects of the removal of a dependency edge are evaluated when updating the function of the dependent system, that is, each system only controls and acts upon its own local specific information regarding dependencies. In this way, cascading effects between the systems, due to dependencies, spread through the dependency edges between the structural models of the systems. Furthermore, interdependencies between two systems exist when there are two or more dependencies to and from the systems. Both direct and higher-order interdependencies are thus captured by the modelling

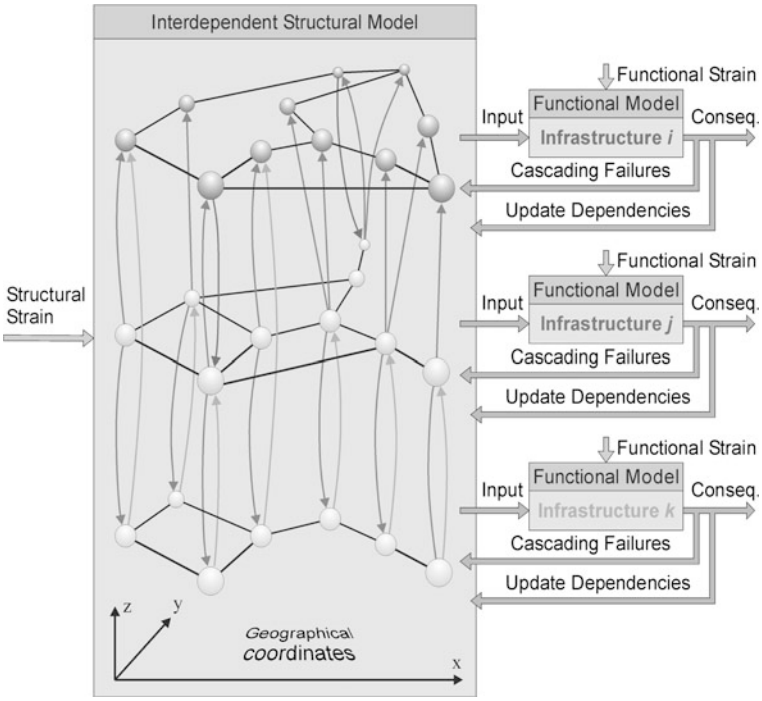

Fig. 5.2 Modelling framework for interdependent technical infrastructures. Two or more individual system models, in accordance with Fig. 5.1, are connected together through dependency edges into a "system-of-system" model

framework, which is essential for any interdependency modelling approach. The exact modelling procedure for how the removal of dependency edges affects a dependent system must be evaluated on a case by case basis depending on how the infrastructure is affected. In Chap. 6, examples of how dependency edges and their effect can be modelled are given.

Technical infrastructures are usually very tightly coupled in the sense that disruptions in one infrastructure have a direct impact on dependent infrastructures. In order to loosen the tight coupling between infrastructures, some type of buffer is often incorporated. Two examples of buffers are the use of uninterruptible power supply (UPS) in telecommunication and SCADA systems, and stocks of fuel in district heating systems and electric power generation systems in order to reduce the effect of disruption in fuel supply. Hence, an important aspect for modelling technical infrastructure dependencies is to incorporate the notion of buffers. The common denominator for these types of buffers is that they have a limited capacity, which in turn can be described as the time it can sustain its function without the service from the infrastructure it depends upon. Since the coupling between infrastructures is time dependent, due to the buffers, the restoration time of infrastructures under strain becomes important. The interdependent modelling

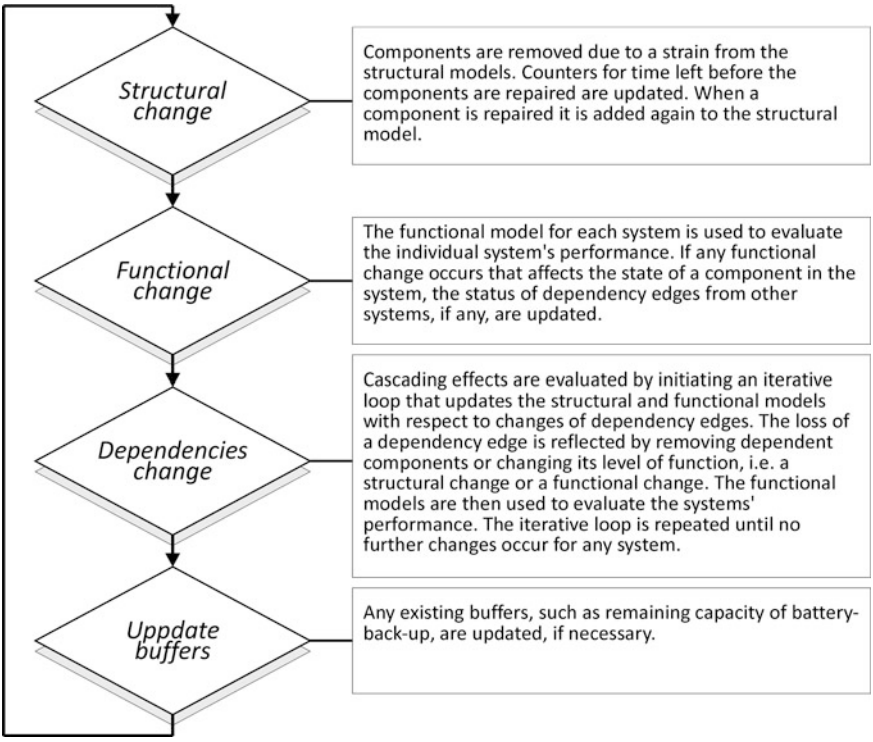

Fig. 5.3 Description of the different steps in one evaluation cycle in the framework for modelling and analysing interdependent infrastructures

framework can thus also incorporate time dependencies where the full cycle of strains to the infrastructures and restoration from the strains, in order to return to normal operation, is taken into account. In the first case study, interdependent water and electricity supply system, a time-independent approach is exemplified and in the second case study in Chap. 6, interdependent railway system, a time-dependent approach is exemplified. In Fig. 5.3, a short description of the steps that are carried out within one evaluation cycle is given.

5.6 Key Aspects to Consider in Applying the Framework

When modelling technical infrastructures in accordance with the proposed framework, the following list of questions or checkpoints can be helpful. In Chap. 6, when applying the framework in actual case studies, examples of considerations involved when modelling infrastructures are given.

1. What is the purpose of the modelling task?
   - The purpose will affect which level of modelling detail that is needed, whether advanced models must be used or if simplified models suffice. If the goal, for example, is to make sound decisions regarding improvements of real-life systems, then the output from the analysis needs to have a higher accuracy and fidelity than if the purpose is only to give a general view of the effects of interdependencies.
2. What consequence measure(s) is/are of interest?
   - This is also highly related to what type of decisions the analysis is going to support. If the analysis is to be used as input for other studies, then more descriptive consequence measures should be used, such as customers without supply or amount of power not supplied, than if the purpose of the analysis is to on a more abstract and general level compares the effect of interdependencies for different infrastructures. It can also be beneficiary to start with simplified consequence measures for enabling initial and broad studies in order to identify problematic areas and possible high-consequence scenarios. These can then be further analysed with more descriptive and accurate consequence measures.
3. What competencies are needed to develop the model?
   - If the model should reflect the real-life performance of an actual infrastructure, in-depth knowledge of the infrastructures of interest must be taken into account. Since any single person will seldom have full knowledge of the operation, maintenance and planning of technical infrastructures, competencies from these areas should be identified and their knowledge should be reflected in the model of the system.
4. Are there any existing models of the systems that can be used?
   - Since technical infrastructures are man-made systems, physical aspects that control the behaviour of the system are generally well known, and in many cases, commercial software exist that could be used to this end. However, care should be taken with respect to both the amount of data these models need (which in some cases can be a vast practical problem to gather and verify) and how computationally burdensome these are (for example, the time it takes to attain a solution for a single scenario or the memory demand).
5. What level of detail of the models is required for capturing the relevant aspects?
   - This has to do with what the required level of fidelity of the results in order to guide decisions. In some cases, a simple model may capture all the relevant aspects, such as guiding decisions towards where weak points are in the systems on a relative scale, and sometimes, a more advanced model should be used in order to capture all the relevant aspects, such as the number of customers that will be affected in order to design emergency plans. More simplified models

may be sufficient to rank vulnerabilities in the system for a broad analysis, which result can be used to achieve consequence measures with higher fidelity by using more detailed models. Another related aspect to consider is which temporal resolution that is appropriate. In some cases, a simple static model (i.e. time independent) might suffice. However, in some cases, the behaviour of the system over time must be captured; and of course, this can be done using very different timescales (from seconds and hours to days and weeks). A single model can usually never capture all timescales, which means that the time resolution must be consciously decided on considering, for example, the purpose of the assessment and the resources at hand.

6. How much does the access of information constrain the modelling task?

- In many cases, the access of information can constrain the modelling approach significantly. Is information available in easily accessible databases or is it only available in blueprints or as knowledge of the actors that plan, operate and maintain the system? The information is easier to both accesses, convert and utilize, in the present modelling approach in the former case compared to the latter. Hence, the access to information puts constraints on what type of functional models that can be used, the level of detail the consequence measure can have, and ultimately, what type of decisions the results that the model generates can be used for.

5.7 Vulnerability Analysis of Technical Infrastructures

An important source of the complexity of today's society is the increasing interdependencies between technical infrastructures. Risk and vulnerability analyses are essential in the proactive decision-making process on how to build and manage these infrastructures, what risks and vulnerabilities we should accept and which measures to take. The reasons for conducting these analyses are basically to understand how systems can fail, the negative consequences of failures and the associated uncertainties (e.g. see Ref. [15]). The analyses are then used to inform decision-makers about risk and vulnerability-reducing measures.

As described in Chap. 2, vulnerability can be defined as the ability of a system to withstand adverse events and strains. Hence, a system can be vulnerable to certain hazard exposures but robust and resilient to others. A vulnerability analysis focuses on the consequences that arise given system failures and not on the likelihood of the various hazardous events. As demonstrated by the last decades of critical infrastructure collapses—for example, the Hurricane Katrina catastrophe, United States, 2005; United States Northeast blackout, United States, in 2003; the Auckland, New Zealand, blackout in 1998, it is important to also address these types of high-consequence scenarios, although their estimated probability of

occurrence might be low. A problem for vulnerability analysis is vast number of scenarios that must be analysed and evaluated in order to cover as many of the possible contingencies, which is a major challenge.

5.7.1 Vulnerability Analysis to Inform Decisions

A risk analysis (see Chap. 2 for an introduction) typically starts with identifying hazards or threats to the system (e.g. [16, 17, 18]), that is, phenomena that can trigger risk scenarios. If the studied system is complex, such as in the case of interdependent technical infrastructures, the number of relevant scenarios to analyse quickly becomes insurmountable. In practice, this forces the analyst to limit the number of scenarios addressed, leading to an incomplete risk analysis of the system. The limitation of scenarios tends to be based on likelihood: if the likelihood for the scenario is below a specific cut-off value, the scenario is disregarded. In practice, these likelihood estimations can be very difficult to make (e.g. lack of knowledge about the phenomena) and have questionable quality (i.e. associated with large uncertainties). Often, the likelihood estimations are based on prior knowledge of the event, for example, historical events, and/or based on assumptions such as generic and independent failure probabilities. This typically leads to very small likelihoods, and potential neglect, of higher-order failure scenarios. However, common causes such as malicious acts and natural hazards are possible, and these may be very difficult to capture in the analysis. An effect of this would be that the likelihood of higher-order failures is actually much higher than the likelihood estimated based on independence assumptions (e.g. Ref. [1]). As such, the traditional risk analysis approach may lead to the failure of accounting for high-consequence low-likelihood scenarios—which is the specific interest of vulnerability analyses. See Fig. 5.4 for a conceptual description of the different points of departures of risk and vulnerability analysis.

Vulnerability can, as described in Chap. 2, be defined as the inability of a system to withstand adverse events and strains. Vulnerability analysis can thus be characterized as the exploration and identification of unplanned or undesired states of a system and the estimation of the associated consequences. An argument in favour of applying vulnerability analysis is that by *first* considering the system's vulnerability and *then* considering plausible hazards and threats, it is likely that a more open mind regarding what can happen in the future is achieved. For a vulnerability analysis, the consequences that could arise due to system failures are the main concern, that is, the screening of important scenarios to consider is based on the consequence as opposed to the likelihood of them occurring as is done in most practical risk analysis. Applying vulnerability analysis means that the probabilities of the strains are not explicitly considered. Instead, the focus is on how well the systems can withstand a large variety of strains, that is, giving a notion of the systems' robustness and resilience. In order to subsequently make risk-related decisions regarding whether to reduce these vulnerabilities, one needs

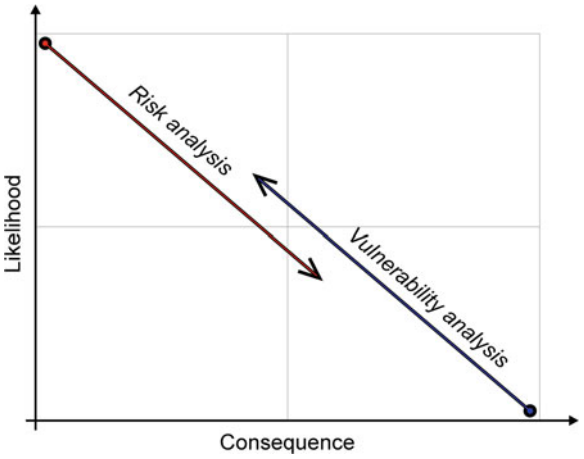

Fig. 5.4 Conceptual description of the difference between risk and vulnerability analysis

to address whether any plausible threats or hazards exist that can exploit these vulnerabilities—thus basically expanding the vulnerability analysis towards a risk analysis. Note, however, that even though an analyst may not be able to imagine a plausible hazard that can exploit the vulnerability, there may be reasons for reducing that vulnerability anyway. On a related issue, Hansson argues that "safety does not mean measures only against those hazards that are known and quantified, but also as far as possible against those that are unknown and unexpected" [19].

Furthermore, risk and vulnerability analyses provide valuable complementing information of the studied system and also typically highlight different mitigation strategies. If the risk is regarded as unacceptable, the mitigation strategy is normally to insert some form of barrier between the threat or hazard and the system. If the vulnerability is regarded as unacceptable, the mitigation strategy is normally to build a more robust and resilient system by changing the system.

Traditional methods for risk analysis, such as fault and event trees, are commonly applied to the analysis of critical infrastructure systems. However, there is growing recognition that these methods have limitations, especially related to handling the complexities of critical infrastructure systems [2, 20, 21]. With the framework for modelling technical interdependent infrastructures, described in this chapter, in combination with the vulnerability analysis presented here, some of the limitations of traditional approaches are addressed.

5.7.2 Perspectives on Vulnerability Analysis

In most of the methods suggested for analysing interdependent infrastructures, a single perspective on vulnerability is adopted, only covering some aspects of the system's vulnerability. Combining several perspectives provides a deeper understanding of possible contingencies and gives better input for policy-making

and planning processes (e.g. see Ref. [22]). Therefore, three different perspectives are pursued here. Each of these perspectives provides partial and complementing views on system vulnerability. Together, they provide a more complete picture, enabling a more comprehensive insight regarding the vulnerability of the system. These perspectives, exemplified in the two case studies in Chap. 6, are as follows:

1. Global vulnerability analysis,
2. Critical component analysis and
3. Geographical vulnerability analysis.

5.7.2.1 Global Vulnerability Analysis

Global vulnerability analysis is carried out by exposing the systems to strains of increasing magnitude and estimating the negative consequences that arise. This is done by simulating failures in a model of the system, for instance by removing an increasing number of components, and then estimating the consequences. And as the strain increases, the performance of the system degrades. If the system degrades slowly, it is robust, but if it degrades rather quickly, it is vulnerable.

A distinction is made between structural and functional strains. *Structural strains* are analysed by removing components, and the magnitude of a strain corresponds to the number/fraction of removed components. A global vulnerability analysis can also be carried out for *functional strains*, but the scope of the present chapter is limited to structural strains.

Since the character of structural strains differ, it is possible to employ different "removal strategies". In a random removal, for example, each component has the same probability of being removed. In addition, various types of directed removals can be employed, such as targeting components that in some sense are defined to be the "most critical" (for instance with respect to threats with malicious intent).

Global vulnerability analysis can provide information about a system's general robustness when exposed to strains of varying magnitude. One can, for example, identify whether there are critical thresholds, and the magnitude of the strain causing the infrastructure to collapse. For interdependent systems, it is also possible to identify how negative effects tend to cascade between systems. However, a global vulnerability analysis does not give an exhaustive picture of the systems' vulnerabilities, since only a sample of the state space, that is, all possible contingencies and operating states, is analysed in order to gain a representative picture of the system's vulnerability for different types and magnitudes of strain.

5.7.2.2 Critical Component Analysis

A critical component analysis is an exhaustive exploration of the system state to estimate the negative consequences of failure of a single or a set of components. The goal is to identify those sets of components that give rise to the largest

negative consequences, that is, those that are most critical for the system's function.

This approach is similar to contingency analysis as used in electric power system analysis (as described in Chap. 8). In such an analysis, normally, all N−1 contingencies (single failures), some selected N−2 contingencies, few N−3 contingencies and in some rare cases very few N−4 contingencies are usually analysed, based on the assumed probabilities of these failure combinations occurring. The combinatorial explosion puts an upper limit for the feasible number of simultaneous failures that can be studied, but in our case studies, there is a focus on covering an extensive part of the system state space. Exhaustive N−x contingency analysis is carried out, where a feasible x is typically in the order of 3–5 for single real-life systems and in the order of 2–3 for interdependent systems, depending on computational burden and allowed simulation times. The key point is trying not to miss out any, unexpected, sets of components that are critical.

5.7.2.3 Geographical Vulnerability Analysis

Geographical vulnerability analysis is an approach to study the effect of geographical interdependencies of critical infrastructures, that is, interdependencies that can for example be triggered by events such as hurricanes, tornados, earthquakes, explosions. This perspective is especially relevant to infrastructures that are highly co-located. The identification of critical geographical locations is carried out by dividing the geographical area, which the systems occupy, into smaller cells and systematically estimate the consequences when systems/components within a specific cell are simultaneously removed. Either a *generic vulnerability* analysis approach is adopted, as presented here, where the interest is to give an overall account of the systems vulnerability to geographically oriented strains, or a *hazard-specific vulnerability* analysis that more clearly relates the analysis to the exposures of a specific hazard, such as hurricanes, ice storms or earthquakes.

References

1. Mili, L., Qiu, W., Phadke, A. G. (2004). Risk assessment of catastrophic failures in electric power systems. *International Journal of Critical Infrastructures, 1*(1), 38–63.
2. IRGC. (2006). *White paper on managing and reducing social vulnerabilities from coupled critical infrastructures*. Geneva: International Risk Governance Council.
3. Koonce, A. M., Apostolakis, G. E., Cook, B. K. (2008). Bulk power grid risk analysis: Ranking infrastructure elements according to their risk significance. *Electrical Power and Energy Systems, 30*, 169–183.
4. Albert, R., & Barabási, A. L. (2002). Statistical mechanics of complex networks. *Review of Modern Physics, 74*(1), 47–97.
5. Rinaldi, S. M., Peerenboom, J. P., Kelley, T.K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine, 21*(6), 11–25.

6. McDaniels, T., Chang, S., Peterson, K., Mikawoz, J., Reed, D. (2007), Empirical framework for characterizing infrastructure failure interdependencies. *Journal of Infrastructure Systems, 13*(3), 175–184.
7. Zimmerman, R. (2001). Social implications of Infrastructure Interactions. *Journal of Urban Technology, 8*(3), 97–119.
8. Lee, E. E., Mitchell, J. E., Wallace, W. A. (2007), Restoration of Services in Interdependent Infrastructure systems: A network flow approach. *IEEE Transactions on Systems, Man, and Cybernetics-Part C: Applications and reviews, 37*(6), 1303–1317.
9. Energimyndigheten (2005). *Stormen Gudrun—Konsekvenser för nätbolag och samhälle*. Stockholm: Swedish Energy Agency.
10. Chang, S. E., McDaniels, T. L., Mikawoz, J., & Peterson, K. (2007). Infrastructure failure interdependencies in extreme events: Power outage consequences in the 1998 Ice Storm. *Natural Hazards, 41*, 337–358.
11. Deverell, E. (2003). *The 2001 Kista blackout: Corporate crisis and urban contingency*. Stockholm: Försvarshögskolan.
12. Leavitt, W. M., & Kiefer, J. J. (2006), Infrastructure interdependency and the creation of a normal disaster: The case of hurricane katrina and the city of New Orleans. *Public Works Management Policy, 10*(4), 306–314
13. Johansson, J., & Hassel, H. (2010). An approach for modelling interdependent infrastructures in the context of vulnerability analysis. *Reliability Engineering and System Safety, 95*(12), 1335–1344.
14. Newman, M. E., (2003). The structure and function of complex networks. *SIAM Review, 45*(2), 167–256
15. Paté-Cornell, M. E., & Dillon, R. L. (2006). The respective roles of risk and decision analyses in decision support. *Decision Analysis, 3*(4), 220–32.
16. Dilley, M., & Boudreau, T. (2001). Coming to terms with vulnerability: A critique of the food security definition. *Food Policy, 26*(3), 229–247.
17. McEntire, D. A., (2003). Searching for a holistic paradigm and policy guide: A proposal for the future of emergency management. *International Journal of Emergency Management, 1*(3), 298–308.
18. Kaplan, S., & Garrick, B. J. (1981). On the quantitative definition of risk. *Risk Analysis, 1*(1), 11–27.
19. Hansson, S.O. (2005). The epistemology of technological risk. *Techné*: *Research in Philosophy and Technology, 9*(2), 68–80.
20. Hollnagel, E., Woods, D. D., & Leveson, N. (Eds.). (2006). *Resilience engineering: Concepts and precepts*. Aldershot, UK: Ashgate Publishing Limited.
21. Zio, E. (2007). From complexity science to reliability efficiency: A new way of looking at complex network systems and critical infrastructures. *International Journal of Critical Infrastructures, 3*(3/4), 488–508.
22. Murray, A. T., Matisziw, T. C., Grubesic, T. H. (2008) A methodological overview of network vulnerability analysis. *Growth and Change, 39*(4), 573–592.

Chapter 6
Vulnerability Analyses of Interdependent Technical Infrastructures

Jonas Johansson and Henrik Hassel

Abstract In this chapter, the modelling framework presented in Chap. 5 will be used to perform vulnerability analyses from three perspectives: global vulnerability, critical components, and geographical vulnerability. Two case studies of two real-world interdependent infrastructure systems are performed; one focusing on an electric distribution system coupled with a water distribution system, and one focusing on a railway system which is composed of seven interdependent systems.

6.1 Introduction

The present chapter utilizes the modelling framework for interdependent critical infrastructures, Sects. 5.3–5.4, in the context of vulnerability analysis, as presented in Sect. 5.5. The goal is to exemplify, through case studies, both the modelling of actual infrastructures and the type of results that can be obtained from vulnerability analyses. Assumptions and simplifications needed for the modelling as well as how to carry out vulnerability analyses in a more practical sense are addressed. The two case studies are both from a Swedish context and the types of infrastructures addressed are as follows:

J. Johansson (✉)
Department of Industrial Engineering and Automation, Lund University, Lund, Sweden
e-mail: jonas.johansson@iea.lth.se

J. Johansson · H. Hassel
Lund University Centre for Risk Assessment and Management (LUCRAM), Lund, Sweden
e-mail: henrik.hassel@lucram.lu.se

H. Hassel
Department of Fire Safety Engineering and Systems Safety, Lund University, Lund, Sweden

P. Hokstad et al. (eds.), *Risk and Interdependencies in Critical Infrastructures*, Springer Series in Reliability Engineering, DOI: 10.1007/978-1-4471-4661-2_6,

1 Interdependent electric distribution system (EDS) and water distribution system (WDS).
2 Railway system consisting of seven interdependent systems.

The modelling of the infrastructures followed the outlined framework given in Sects. 5.3 and 5.4. In each of the case studies, specific information of simplifications, assumptions and how the infrastructures were represented, in terms of structural and functional models, are given. The models of the systems were represented in numerical matrix forms (structural model) and algorithms (functional model). The simulation cycle structure given in Fig. 5.3 was implemented in computer executable code. The system representation and implementation were carried out using MATLAB.

The first case study is presented in Sect. 6.2, and the second case study is presented in Sect. 6.3. In Sect. 6.4, some general conclusions from the case studies are presented, focusing on the effects of interdependencies between critical infrastructures.

6.2 Case Study 1: Electric Distribution System and Water Distribution System

This case study presents the results from a vulnerability analysis of an electric power distribution system (EDS) and a water distribution system (WDS), which is dependent on the EDS, located in a Swedish municipality (based on a master thesis work, Öberg [4]). The analysis covers the three perspectives of vulnerability analysis as presented in Sect. 5.5. Figure 6.1 and Table 6.1 give an overview of the two systems and the dependencies between them. The total amount of customers that is supplied by the EDS is 47,523 and 47,108 customers for the WDS.

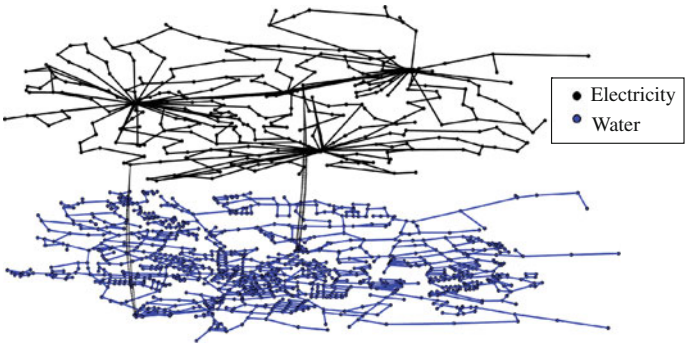

Fig. 6.1 An overview of the water distribution and the electrical distribution system with dependencies represented as edges between the systems

Table 6.1 Overview of the modelled system

System		Structural model	Conditions and dependencies	Functional model/ consequence measure
1. Water distr.	Nodes 1118	Pumps, water reservoirs, pipe junctions and customer points	10 dependency edges from pumping stations to substations in the electric distribution system. If dependency edge lost, the associated pump no longer can supply water	Functional model: Breadth first search algorithm with capacity constraints Consequence measure: Number of customers not supplied with water
	Edges 1513	Pipes	–	
2. Elec. distr.	Nodes 352	Transformers, substations and busbars	–	Functional model: Breadth first search algorithm with capacity constraints Consequence measure: Number of customers not supplied with electricity
	Edges 452	Cables (no overhead lines in the system)	–	

Total number of nodes is 1,470 and total number of edges is 1,965 for the system, giving a total number of components of 3,435. Total number of dependency edges is 10

6.2.1 System Description and Network Modelling

Here, the modelling of the systems in terms of structural models and functional models is addressed, exemplifying how the framework presented in the previous chapter can be utilized for real systems. First, the modelling of the electrical distribution systems (EDS) is given, which is then followed by the WDS and its dependency on the EDS. There is no dependency for the EDS on the WDS.

6.2.1.1 The Water Distribution System

The structural model, shown in Fig. 6.2, of the WDS is based on water pipe drawings provided by the utility owner. In total, there are 1,118 nodes and 1,513 edges in the structural model. The nodes represent pumps, water reservoirs, pipe junctions and points where customers get access to the water. Pumps and water reservoirs are modelled as *in-feed nodes,* and points where customers get access to water are modelled as *load nodes*. The edges represent water pipes. Water pipes with dimensions between 30 and 600 mm in diameter are modelled; hence, the smallest pipes from distribution pipes to the households are not considered. Under normal operation, the system is divided into two sections ("zones"), one low-pressure zone and one high-pressure zone. These two zones are treated as networks isolated from each other (as they are operated in real life). There are ways of connecting the zones together through valves; however, in reality, this has not been done or tested by the utility company during the last 20 years and therefore not taken into account here.

There are two pump stations in the system. At pump station A, the water is fed into the system (the only in-feed point). The water is pumped to pump station B, where a water reservoir (A) is located. This reservoir serves as a pressurizer to the

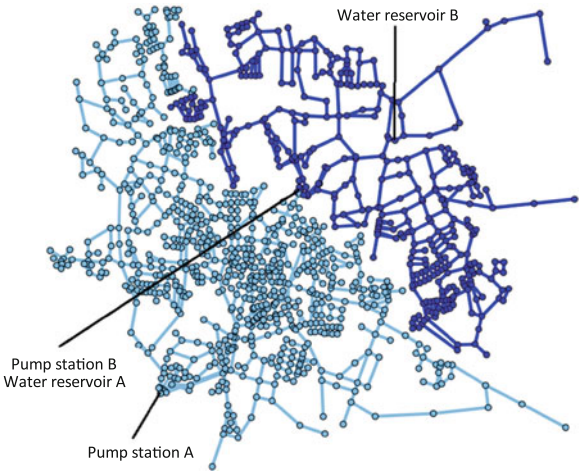

Fig. 6.2 An overview of the structural model of the water distribution system. *Light blue* indicates the low-pressure zone and *dark blue* indicates the high-pressure zone

low-pressure zone. Pump station B pumps the water to another water reservoir (B), a water tower, which pressurizes the high-pressure zone. The pump stations and water reservoirs are treated as in-feed nodes to each zone. In practise, the reservoirs can supply water as long as there is water left in them, that is, they act as buffers in the system. In order to simplify the modelling of the system, a time-independent simulation is performed which means that the time limitations of the reservoirs are not accounted for. Due to this simplification, the results of the analysis can mainly be used as a general guidance towards the magnitude of consequences that can arise, but not to guide decisions regarding, for example, the appropriate capacity for reservoirs or fuel tanks of auxiliary power generators.

Pump station A has four water pumps and pump station B has six water pumps, modelled as in-feed nodes. The water pumps are dependent on electric power to function. This is modelled as dependency edges between the nodes in the WDS (pump stations) and the nodes in the EDS (substations) being closest to the particular station. Since data were not easily accessible for determining the exact substations in the power distribution system that feed the pump stations, these dependencies were approximated with respect to their geographical distance.

There is a diesel backup power supply installed in the pump stations; however, since a time-independent simulation is performed, the backup supply is not accounted for. Hence, the simulations will depict a worst-case scenario with respect to the dependence on electric supply.

The functional model of the WDS is used to estimate the consequences that arise when the system is strained. The functional model used here is a capacity model taking into account in-feed node capacity and load node demands, but not taking capacity constraints for pipes (edges) into account. The algorithm starts from an in-feed node and tries to reach load points through breadth first searches[1] in the network. Once a load point is found, the demand of the load point is compared to the remaining in-feed capacity. If the in-feed capacity is higher than the demand, then the load point is flagged as supplied and its demand is subtracted from the in-feed capacity. This is continued until no capacity is left for the in-feed node or if there are no more unsupplied load points that can be reached. The same procedure is then repeated for each in-feed node (or until all load points are supplied).

At pump station A, the capacity of the water pumps was 400 l/s, and for the pumps at pump station B, it was 100 l/s. Detailed data on customer demands were not available, only total demand in the city (27,000 m^3/day), and the distribution between the high-pressure and low-pressure zone (58 and 42 %, respectively). The geographical distribution of customers and electric power demand for the electrical distribution system, see next Section, was used as a basis for determining customers and the total water demand for the load-point nodes in the WDS. It was

[1] Breadth first searches can be contrasted against depth first searches. Breadth first searches start in a node and find adjacent (neighbouring) nodes, the algorithm then continues to search in all these adjacent nodes before moving on and searching these nodes' neighbours. Contrasted against a depth first search where a single path from the start node to neighbouring nodes is explored, that is, only one neighbour at a time is considered and the search continued for.

assumed that the water reservoirs are able to completely cover the demand in each zone, giving a capacity of 11,300 and 15,700 m^3/day for reservoir A and B, respectively. The negative consequences are here equivalent to the measure chosen for the electric power distribution system, namely the *number of customers that do not receive water supply*.

6.2.1.2 The Electric Power Distribution System

The structural model of the urban power distribution system (voltage level of 10 kV) is shown in Fig. 6.3. There are a total number of 352 nodes and 452 edges in the model. The nodes represent transformers (from higher voltage levels to feed the 10 kV distribution system) and busbars (at the 10 kV level) and the edges represent cables (the network only compromises of underground cables with no overhead lines). Power is fed into the distribution network at three different geographical points. There is no local electricity production within the distribution system. In the in-feed points, the power is transformed from the sub-transmission system to the distribution system (from 130 to 10 kV). Two of the locations have three 130/10 kV transformers, whereas the third have two 130/10 kV transformers. Each transformer is modelled as an *in-feed node*, *that is,* as a node with a limited capacity to feed electricity to the distribution system. *Load-point nodes*, that is, nodes where electricity is consumed, are here modelled as the substations where customers are connected either directly (large power consumers such as hospitals or industries) or through 10/0.4 kV transformers and low-voltage networks (e.g. households, smaller industries and commercial buildings). Here, only the distribution system (10 kV) is modelled, that is, transformers from medium voltage (10 kV) to low voltage (0.4 kV), and the low-voltage networks are not modelled. Instead, the customers in the low-voltage networks are aggregated to the substations that they are normally feed from. This is one way to simplify the structural model of the distribution system without sacrificing too much fidelity of the results

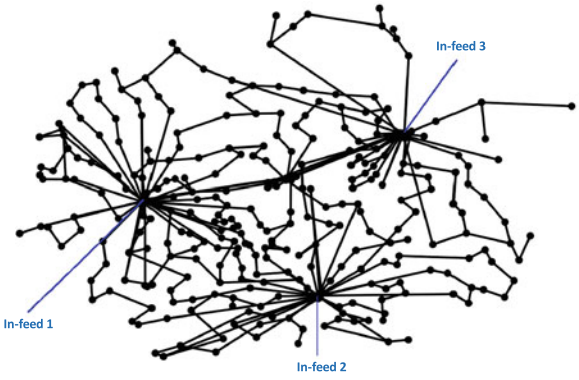

Fig. 6.3 An overview of the structural model of the electric power distribution system

and not having to gather all the information needed to model the low-voltage network. Furthermore, by limiting the size of the system to model, reasonable simulation times can be achieved.

The functional model determines which load-point nodes that are supplied with power, given a certain network configuration and available capacity. The functional model used for the EDS is similar to the one used for the WDS. Instead of considering water flows and consumption in terms of m^3/s, capacity in terms of MW (electric power) is considered for the EDS. As for the functional model for the WDS, capacity constraints for edges (i.e. the cables) are not accounted for in order to give reasonable simulation times. The capacities of the in-feed nodes (transformers) are 40 MW each (i.e. 320 MW in-feed capacity in total), and the total power demand of the municipality is 180 MW (distributed over the various load nodes according to actual data from the utility company). The negative consequences are here characterized as *the number of customers that do not receive power supply*.

6.2.2 Global Vulnerability Analysis

Here, we will exemplify some results from a global vulnerability analysis of the interdependent system. The analysis was carried out in accordance with Sect. 5.5, that is, components of the systems were randomly removed in increasing order and the consequences of the strained infrastructure were measured in terms of the fraction of customers who lost supply of the service provided by the infrastructure. The results in Figs. 6.4 and 6.5 are mean values from 1,000 iterations.

In Fig. 6.4, the strain is applied to either the WDS or the electric power distribution system (EDS). The consequences due to the strains are measured for both of the systems: in Fig. 6.4a the consequences for the WDS and in Fig. 6.4b the consequences for the EDS. When 10 % of the components of the WDS have been removed, roughly 42 % of the customers have lost water supply. When about 10 %

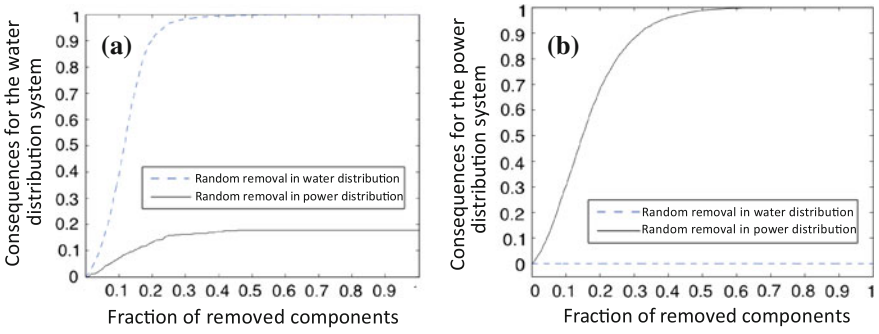

Fig. 6.4 The consequences in water distribution (**a**) and power distribution (**b**) when either water or power distribution system is exposed to random removal

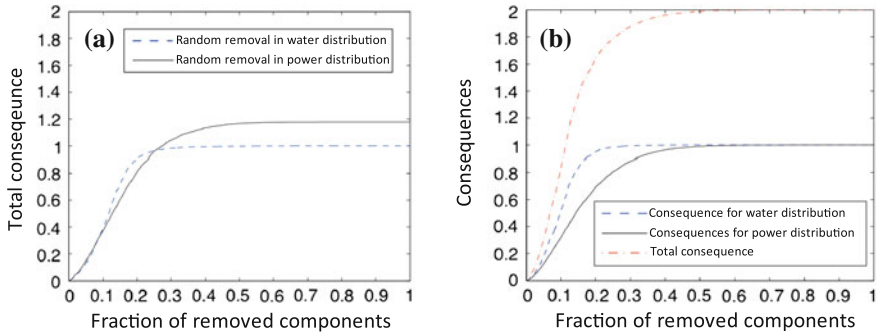

Fig. 6.5 The total consequences for random removal in either water distribution or power distribution (**a**), and the consequences in either water or power distribution for random removal in both systems simultaneously (**b**)

of the components of the EDS have been removed, roughly 25 % of the customers have lost power supply. Hence, from a vulnerability standpoint, the EDS is more robust when it comes to withstanding strains and still maintaining its function. In Fig. 6.4a, it can also be seen that when the electricity distribution is exposed to strain, up to about 20 % of customers will lose water supply—hence describing the effect of dependencies between the infrastructures. Contrasting this result with Fig. 6.4b, it is seen that there are no dependencies from the EDS to the WDS, since even if the water distribution is exposed to strain, no consequences arise for the EDS.

In Fig. 6.5, the focus has shifted to the "system-of-systems" instead of the individual systems. In Fig. 6.5a, the total consequences, in terms of the sum of customers that have lost water supply and/or electricity supply, are depicted given different magnitudes of strain to either the WDS or the EDS. The results reveal that the total consequences are higher when the EDS is exposed to strain than when the WDS is exposed. In Fig. 6.5b, the result is shown from an analysis where components from both the WDS and the EDS are removed simultaneously. It can be seen that when 10 % of the components in the infrastructures have been removed, 50 % of the customers have lost water supply and 30 % of the customers have lost power supply, giving the total consequences of 0.8. More or less, all customers have lost both water and power supply when about 60 % of the system components have been removed.

The global vulnerability analysis gives valuable information of the consequences when the system is exposed to strains of any magnitude. In order to carry out such an analysis, only a sample of the systems' states is covered.

6.2.3 Critical Component Analysis

A critical component analysis can be carried out to complement the picture of the system's vulnerability achieved in a global vulnerability analysis. Here, exhaustive

Table 6.2 The top ten critical components for single component failure

Single failure		Consequence WDS	Consequence EDS	Total consequences
Rank	System {Component}			
1	EDS {6}	8,373	1	8,374
2	EDS {204}	0	1,378	1,378
3	EDS {158}	0	1,364	1,364
4	WDS {279}	1,109	0	1,109
5	EDS {196}	0	1,096	1,096
6	WDS {1520}	1,087	0	1,087
7	WDS {284}	1,087	0	1,087
8	EDS {57}	0	1,054	1,054
9	EDS {157}	0	1,018	1,018
10	EDS {209}	0	1,010	1,010

analyses of the consequences of single and multiple component failures are carried out, as described in Sect. 5.5.

Table 6.2 gives the ten most critical single component failures, and the associated consequences, in any of the analysed systems. In total, 3,435 failure scenarios were analysed. The top three critical components all belong to the EDS. It is interesting to note that failure of component 6 in the EDS leads to 8 374 customers without water supply. This is due to the fact that component 6 in the EDS is feeding the main water pumps in the WDS (giving a strong dependency between EDS and WDS). For the remaining single component failures, consequences arise only in the system that is affected,that is, there are no single failures in either system that spread to the other system through dependencies other than the top-ranked one in Table 6.2.

Table 6.3 gives the top ten combinations of two component failures in any of the analysed systems and the associated consequences. In total, about 5.9 million failure scenarios were analysed.

Of all the scenarios, roughly 70.5 % have consequences in either of the systems and roughly 6.5 % have consequences in both systems simultaneously.

Table 6.3 The top ten sets of critical components for two simultaneous failures

Two simultaneous failures		Consequence WDS	Consequence EDS	Total consequences
Rank	System {Component}			
1	WDS {2028} EDS {6}	32,055	1	32,056
2	WDS {1115} EDS {6}	32,055	1	32,056
3	WDS {650} EDS {6}	32,055	1	32,056
4	WDS {915} EDS {12}	15,503	1	15,054
5	EDS {299} EDS {314}	8,373	3,706	12,079
6	WDS {418} EDS {6}	11,329	1	11,330
7	WDS {423} EDS {6}	11,168	1	11,169
8	WDS {419} EDS {6}	11,168	1	11,169
9	WDS {613} EDS {6}	10,979	1	10,980
10	WDS {1975} EDS {6}	10,932	1	10,933

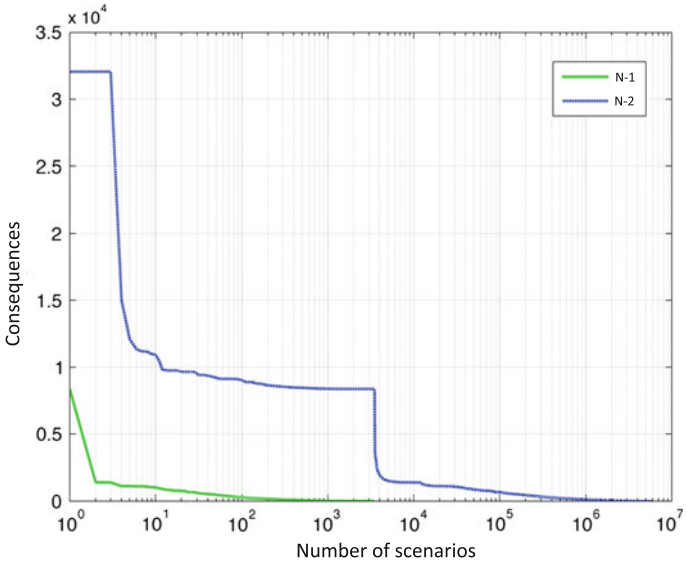

Fig. 6.6 Distribution of the severity of the consequences for single and two simultaneous failures

When contrasted with Table 6.2, it is apparent that the magnitude of the consequences drastically increases and that the consequences stem from the fact that single component in the two different systems fails simultaneously. The top three ranked failure sets give rise to 32,0565 customers without water and power supply. All these are combinations of component 6 in the EDS (electricity supply to pumps) and components that are related to water supply from reservoir A. Given the combined failure of electricity supply and one of these components in the water supply system leads to, all the customers in the low-pressure zone will be without water supply.

Figure 6.6 gives a summary of the critical component analyses in a distribution plot. This type of plot gives a notion of both the severity of the scenarios and the number of scenarios that give rise to considerable consequences, that is, the systems' robustness for these types of failures. For one component failures, not many scenarios give rise to considerable consequences; so, as expected, the system is not particularly vulnerable to these types of strains. However, for two simultaneous failures, the consequences drastically increase; roughly 2.6 % (153,529) scenarios have consequences with at least 500 customers without water and/or electricity supply, in contrast to one component failures where only 1.2 % (40) scenarios gave rise to equally high consequences.

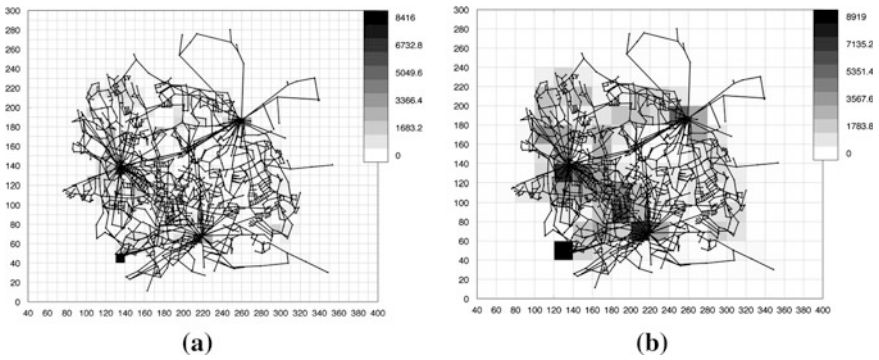

Fig. 6.7 Critical geographical locations when single areas are exposed to a strain. 250 m (10 scale units) cell size to the *left* (**a**) and 500 m (20 scale units) cell size to the right (**b**)

6.2.4 Geographical Vulnerability Analysis

The geographical vulnerability analysis, described in 5.5, was conducted by dividing the geographical area into squared cells. Three simulation studies were conducted. In the first study, the cell size was 250 × 250 m^2 (10 × 10 scale units), and in the second study, the cell size was 500 × 500 m^2 (20 × 20 scale units). In both these studies, one cell at a time was exposed to a strain, and all components located in that cell are removed. This could, for example, be related to a hazard such as a pipe break that leads to a flooding of substations, causing an electric short circuit and the substation to go out of operation. The results from the two studies are shown in Fig. 6.7a, b. The figures show the sum of the number of customers who lose power supply and the number of customers who lose water supply when the different geographical areas are exposed to strains. It can be seen that the most critical areas are around the three electric in-feed points and around the pump station A. Contrasting the results in the two figures indicate that the size of the strain, given the two cell sizes, leads to similar consequences and identification of critical areas.

In the third simulation study, two simultaneous geographical areas were exposed to a strain simultaneously. This was done only for the 500 × 500 m^2 cell size, and again, all components in each strained cell were removed. The result from the simulation is shown in Fig. 6.8. The figure describes the average consequences for all pairs of cells which include the specific cell under consideration. It can be seen that the average negative consequences are slightly larger than for the "single cell" case; however, the relative criticalities of the cells are very similar to that case. Analysing the results closer, it is possible to find locations were meshed parts or critical locations of the system that will be rendered out of function, giving rise to a high increase in the consequences in the study of two cells exposed, see Table 6.4. As seen in the table, for some simultaneously hit geographical areas, the total consequence to a large extent stems from one system,

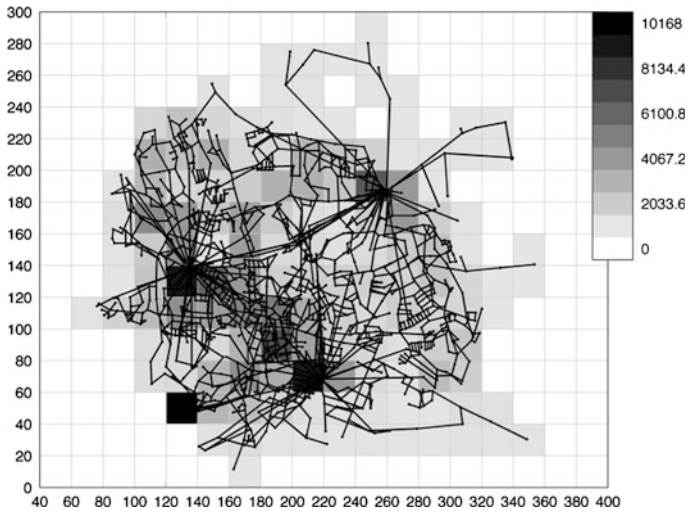

Fig. 6.8 Critical geographical locations, for a grid size of 500 m, where two areas are exposed simultaneously to failures. The criticality of a cell is the mean of the consequences for all pairs of cells which include the particular cell

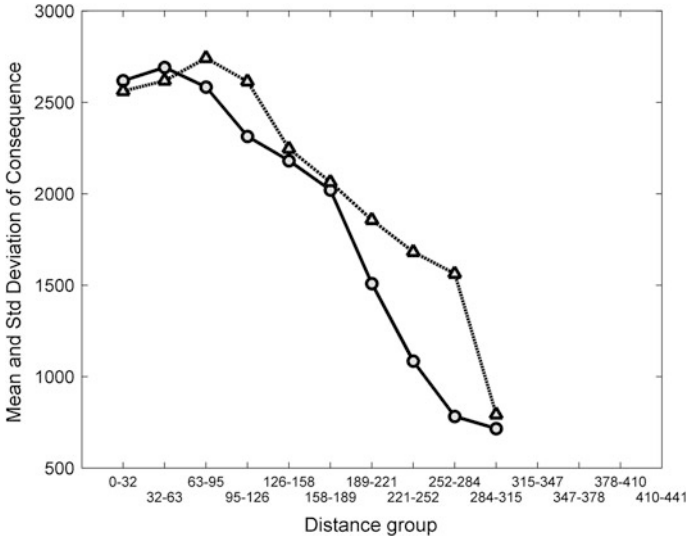

Fig. 6.9 Consequence versus distance plot for two simultaneously exposed areas. The mean (o) and standard deviation (Δ) of the consequences with respect to distance between the cells are shown. Only cells containing components have been included in the dataset

while for others, the consequences are more equally distributed between the systems. However, the consequences increase drastically, from the highest total consequence of 8416 in the "single cell" study to 36 695 for the "double cell"

Table 6.4 The top ten sets of critical cells for simultaneous failure of two cells

Rank	Cell 1 (x,y)	Cell 2 (x,y)	Consequence WDS	Consequence EDS	Total consequences
1	210, 70	130, 130	9,785	26,910	36,695
2	130, 50	210, 130	32,055	833	32,888
3	130, 50	210, 150	32,069	526	32,595
4	190, 70	130, 130	8,929	18,900	27,829
5	210, 70	250, 170	15,960	8,459	24,419
6	210, 70	130, 110	10,594	10,447	21,041
7	170, 70	130, 130	2,505	15,466	17,971
8	210, 90	250, 170	15,916	2,028	17,944
9	210, 70	110, 110	9,808	7,895	17,703
10	210, 110	250, 170	15,724	1,923	17,647

study. In Fig. 6.9, the consequence versus the distance between the simultaneously affected cells are plotted. The evaluated scenarios are divided into fourteen distance groups, characterized by the distance between the exposed areas. The mean consequences are highest at when the exposed areas are at between 0 and 95 scale unit distance (0–2.4 km) and then steadily decline as the distance grows. This indicates that the system is most vulnerable to hazards and threats that fit this description, that is, has exposure areas of 500×500 m^2 and can be separated by 0 up to 2.4 km. The standard deviations, in Fig. 6.9, for the different distance groups are relatively high compared to the mean values, which means that some combination of exposed areas gives rise to low consequences when simultaneously affected, while others give rise to high consequences. Hence, care should be taken to fully explore which combination of areas, and the components that fail to function, that renders the system vulnerable.

6.3 Case Study 2: Interdependent Railway System

This Section presents a case study of an interdependent railway system. The aim is to analyse the vulnerability of the railway system in Sweden, using the three different perspectives of vulnerability described above. In order to limit the scope of the study, only the southern part of the railway system in Sweden is included, see Fig. 6.10, and only structural strains to this system are analysed. This is a heavily trafficked part of the Swedish railway system corresponding to approximately a third of the Swedish railway system. The system consists of several technical infrastructures, and here, in order to limit the scope of the analysis, the system is analysed with respect to how disturbances in the technical infrastructures can spread through dependencies and affect the operation of trains. In Johansson and Hassel [2] and Johansson et al. [1], a more detailed account of the modelling approach and the vulnerability analyses are given.

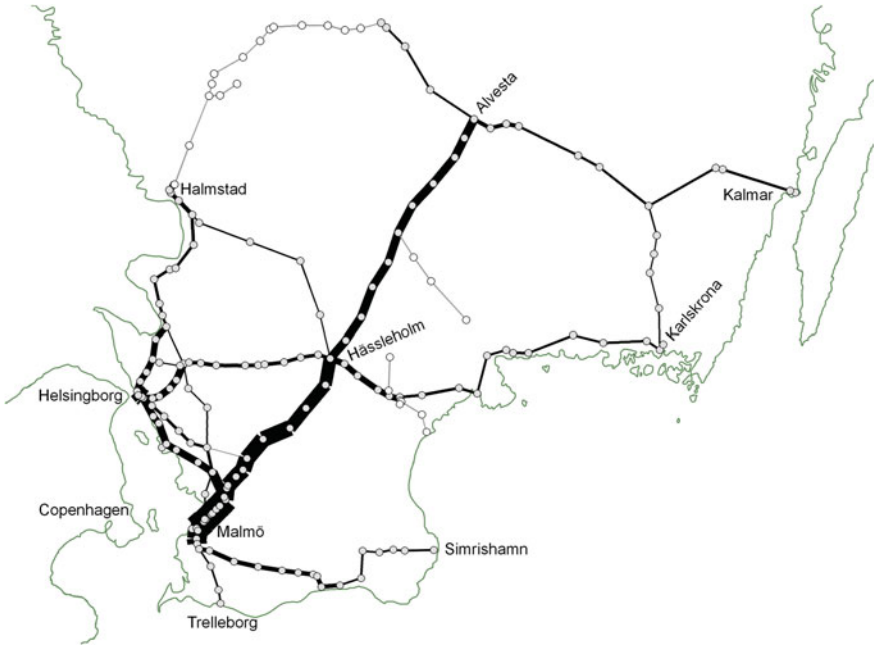

Fig. 6.10 The railway system in southern Sweden. The nodes are stations. The traffic loading on railway lines is indicated (*relative thickness of the line*). The figure also shows whether a segment is electrified (*grey nodes and black edges*) or not (*white nodes and grey edges*)

6.3.1 System Description

The main task of the Swedish railway system is to provide a railway infrastructure to a number of private train operators. The model of the railway system is based on documentation from and workshops with the former Swedish Railway Administration (Swedish: Banverket[2]). Four workshop sessions were conducted, involving staff from the Swedish Railway Administration and the Swedish Railway Training Centre. In total, 9 experts with specialist knowledge of different functions of the Swedish railway system participated in these workshops.

The railway system is decomposed in seven systems: Train operation, Railway tracks, Signal, Telecommunication, Traction power, Internal power and External power. The Train operation represents the railway traffic (i.e. the operation of trains), which is the *focus system* of the study since the interest is to study how disturbances in the other systems affect the railway traffic. The other systems are *supporting systems* since they provide no *direct* services to society. In Table 6.5, an overview of the systems and the main assumptions made are given. Figure 6.11

[2] The Swedish Railway Administration was in 2010 replaced with the new Swedish Transport Administration.

Table 6.5 Overview of the modelled railway system

System		Structural model	Key attributes	Conditions and dependencies	Functional model/Consequence Measure
1. Train operation	Nodes 169 (0)	Stations	–	–	Functional model and consequence measure in accordance with subsection "Railway track and Train operation below"
	Edges 179 (0)	Lines between stations	Maximum edge capacity (trains/h) Electrified or not	Edge capacity reduced when dependency edges to Signal, Railway tracks, or Traction power (only if electrified) are lost. 718 dependency edges in total	
2. Railway track	Nodes 500 (0)	Main switches	Restoration time: 12 h	–	No functional model Consequence measure: Fraction of components not functioning
	Edges 530 (238)	Single physical tracks	Restoration time: 12 h	–	
3. Trac. power	Nodes 456 (17)	Converters	Capacity Restoration time: 12 h	17 dependency edges to External power system	Functional model: Breadth first search algorithm with capacity constraints Consequence measure: Fraction of unsupplied nodes
		Overhead line connection points	Power consumption Restoration time: 6 h	Unbroken path to a converter Sufficient capacity left	
	Edges 465 (213)	Power lines	Restoration time: 6 h	Adjacent nodes supplied with power	
4. Signal	Nodes 122 (122)	Signal stations	Restoration time: 12 h	Dependency edge to telecommunication, to power switch or to external power. 232 dependency edges in total	No functional model Consequence measure: Fraction of components not functioning
	Edges – (–)	–	–	–	
5. Telecom	Nodes 111 (111)	Traffic management centre node	2 h UPS Restoration time: 2 h	111 dependency edges to power switch and to external power	Breadth first search algorithm without constraints Consequence measure: Fraction of nodes without any connection to traffic management centre node
		Routers	2 h UPS Restoration time: 2 h	Unbroken path to traffic management centre node. Dependency edge to power switch and/or to external power	
	Edges 124 (124)	Copper and fibre cables	Restoration time: 6 h	–	

(continued)

Table 6.5 (continued)

System		Structural model	Key attributes	Conditions and dependencies	Functional model/Consequence Measure
6a. Power switches	Nodes 122 (122)	Switches	Restoration time: 4 h	244 dependency edges to internal power	No functional model Consequence measure: Fraction of components not functioning
	Edges – (–)	–	–	–	
6b. Internal power	Nodes 128 (128)	In-feed transformer from External power	Capacity Restoration time: 4 h	6 dependency edges to external power	Functional model: Breadth first search algorithm with capacity constraints Consequence measure: Fraction of unsupplied nodes
		Transformers for power supply to the Signal stations	Power consumption Restoration time: 4 h	Unbroken path to transformer Sufficient capacity left	
	Edges 137 (137)	Power lines	Restoration time: 4 h	–	
7. External power	Nodes 128 (128)	Regional in-feeds, 130 kV	Capacity Restoration time: 2 h	–	No functional model Consequence measure: Fraction of components not functioning
		Local in-feeds 10/0,4 kV	Capacity Restoration time: 4 h	–	
	Edges – (–)	–	–	–	

The total number of nodes for the system is 1,736 (628 removable[a]) and the total number of edges is 1,435 (712 removable), giving a total number of components of 3,171 (1,340 removable). The total number of dependency edges is 1,328

[a] Certain components have been designated to be not removable in the vulnerability analyses. For Train operation, no components are removable since this is the focus system for the study of the effects of interdependencies. For the Railway track, switches and tracks in the stations are not removable, that is, only the tracks of the main railway lines are removable. For the Traction power system, only converters and the power lines between stations and power lines over the main tracks in stations are removable; the rest of the components in this system are not removable. The choice to set some components to be non-removable for Railway track and Traction power was done to reduce the complexity of the problem and study only main failures for these systems. Larger stations can have quite large networks of rails, switches and Traction power, and here, the focus was to study failures of the systems between stations and not in stations, hence setting these components to be non-removable

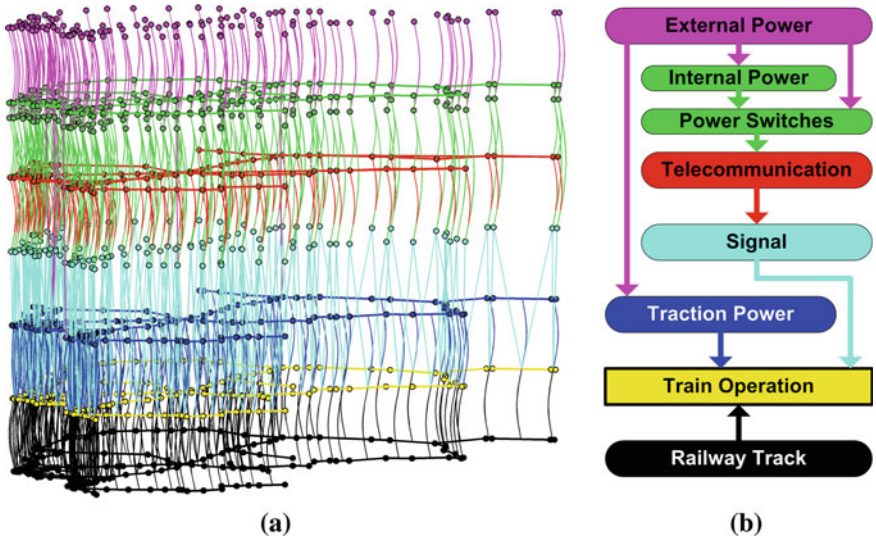

Fig. 6.11 The modelled railway system. From *top to bottom* External power, Internal power, Power switches, Telecommunication, Signal, Traction power, Train operation, Railway track. The dependency edges between the systems' components are also shown

provides an overview of the system including dependencies between the various components. The Train operation and the seven supporting systems of the railway system are described in the following

Sections, utilizing the following grouping: Railway track and Train operation, Telecommunication and Signal systems and Power systems.

6.3.1.1 Railway Track and Train Operation

For the Railway track system (system 2), each track is modelled explicitly as edges and the main railway switches are modelled as nodes. The consequences for the Train operation system are calculated as fraction of trains unable to reach their destinations. This requires a comparison between the number of trains that is planned to utilize a particular section of the railway, that is, the *traffic load*, and the number of trains that can be accommodated, that is, the *railway section capacity* (RSC). Both these parameters are measured as number of trains per hour.

The railway section capacities depend on the maximum RSC (RSC_{max}), given as the maximum number of trains per hour that can traverse a section of the railway. A railway section is defined as the direct path between two neighbouring railway stations. The maximum capacity stems from data derived from capacity calculations performed by the Swedish Railway Administration. The RSC for a specific section i is calculated as a function of the status of the Railway track (R), the Traction power (T) and the Signal systems (S):

Table 6.6 Capacity factors for a given section of the Railway system

Railway track		Traction power		Signal	
Functioning	FL_R	Functioning	FL_T	Functioning	FL_S
All dep.	1	All dep.	1	All dep.	1
1 of 2 dep.	0.3	1 of 2 dep.	0.3	No dep.	0.3
3 of 4 dep.	0.75	3 of 4 dep.	0.75		
2 of 4 dep.	0.5	2 of 4 dep.	0.5		
1 of 4 dep.	0.2	1 of 4 dep.	0.2		
No dep.	0	No dep.	0		

$$RSC_i = RSC_{max,i} \cdot FL_{R,i} \cdot FL_{T,i} \cdot FLS_{S,i} \tag{6.1}$$

where FL_R, FL_T and FL_S express the functioning level, [0, 1]. The functioning level describes how much the capacity of a section becomes if it loses dependency edges to the supporting systems. These factors were estimated in discussions with experts. In Table 6.6, an overview of the factors is given.

In order to estimate the traffic load, data were extracted from timetables for 2010. The timetables are used by the Swedish Railway Administration as a planning tool and include all trains utilizing the Swedish railway system during one year (7,999 unique trains in total). The timetables consist of data describing, for each individual train: start station, route stations, end station, travel time and the days of operation. These data were then processed based on the following criteria: first, trains with all of their route stations, the stations where the train is scheduled to pass, outside the studied region were omitted (1,947 trains left). Second, the part of the route that was outside the studied region for a given train was deleted. Third, trains that were identical in terms of having the same route were aggregated into specific *train routes* (321 train routes). Finally, train routes that had mirrored train routes, but in all other aspects were identical, were aggregated (198 train routes left). For each train route, a mean value of the average number of trains travelling that specific route during one hour was calculated. An overview of the traffic load is presented in Fig. 6.10. The processing of the data from individual trains into train routes was necessary in order to achieve feasible simulation times for the functional model of the Train operation.

The data regarding the traffic load are used to calculate the fraction of trains unable to reach their destinations, by comparing the number of trains per hour for the route with the capacity (maximum number of trains per hour) of the railway sections of the route. If the railway section capacity is sufficient for the train route, all trains within the train route are considered to be able to reach their destinations. The number of trains for the train route is then subtracted from the railway section capacities included in the route. The same procedure is carried out for all train routes. The negative consequence is then calculated as the *number of trains not able to reach their destinations*. Of course, there might be other relevant ways to estimate negative consequences, such as fraction of trains arriving late or estimates of the mean amount of time trains are arriving late given failures in the systems.

However, the modelling approach for Train operation utilized here does not capture these more detailed consequence estimates, which would require a model of the Train operation with a much higher level of detail—and subsequently would render the types of analyses carried out here impossible within reasonable time limits (here simulation times of less than a week was deemed reasonable). Contrast with discussions in Sects. 1.2 and 5.5.

6.3.1.2 Telecommunication and Signal Systems

The Telecommunication system (system 5) enables the transmission of information related to supervision and control of the railway system. It is composed of both copper and fibre optic cables that connect various routers, located in close proximity to the Signal stations, with the Traffic management centre node located in Malmö. Nodes in the Telecommunication system need power supply to function, and they also have uninterruptable power supply (UPS) backup (approximately 2 h) in case the power supply is disrupted. Supervision and control is conducted at the Traffic management centre, which means that routers must be connected to the Traffic management centre node in order to transmit information (i.e. to function).

The Signal system (system 4) gathers information regarding the status of the railway system and the Train operation as well as enables control functions to be executed, for example, changing the state of switches and signals along the railway track. It requires power supply in order to function, and the Telecommunication routers connected to the individual Signal stations must also function.

6.3.1.3 Electric Power Systems

There are three electric power systems. The Traction power system (system 3) is a distribution system for supplying electricity to trains (16 kV, 16 2/3 Hz). This system is supplied from converters located in five different stations in the studied area. A few parts of the studied system are not electrified and operated with diesel trains, as marked in Fig. 6.10.

The Internal power system (system 6) is an EDS (10 kV, 50 Hz), owned and operated by the Swedish Railway Administration, which supplies the Signal stations and Telecommunication routers with electricity. It also supplies other important functions, not included in the present model, such as heating of railway switches.

The External power system (system 7) includes both the sub-transmission (130 kV) and the local distribution systems (10/0.4 kV), which are owned and operated by a number of different private electricity distribution companies. The External power system feeds electricity to the Internal and Traction power systems (the sub-transmission system) and to the Signal stations and Telecommunication routers (the local distribution system). Here, the External power system is only

modelled as in-feed points, since it is primarily the vulnerability of the systems owned by the Swedish Railway Administration that are of interest and not the vulnerability of the External power system in itself.

6.3.2 Global Vulnerability Analysis

Simulations were performed for each of the seven supporting systems separately, by exposing them, one at a time, to a given structural strain and evaluating the consequences. The structural strain here was carried out as random removal of components in each of the supporting systems, in accordance with Sect. 5.5. One iteration consists of the random removal of one component all the way up the removal of all the components in the system and, for each removal step, estimates the consequences that arise. For each simulation, 1000 iterations were run. In Fig. 6.12, average values of the consequences for the Train operation system are presented. In Fig. 6.13, box plots are presented over the variation in consequences to the Train operation system for four different magnitudes of strain.

The results from the global vulnerability analysis reveal that the Railway track, on average, is the most critical system. To a large extent, this is an effect of the long restoration times of components in this system, clearly indicating the impact of restoration times on the outcome of the analysis. Only removing components in the Internal power system does not yield any consequences in the Train operation, simply because all systems that are normally dependent on the supply from the Internal power system can also receive power supply from the local in-feed points in the External distribution system via the Power switch. If strains would affect both the Internal Power and the External power simultaneously, the result would have been different. The result from a global vulnerability analysis gives valuable information of how the system reacts to varying magnitudes of strain, that is,

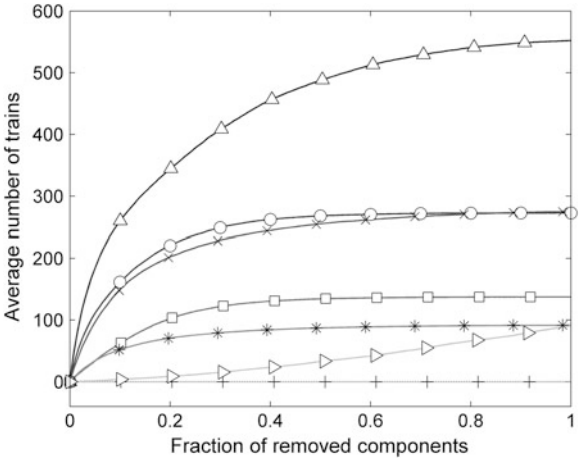

Fig. 6.12 Results from the global vulnerability analysis. The consequence for Train operation is displayed as a function of the fraction of components removed from the supporting systems: Railway tracks (*triangle*), Traction power (*circle*), Signal (*multi symbol*), Telecommunication (*square*), Power switch (*asterisk*), Internal power (*plus symbol*), External power (*right-faced triangle*)

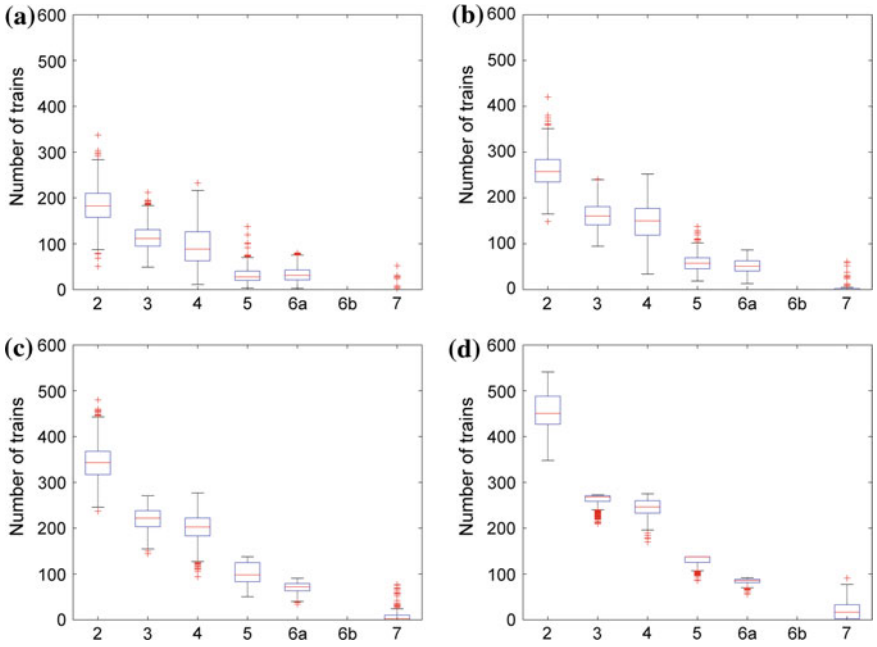

Fig. 6.13 Box plots displaying the variation in consequences, over 1,000 iterations, for the Train operation system when the supporting systems are exposed to random removal. Four different magnitudes of strain (fractions of removed components) are displayed: (**a**) 0.05, (**b**) 0.1, (**c**) 0.2 and (**d**) 0.4 are shown. The box corresponds to the lower and upper quartile values. The line in the box is the median value. The whiskers correspond to 1.5 times the interquartile range from the ends of the box. The + markings are data with values beyond the end of the whiskers

depicts the resilience of the system and also gives a picture of which support system that is most critical for the Train operation.

Figure 6.13 reveals that there are rather large variations in consequences over the 1000 iterations, indicating that the vulnerability of the system greatly varies depending on both which components that are removed and on the order of removal, illustrated by the data values marked with "+" above and below the whiskers for given magnitude of strain. This in turn indicates that some components are more critical for the system function than others. Since global vulnerability analysis only displays results on a system level, analysis on a component level is required to identify which these highly critical components are. This is done in the next Section.

6.3.3 Critical Component Analysis

Critical components and sets of components were analysed by performing exhaustive simulations of single failures and of two simultaneous failures, with

Table 6.7 Results from the analysis of critical components

Single failure		Consequences							
Rank	System {Comp}	Syst 1	Syst 2	Syst 3	Syst 4	Syst 5	Syst 6a	Syst 6b	Syst 7
1	3 {8}	144.6	0	24.2 %	0	0	0	0	0
2	4 {1}	141.1	0	0	0.82 %	0	0	0	0
3	5 {112}	137.4	0	0	45.1 %	100 %	0	0	0
4	4 {2}	114.0	0	0	0.82 %	0	0	0	0
5	4 {3}	110.6	0	0	0.82 %	0	0	0	0
6	2 {549}	110.2	0.42 %	0	0	0	0	0	0
7	2 {548}	110.2	0.42 %	0	0	0	0	0	0
8	2{545}	110.2	0.42 %	0	0	0	0	0	0
9	2{544}	110.2	0.42 %	0	0	0	0	0	0
10	2{533}	110.2	0.42 %	0	0	0	0	0	0
Two failures		Consequences							
1	3 {8} 5 {112}	241.9	0	24.2 %	45.1 %	100 %	0	0	0
2	3 {8} 4 {2}	235.0	0	24.2 %	0.82 %	0	0	0	0
3	3 {8} 4 {1}	234.5	0	24.2 %	0.82 %	0	0	0	0
…									
24	4 {1} 5 {112}	208.0	0	0	45.5 %	100 %	0	0	0
…									
27	2 {549} 5 {112}	202.6	0.42 %	0	45.1 %	100 %	0	0	0
28	2 {548} 5 {112}	202.6	0.42 %	0	45.1 %	100 %	0	0	0
…									
50	2 {959} 4 {1}	192.7	0.42 %	0	0.82 %	0	0	0	0
51	2 {957} 4 {1}	192.7	0.42 %	0	0.82 %	0	0	0	0

results presented in Table 6.7 and Fig. 6.14. Table 6.7 shows the ranking of the most critical components for single and two simultaneous failures. The first column of Table 6.7 shows the ranking in terms of the consequences that arise for Train operation. The second column shows the affected system, denoted in accordance with Table 6.5 and the identification number of the critical component(s), denoted as {X}. The third column of Table 6.7 describes the consequence for Train operation in terms of number of trains unable to reach their destination due to removal of the component(s). This number is estimated as an average value (see Sect. 6.2.1) and is therefore not an integer. Columns 4–10 show the consequences for the respective system in percentage, as defined in the System description section.

The results from single critical component analysis show that the component with identification number 8 in system 3 (Traction power) results in the highest consequences for the Train operation. This is a converter feeding two different segments of the railway system, including one of the most highly trafficked segments. The second most critical component has identification number 1 and belongs to system 4 (Signal). This component represents a Signal station located at one of the most highly trafficked sections of the studied railway system. The component resulting in the third largest consequence, if removed, is 5 {112}, that is, one of the components in the Telecommunication system. This component represents the Traffic management centre node and is highly important for the monitoring and control of the railway system. The fourth and fifth most critical components are Signal stations covering the monitoring of highly trafficked railway segments. Components ranked six to ten are all Railway tracks that belong to railway segments that have a high load of traffic.

The analysis of two simultaneous failures shows that the combination of failures in components 3 {8} and 5 {112}, that is, the converter and the Traffic management centre node described above, gives rise to the highest consequences. Component 3 {8} is included in combination with other components for the two simultaneous failures with rank 1–23 and 25–26. Screening out this component gives that the most critical simultaneous component failures include the component 5 {112} in combination with various other components, rank 27–49. Screening out also this component, component 4 {1} becomes critical in combination with various different components. This illustrates the problems regarding ranking the criticality of simultaneous failures, since single component that is highly critical themselves will pervade in the ranking of simultaneous component failures. In Jönsson et al. [3], we have presented an approach to overcome this problem by introducing the concept of "synergistic consequences" and various criticality measures, not introduced here to limit the extent of the case study example.

In Fig. 6.14, all the critical components for single failures (1,340 in total) and two simultaneous failures (897,130 in total) are given. These plots present the consequences for the supporting systems and the consequences that arise in the Train operation system. The general trend for both of the plots is that the consequence is much higher for the Train operation than the consequences that arise in the system(s) in which the component(s) is/are removed. They also clearly depict

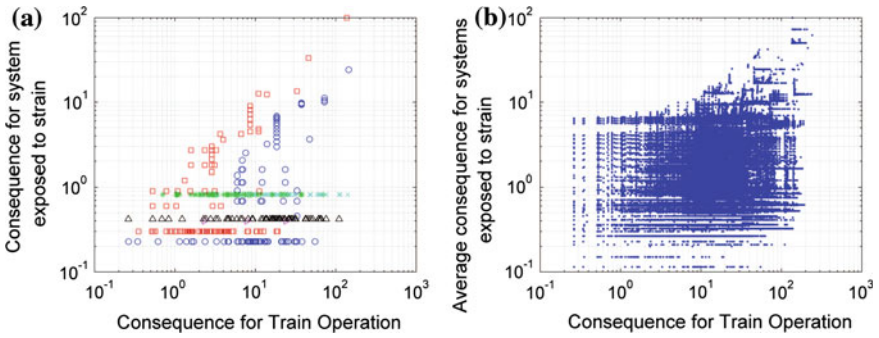

Fig. 6.14 The critical components for the interdependent system: (**a**) for single component failures and (**b**) for two simultaneous failures. The x-axis, for both (**a**) and (**b**), is the consequence for Train operation, and on the y-axis, (**a**), is the consequence for the system in which the component was removed or, (**b**), the average consequences for the systems from which the components were removed, (**b**). In (**a**), the system marking of the removed component correspond to that of Fig. 6.12, and in (**b**), only the level of the consequence is displayed and no reference to system is given

the varying consequences that arise depending on which components are removed, supporting the findings from the global vulnerability analysis.

The identification of critical components gives valuable insight into which components and combinations of components are highly important for the system function. This information can be used to point out which components should be especially protected and which components should be analysed in more depth in terms of whether there are possible hazards or threats that could render these components out of function.

6.3.4 Geographical Vulnerability Analysis

The geographical vulnerability analysis was carried out as an analysis of critical geographical locations, as described in Sect. 5.5. The study area was divided into 5 × 5 km large grid cells. The placement of the grid was random. The choice of cell size was guided by the interest to analyse the system's vulnerability to strains covering large geographical areas. Hazards that can correspond to this type of strain are, for example, strong wind, heavy snowfall, ice storm, flooding and earthquakes. For more in-depth analysis, the placement of the grid and the cell size should be further addressed. The analysis can also be viewed as a screening approach, identifying critical geographical areas where more studies should be carried out. In Johansson and Hassel [2], a more comprehensive geographical vulnerability study is carried out.

In Fig 6.15a–d, the result from the analysis is presented, displaying the consequences for Train operation when the supporting systems are put under strain. In Fig 6.15a, the simultaneous removal of all the components in each grid

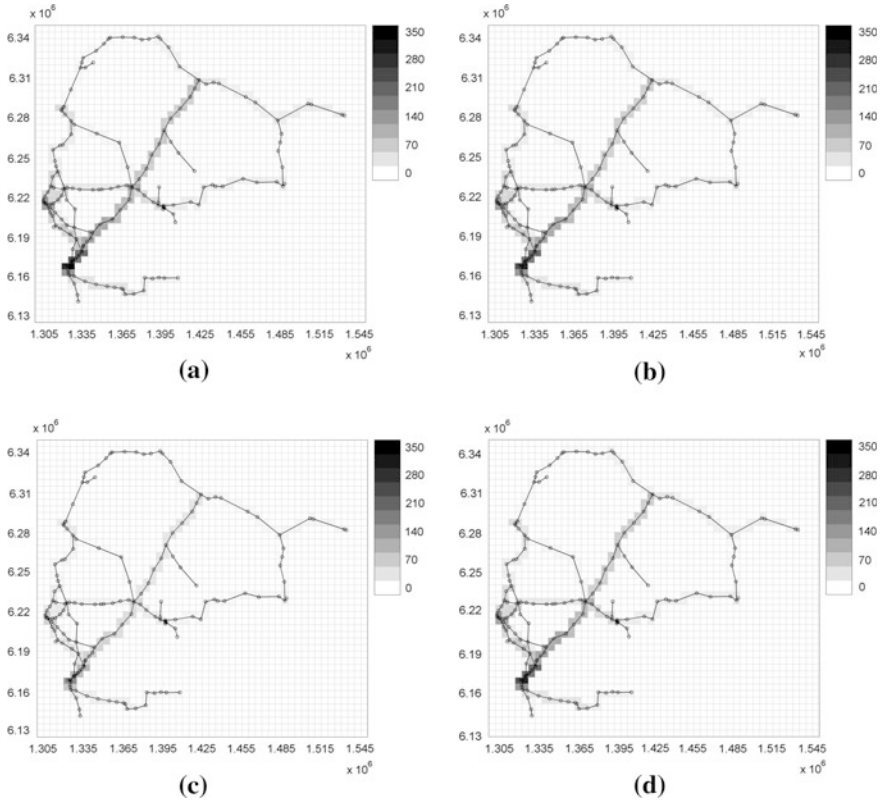

Fig. 6.15 Analysis of critical geographical locations. The shade of the cell corresponds to the consequence for Train operation in a linear scale from 0 to 350 trains. **a** System 2–7 are simultaneously affected by the strain. **b** Only system 2, Railway, is affected by the strain. **c** Only system 3, Traction Power, is affected by the strain. **d** Only system 4, Signal, is affected by the strain. The results for system 5–7 are not shown in order to limit the amount of figures, the consequences were generally lower and had the same trend as to which regions that were vulnerable

cell for systems 2–7 is presented. In Fig 6.15b-d, the effect of removing components in systems 2–4, respectively, is presented. The vulnerability of the geographically constrained strains largely corresponds to the most heavily trafficked railway segments, compare with Fig. 6.10. From these figures, it can be clearly concluded that the most critical location is in the Malmö region. A strain affecting all of the supporting systems, systems 2–7, in this cell gives a consequence of 345 trains for the Train operation.

The result above should be contrasted against the consequences that arise for this cell when only the Railway is affected, roughly 293 trains, when only Traction power is affected, roughly 151 trains, and when only Signal is affected, roughly 66 trains. The consequences for the Train operation due to geographically constrained

strains can thus not simply be aggregated (here it would lead to a too high of a value), since this would give inappropriate consequence estimations.

As such, it is important to address both functional dependencies and geographical dependencies at the same time when assessing the vulnerability of interdependent infrastructures.

For the individually affected systems, the highest consequences for Train operation arise when the Railway track is exposed to strains. This is largely due to the relatively long restoration times for this system in comparison to the other systems, see Table 6.5, and the capacity reduction factors when a whole segment of the railway is affected.

When contrasting the result of the geographical vulnerability analysis against the global vulnerability analysis, the ranking of the supporting systems' importance to the vulnerability of the Train operation generally remains the same. When the Railway track in the Malmö area is affected, 38 components are removed and the consequence for the Train operation is roughly 293 trains. In Fig. 6.12, the same average consequence arises with the random removal of roughly 31 Railway track components. The system is thus on average more vulnerable to the removal of 31 randomly chosen Railway track components than compared to a geographically constrained strain that removes 38 Railway track components. This seems intuitively correct since the random removal of Railway components can affect the Train operation throughout the whole studied area and not only a limited area. In Fig. 6.16, the consequence versus the distance of the simultaneously affected cells are plotted. The evaluated scenarios are divided into fourteen groups with an incremental step of 25 km. The mean consequence has a peak around 225–250 km with a slightly lower mean for shorter distances. This indicates that the system is most vulnerable to hazards and threats that could simultaneously expose two geographically decoupled areas, for example, two storms separated by roughly 235 km.

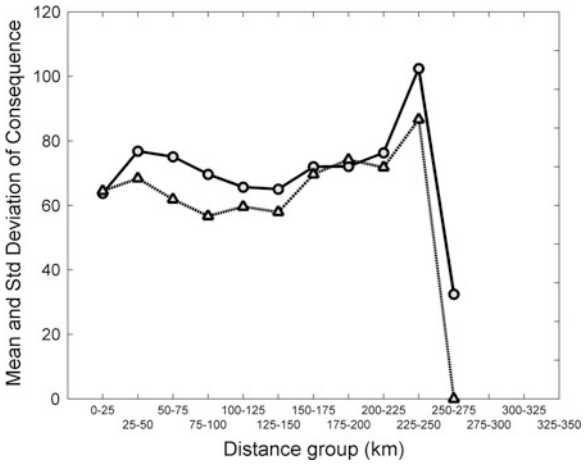

Fig. 6.16 Consequence versus distance plot for two simultaneously exposed areas. The mean (o) and standard deviation (Δ) of the consequences with respect to distance between the cells are shown. Only cells where components are located have been included in the dataset

The critical component analysis showed that the highest consequence for single failures is roughly 150 trains and for two simultaneous failures, roughly 240 trains. This should be contrasted with the worst possible consequences of roughly 550 trains. The failure of highly critical individual components can thus give rise to equally large consequences as the effect of large geographical strains. Hence, the protection of these critical nodes should be of utmost importance, if there is no viable option to redesign and restructure the systems to be more robust. The critical components, as listed in Table 6.7, are all located in the Malmö region. Complementing the information regarding the railway system's vulnerability has thus been found, from two different perspectives.

6.4 Concluding Remarks

The two case studies demonstrate that three perspectives give complementing information of the systems' vulnerability towards different types of strains. The global vulnerability analyses highlighted both the degree of dependence and the system-of-systems' ability to cope with small up to very large-scale strains. It could, for example, be concluded in the first case study that the WDS is in general more vulnerable than the EDS when it comes to removal of system components. Furthermore, it could be noted that even if the EDS is blacked out, the WDS can still deliver water to roughly 82 % of its customers (for a limited period of time), and in this perspective, the dependency between the systems are rather limited. In the second case study, the consequence for Train operation was described depending on which supporting system that was affected. Here, it could be concluded that the Railway tracks and the Traction power were the most critical systems and more significantly that high consequences could arise already for small amount of components out of function.

In order to exhaustively analyse the vulnerability of the systems for small magnitudes of strains, *critical component analyses* were carried out. The first case study revealed that the simultaneous failure of two components in the two different systems, electrical distribution system and water supply system, could lead to roughly 68 % of the customers without water supply. What is especially interesting to note is that two simultaneous failures in two different infrastructures gave rise to much higher consequences than two simultaneous failures in the same infrastructure; in fact, nine out of the ten top-ranked simultaneous failures belonged to the first category—clearly showing the need for studying the effects of interdependencies. The consequences for two simultaneous failures can be contrasted against roughly 18 % of the customers being without water supply for the worst single failures. The second case study also revealed that the highest consequences arise when components in different system fail as opposed to several components in the same system. These results clearly stress the importance of adopting a holistic system-of-systems view when analysing vulnerabilities of critical infrastructures.

The *geographical vulnerability analyses* give another perspective on the systems' vulnerabilities. Here, the focus is to address vulnerabilities due geographical dependencies, that is, components that are co-located and could be affected by geographically oriented common cause events. The geographical vulnerability analysis in the two case studies clearly depicted which geographical areas of the systems are more vulnerable to strains. Furthermore, the consequence versus the distance plots of simultaneously affected cell also revealed some interesting results. For the first case study, the system-of-system is most vulnerable to hazards and threats that simultaneously expose an area of limited size, whereas for the second case study, the system-of-system was more vulnerable to hazards and threats that can arise in two geographically decoupled regions simultaneously.

References

1. Johansson, J., Hassel, H., & Cedergren, A. (2011). Vulnerability analysis of interdependent critical infrastructures: case study of the Swedish railway system. *International Journal of Critical Infrastructures, 7*(4), 289–315.
2. Johansson J. & Hassel H. (2011). *Geographical vulnerability analysis of interdependent critical infrastructures*: *11th International Conference on Applications of Statistics and Probability in Civil Engineering* (*ICASP11*), Zurich, Switzerland, Aug 1–4 2011.
3. Jönsson, H., Johansson, J., & Johansson, H. (2008). Identifying critical components in technical infrastructure networks. *Journal of Risk and Reliability, 222*, 235–243.
4. Öberg E. (2011). Sårbarhetsanalys av samberoende infrastrukturer med användning av nätverksmodellering—En fallstudie av ett vatten- och eldistributionssystem. English edition: Vulnerability Analysis of Interdependent Infrastructures Using Network Modeling—A Case Study of a Water and a Electric Distribution System. Rapport 5357, Department of Fire Safety Engineering and Systems Safety, Lund University, Sweden.

Chapter 7
Risk Analysis of Electricity Supply

Gerd Kjølle and Oddbjørn Gjerde

Abstract Society is critically dependent on a reliable electricity supply to maintain its functionality. Electricity supply interruptions lead to direct consequences for the electricity users and will in general have an impact on dependent infrastructures and their services. This chapter describes a quantitative analytical approach for risk analysis of electricity supply. In this approach, the consequences of failures in the electricity system are analysed in terms of electricity supply interruptions to delivery points (DPs) serving for instance societal critical functions or other infrastructures. In a cross-sector risk analysis, this approach can be used in a detailed analysis for instance as input to cascade diagrams in the risk analysis of cascading failures and interdependencies with other infrastructures.

7.1 Introduction

Failures in the electricity system occur occasionally and most often with minor consequences. The electricity system on the national transmission level is a meshed network usually designed and operated according to the N-1 criterion, meaning that the system should withstand loss of a single principal component without causing interruptions of electricity supply. Local networks are mostly operated as radials and any component outage due to a failure will lead to interruption of electricity supply but reconfigurations are possible in some parts of the network.

G. Kjølle (✉) · O. Gjerde
SINTEF Energy Research, Trondheim, Norway
e-mail: Gerd.Kjolle@sintef.no

P. Hokstad et al. (eds.), *Risk and Interdependencies in Critical Infrastructures*, Springer Series in Reliability Engineering, DOI: 10.1007/978-1-4471-4661-2_7,

Blackouts or wide-area interruptions causing devastating impact on societal critical functions are most likely caused by combinations of failure events. However, coinciding independent or dependent failures in the electricity system is usually regarded to have (very) low probability compared to single failures. It is a major challenge in risk analysis of electricity supply to identify possible chains of events that could lead to wide-area interruptions and to further identify the consequences of cascading failures (cf. Sect. 2.7).

This chapter describes a quantitative analytical approach for risk analysis of electricity supply based on contingency and reliability analysis of electricity supply. In this approach, the consequences of failures in the electricity system are analysed in terms of electricity supply interruptions to delivery points (DPs) serving for instance societal critical functions or other infrastructures. The approach requires a rather profound knowledge of the electricity system, detailed computer models and specialized computer tools. Combined with reliability models describing failure and restoration processes of the electricity system and its components, this approach gives as result the risk of electricity supply interruptions. The approach can be used as a part of a detailed risk analysis (cf. Chap. 3) and the results as input for instance to cascade diagrams (cf. Chap. 4) in the risk analysis of cascading failures. In a cross-sector risk analysis, where the initiating event occurs in the electricity supply system, this approach constitutes the basis for describing the initiating undesired event before moving on to analysis of interdependencies in other critical infrastructures.

7.2 An Overview of the Risk Analysis Approach

The scope of risk analysis of electricity supply is to calculate the probability and consequences of electricity supply interruptions to certain DPs or parts of the network. Quantitative probabilistic approaches to reliability evaluation of the electricity system have been available for decades. Generally, these approaches aim to measure the adequacy of the system, *that is*, the ability of the system to supply the electricity required by the customers at all times. Adequacy relates to the existence of sufficient generation and network facilities within the system to satisfy the electricity demand. Various alternative methods are described in the literature, and tools have been developed, usually based on Monte Carlo simulations or analytical approaches. The essential task in either approach is to select different system states and assess their contribution to interruptions in electricity supply.

The different methods need input data of network (electrical) topology and power flow models, in addition to component reliability data. Basic results gained are reliability of supply indices for the DPs in terms of frequency of electricity supply interruptions, and severity indices, such as interruption duration, interrupted power and energy not supplied (ENS), as well as interruption costs (IC). These indices describe the risk of electricity interruptions. Further, consequences for dependent infrastructures, industrial sites or other types of DPs may be pursued.

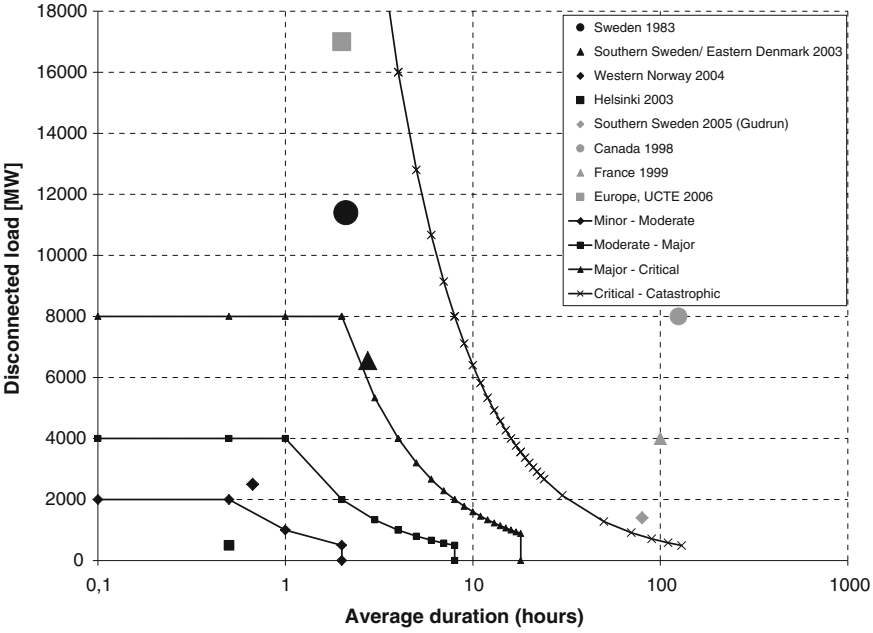

Fig. 7.1 Consequence diagram based on [1, 2]

Consequences of power system failures can, for instance, be classified according to the amount of disconnected load (i.e. interrupted power) and stipulated average (weighted) duration. Figure 7.1 gives an example of a consequence diagram using the two dimensions, disconnected load (MW) and average duration, for some blackouts in the past, based on [1, 2]. Figure 7.1 also shows an example of the classification of consequences from minor to catastrophic as defined by [1]. This classification will depend upon the system or area under study. The disconnected load-dimension will typically be scaled down for a small city compared to a large city, for a local area compared to a region of a country, and so on (see example in Chap. 8).

There are two groups of events shown in Fig. 7.1. Events in the first group to the left are typically initiated by technical or operational failures causing interruptions of limited duration but varying size in terms of area and load affected. The second group to the right consists of events where natural hazards (wind, icing) have caused wide geographical area damages to power lines resulting in comprehensive repair and extremely long durations.

Figure 7.2 gives an example of a risk matrix for those of the undesired events in Fig. 7.1 where information is available about the expected frequency of the event [1]. In this figure, the two dimensions of the consequence are combined into energy not supplied (MWh). Figure 7.2 shows that even though two of the events have critical consequences (Fig. 7.1), the risk is moderate due to the expected infrequent occurrence. The consequence diagram and risk graph are similar to the

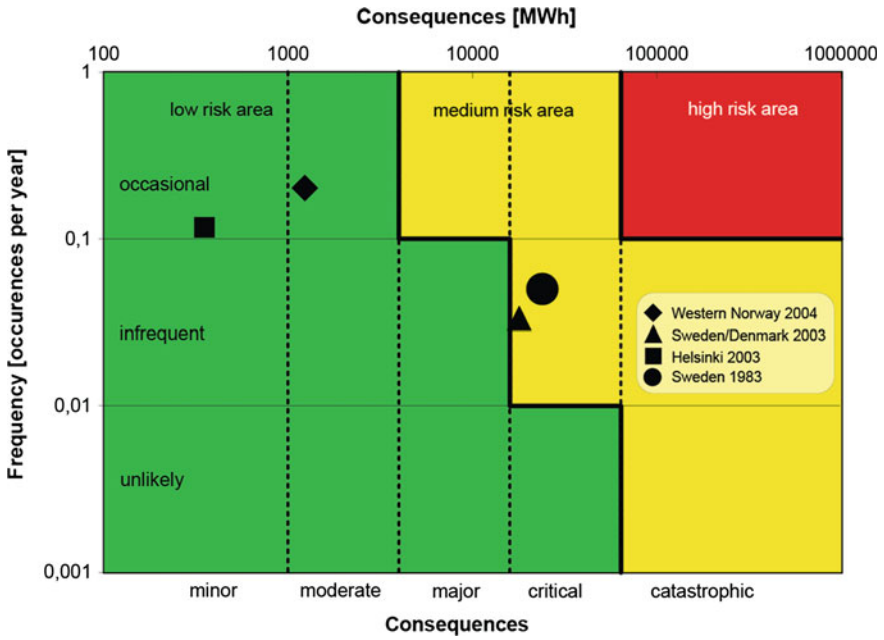

Fig. 7.2 Risk matrix based on [1]

consequence and risk matrices in Chaps. 2 and 3 with the *y*-axis representing the affected area and frequency inverted.

The electricity system is an extremely complex and comprehensive infrastructure. The number of system states increases exponentially by 2^n for a system of *n* components that typically are assumed to be in one of two possible states ("up" or "down"). For a real system, the number of system states will "explode", and it is a demanding task to analyse all possible system states. Due to a variety of reliability and risk influencing factors, as well as the complexity and size of the problem, there is no single methodology suitable for an all-encompassing risk and vulnerability analysis of electricity supply. Such analyses are usually carried out by combining different qualitative and quantitative methods. In this chapter, it is chosen to describe a quantitative analytical method denoted the contingency enumeration approach *for example*, [3]. This approach may be supported by fault tree analysis (FTA) and event tree analysis (ETA), as well as expert judgments and various other qualitative methods in a risk analysis framework.

The basic structure of the contingency enumeration approach is depicted in Fig. 7.3. Instead of enumerating all possible system states, this approach puts the critical contingencies into focus. A contingency is an undesired event composed by outages of one or more components in the electricity system due to failures, which may have technical, human or nature related causes. The critical contingencies are those potentially leading to electricity interruptions.

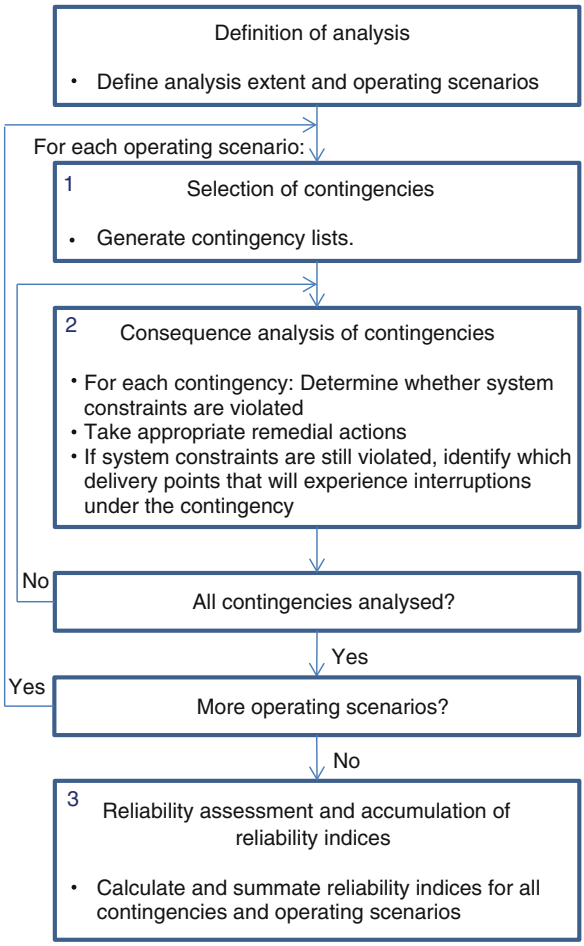

Fig. 7.3 Basic structure of the contingency enumeration approach, based on [3, 4]

The contingency enumeration approach comprises three main steps (as indicated in the figure):

1. Selection of contingencies
2. Consequence analysis of contingencies
3. Reliability assessment and accumulation of reliability indices.

The first two steps constitute the contingency analysis where the major challenge is to identify those contingencies causing system problems, *that is*, violating system operating constraints related for instance to voltage limits and thermal overload, and determine the consequences in terms of electricity interruptions to DPs. These results are combined with reliability models and data in the reliability assessment to calculate and accumulate the reliability (or risk) indices.

As indicated in Fig. 7.3, the analysis starts with defining the extent of the analysis, t*hat is*, defining which area, part of the network and DPs to study and the

depth of contingencies (single- , double- , higher-order combinations of outages, etc.) to be analysed. It should also be defined for which operating scenarios the analysis should be performed.

The contingency analysis followed by the reliability assessment according to Fig. 7.3 gives as result the consequences (or severity) and frequencies of electricity supply interruptions. This information is the basis for further evaluation of the risk of electricity interruptions and measures to reduce the risk. The contingency analysis and reliability assessment are described more in detail in the following sections.

7.3 Contingency Analysis

As shown in Fig. 7.3, the contingency analysis comprises selection and consequence analysis of contingencies. The aim is to identify the various contingencies that may lead to the event "loss of electricity supply to a DP". The analysis starts with an operating scenario (see Fig. 7.3) based on a network model with input data from a specific electricity generation and load scenario for each node in the network. The generation and loads typically vary significantly during the year. Often, the "worst case"; the heavy (peak) load situation only, is applied in these kinds of analyses. The contingency analysis should ideally be carried out for a set of operating scenarios regarded to be representative for a year.

In the first step of the contingency analysis, the objective is to reduce the number of contingencies for detailed analysis. The goal is to determine the set of contingencies that will cause violation of system operating constraints (overload and voltage limits) potentially leading to electricity supply interruptions. Since the electricity system on the national and regional transmission levels is designed to withstand the loss of a single major component (N-1 criterion), it is usually necessary to select contingencies of higher order to identify contingencies potentially leading to electricity interruptions. The total number of contingencies selected for the detailed studies may be based on some kind of cut-off criteria, *for example*, according to the probability or frequency of the contingencies [3]. The number can also be reduced by using screening or ranking techniques, for example, see [4]. A typical analysis depth is to include all first- and second order independent outages, and dependent outages such as common cause, transformer station originated outages or other specified outages. The probabilities of multiple independent outages may be very small, whereas dependent outages may have significantly higher probabilities. As mentioned above, it might be necessary to analyse higher-order contingencies to reveal the high impact events. On the other hand, increasing the analysis depth means that a large number of contingencies need to be further analysed in detail running power flow analyses. These analyses can be very time consuming. The choice of analysis depth is thus a trade-off between the accuracy needed to identify critical contingencies and the computational burden. Chapters 5 and 6 describe techniques that can be utilized to identify important higher-order contingencies.

In the second step of the contingency analysis, the objective is to identify which DPs in the electricity system under study that will experience interruptions (or reduced supply). The selected contingencies are analysed to determine whether the contingency leads to violation of any system limits related to overloading of lines or transformers, too high or low voltage in some parts of the network or network separation. This analysis of electrical consequences is based on simulations of contingencies in the electricity system using physical power flow models, as described in, *for example*, [3, 4].

If the system is outside its operating limits for a specific contingency, there might be possibilities for taking some automatic or manual corrective (remedial) actions to bring the system back within its limits. These actions can be related to, for example, electricity generation rescheduling, network reconfiguration, transformer tap adjustment or automatic disconnection of specific generators or curtailable loads with low priority. If the corrective actions are not sufficient for bringing the system back within its limits, load shedding is necessary resulting in partial or total interruption for some DPs. The computer programs used for contingency analysis try to mimic operation of the electricity system by representing remedial actions in the power flow analysis. In some programs, optimal power flow (OPF) is used. With OPF, the load shedding is minimized based, for instance, on the interruption cost which is an indicator of type and importance of different loads.

The results of the consequence analysis of a given contingency, under the specified operating conditions, show which DPs that will experience interruptions due to the contingency. For each affected DP, it is determined how much of the load in the DP that can be served. This is described in [4]. In principle, an interruption (partial or total) can be defined as when the total available capacity after occurrence of the given contingency is unable to match the load:

$$P > \text{SAC} + \text{LG} \tag{7.1}$$

where P is the load in the DP, SAC is the system available capacity to serve the load after the given contingency, and LG represents the local generation at the DP if available.

The main results from the contingency analysis are lists of DPs that will be interrupted by the analysed contingencies as well as the corresponding system available capacities for the different operating scenarios. These results are input to the reliability analysis.

7.4 Reliability Analysis

The objective of the reliability analysis is to determine the reliability of supply for the system and DPs under study. This is the third and final step of the total analysis (see Fig. 7.3) comprising the reliability assessment for DPs and the accumulation of various electricity supply interruption measures. These measures are termed reliability indices. The method combining contingency and reliability analysis is

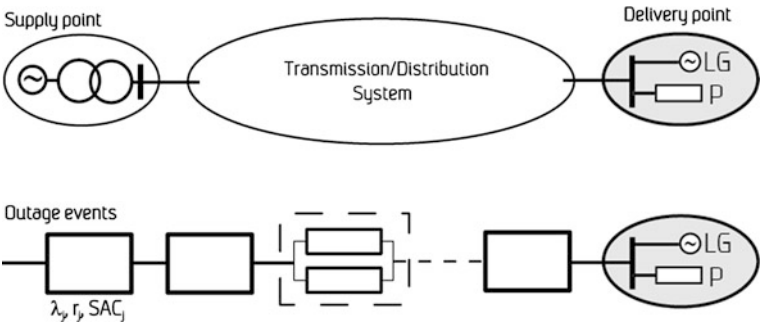

Fig. 7.4 Reliability model for a general delivery point, based on [4]

described in [4]. The reliability analysis requires a reliability model describing electricity supply interruptions to DPs.

The reliability model for a general DP is shown in Fig. 7.4. The upper part of the figure gives a simplified picture of the electricity system supplying the DP while the lower part shows the reliability model as a minimal cut set structure.

This model takes the critical contingencies for a DP as a starting point. Critical contingencies are those found in the contingency analysis to cause interruptions in the DP. All combinations of contingencies (outage events) that will lead to DP interruptions according to Eq. 7.1 can be viewed as the minimal cut sets for a particular DP. The minimal cut sets are described by the blocks in the lower part of Fig. 7.4. A minimal cut set may represent a single component failure or a multiple independent or dependent event. The parallel components and dotted lines in the Figure illustrate a double contingency. Each minimal cut set (block) is represented by an equivalent failure rate (λ_j), outage time (r_j) and the available capacity (SAC_j) to supply the load (P) after the occurrence of contingency j.

The equivalent failure rates (λ_j) and outage times (r_j) are determined from the failure rates and outage times for the individual components based on their failure and restoration processes. For a minimal cut set consisting of an independent overlapping failure of two components, these are considered as two components in parallel while there are separate models for common cause and other dependent failures, *for example*, see [4]. The equivalent failure rate and outage time for an independent failure of two components can be determined as follows:

The number of failures per year for the parallel of component 1 and 2:

$$\lambda_{1\text{ and }2} = \frac{\lambda_1 \lambda_2 (r_1 + r_2)}{8,760 + \lambda_1 r_1 \ + \ \lambda_2 r_2} (\text{failures/year}) \tag{7.2}$$

The equivalent outage time for the parallel of component 1 and 2, in hours per failure:

$$r_{1\text{ and }2} = \frac{r_1 r_2}{r_1 \ + \ r_2} (\text{hours/failure}) \tag{7.3}$$

If we are able to determine the most important minimal cut sets and the corresponding available capacity SAC, we are able to assess the reliability of supply for the DP. The reliability indices for each DP are thus determined based on the series structure of the minimal cut sets, and the indices are accumulated by the summation of contributions from the critical contingencies, using the principles for series systems as outlined in [5]. The basic reliability indices are expected frequency of interruptions and interruption duration:

$$\lambda = \sum_{j=1}^{J} \lambda_j \,(\text{number of interruptions/year}) \tag{7.4}$$

$$U = \sum_{j=1}^{J} \lambda_j r_j \,(\text{hours/year}) \tag{7.5}$$

$$r = \frac{\sum_{j=1}^{J} \lambda_j r_j}{\sum_{j=1}^{J} \lambda_j} \,(\text{hours/interruption}) \tag{7.6}$$

where j = number of minimal cut sets, λ = number of interruptions per year, U = annual interruption duration (unavailability) and r = average interruption duration.

Usually, these indices are calculated on an annual basis for all DPs for a given operating scenario. It is recommended to perform the contingency and reliability analysis for a set of operating scenarios regarded as representative for a year. When more than one scenario is used the reliability indices for the different scenarios are weighted together by their individual portions of the year.

In addition to the basic reliability indices represented by Eqs. 7.4–7.6, it is possible to calculate the severity of the contingencies, *that is*, expected consequences for the DPs, in terms of interrupted power (P_{interr}), ENS and IC based on information about the load. This is shown in the following for each minimal cut j for a given DP and a given operating scenario:

$$P_{\text{interr},\,j} \;=\; P - \text{SAC}_j - \text{LG}\,(\text{MW/interruption}) \tag{7.7}$$

$$\text{ENS}_j \;= r_j\, P_{\text{interr},\,j}\,(\text{MWh/interruption}) \tag{7.8}$$

$$\text{IC}_j = c(r_j)\text{ENS}_j \;= c(r_j) r_j\, P_{\text{interr},\,j}\,(\text{Euro/interruption}) \tag{7.9}$$

Where $c(r_j)$ is the specific cost of interruptions in Euro/MWh.

These indices for a given operating scenario are determined on an annual basis (per annum a) as follows:

$$P_{\text{interr},\,j,\,a} \;=\; \lambda_j P_{\text{interr},j}\,(\text{MW/year}) \tag{7.10}$$

$$\text{ENS}_{j,\,a} = \;\lambda_j \text{ENS}_j \;= \lambda_j r_j P_{\text{interr},\,j}\,(\text{MWh/year}) \tag{7.11}$$

$$\text{IC}_{j,\,a} \;=\; c(r_j)\lambda_j \text{ENS}_j = \lambda_j r_j c(r_j)\; P_{\text{interr},\,j}\,(\text{Euro/year}) \tag{7.12}$$

Equations 7.10–7.12 give the contribution from the minimal cut set j to the expected consequences in the DP. The total interrupted power, ENS and IC for the DP are found by the summation of the contributions from each cut set (similar to Eqs. 7.4–7.6).

The contingency analysis described in the previous section gives answers to what can go wrong in the electricity supply to the DPs, and if it happens; what are the consequences in terms of interrupted power (load). The reliability analysis, on the other hand, provides information about the frequency and duration of events. Thus, the DP indices presented in Eqs. 7.4–7.6 can be regarded as risk indices or risk measures.

To derive these risk measures, the contingency and reliability analysis require various types of data about the electricity system under study, network (electrical) topology, components, loads and end-users, component reliability data from failure statistics, operating procedures, reserve supply possibilities, and so on.

The contingency enumeration approach, combining contingency and reliability analysis, can be used to derive annual indices as described above, including all critical contingencies for a set of operating scenarios regarded to be representative for the year. As such, this methodology is suitable for long term planning and operation planning of the electricity system. The approach can also be used for assessing consequences and risk related to a specific undesired event (contingency) in a given operating scenario which results are input to the consequence and risk diagrams in Figs. 7.1 and 7.2, respectively. These types of applications are described in Chap. 8 in relation to case studies.

7.5 Interdependent Failures and Time Dependencies

The reliability indices (calculated based on the contingency enumeration approach as described in the previous section) are in practice influenced by a range of factors: the reliability models and network solution (power flow) techniques used, the load shedding philosophies, the contingency depth and how the corrective (or remedial) actions are represented. In addition there are various dependencies in the electricity system itself to take into account. In some parts of the electricity system there are geographical interdependencies, for instance two power lines on the same tower or in the same right-of-way, or cables in the same culvert. Such combinations of components or parts of the system are exposed to common cause failures (cf. Chap. 2). There are also functional interdependencies related to the protection and control systems (ICT). The main function of the protection and control systems is to mitigate the consequences of the failures (*i.e.*, to clear the fault by disconnecting the faulty part) in the electricity system to ensure personal safety and to protect the components against damage. Sometimes the protection system fails to respond as required, reacts spuriously or causes non-selectivity between protection devices in the fault clearance. An approach for how to include protection system failures in the reliability assessment is described in [4].

Human factors may contribute to cascading events, *e.g.*, situational unawareness or inadequate behaviour of operators. Human factors are usually not incorporated in the quantitative risk analysis methodology for power systems and additional qualitative methods are necessary to analyse the impact. Unfortunate circumstances, such as generators or lines being out due to maintenance can be dealt with when defining the operating scenarios for the analysis.

The dependencies and conditions described here may increase the probability of a system entering an emergency or blackout state and should be included in the risk analysis of electricity supply. Furthermore, there are time dependencies to be considered. The load varies by time of year, day of week and time of day. So does the failure frequency for some of the main components. For instance are overhead lines exposed to weather and seasonal effects, while underground cables are exposed to digging particularly on work days. Time dependencies might have a significant influence on the risk of electricity interruptions, see for instance [6].

Different failure types and dependencies mentioned in this section are modelled separately in the reliability analysis using more advanced models and methods. How various dependencies can be included in the analysis is described in, *e.g.*, [4]. The assumptions, reliability aspects included and representation of failure modes and solution techniques may differ between the available computer tools for contingency and reliability analysis. Thus, the results of two different tools based on the contingency enumeration approach will give more or less different results. The user of a tool for reliability assessment of the electricity system should be aware of these aspects when the results are evaluated.

7.6 An Example: The Reliability Test System

As an example, the contingency enumeration approach is used for the well-known Roy Billinton Test System (RBTS), see [7], shown in Fig. 7.5. The RBTS, which was developed for educational purposes, is frequently used to examine new techniques and methods. It is a six-bus electricity system consisting of 9 transmission overhead lines and 11 generators. The annual peak load is 185 MW and the voltage level is 230 kV. The individual loads are given in the Figure, while line lengths and reliability data are given in Table 7.1.

The contingency and reliability analysis is performed using the methodology described in [4] implemented in a prototype tool in Matlab. This tool performs reliability analysis for calculation of reliability indices for DPs and for the system as a whole using MATPOWER for power flow analysis in the consequence assessment of contingencies. The tool utilizes OPF to decide the amount of disconnected load. The contingencies selected for further power flow analyses include line outages up to third-order and generator outages up to fourth order, as well as third-order combinations of line and generator outages. Common cause or other dependencies in the electricity system are not included in the analysis. The results are shown in Table 7.2 for DP (bus) no 3 and 6. The reliability indices for the other

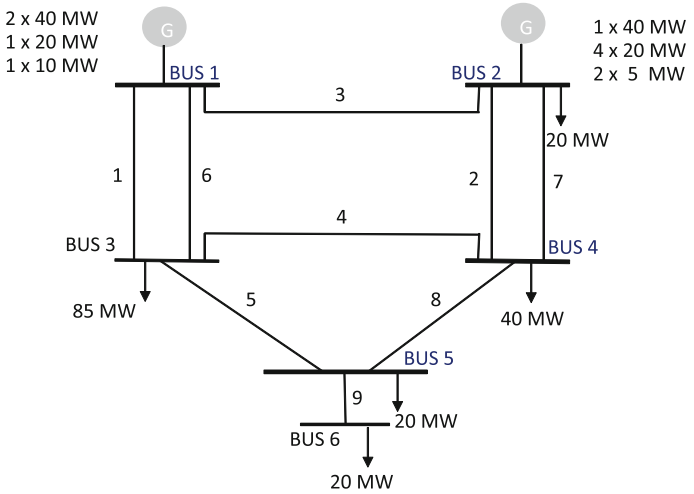

Fig. 7.5 Roy billinton test system (RBTS) based on [7]

Table 7.1 Transmission line length and reliability data

Line	From bus[a] no	To bus no	Length (km)	Failure rate (per year)	Outage duration (h)
1	1	3	75	1.5	10
2	2	4	250	5.0	10
3	1	2	200	4.0	10
4	3	4	50	1.0	10
5	3	5	50	1.0	10
6	1	3	75	1.5	10
7	2	4	250	5.0	10
8	4	5	50	1.0	10
9	5	6	50	1.0	10

[a] BUS = delivery point

Table 7.2 Reliability indices (annualized) for delivery point 3 and 6 in the RBTS system

Reliability or risk index	Delivery point (bus) no 3	Delivery point (bus) no 6
No of interruptions per year λ	6.9	1.0
Annual interruption duration U (h/year)	123.4	10.0
Average interruption duration r (h/interruption)	17.9	10.0
Interrupted power P_{interr} (MW/year)	50.6	20.1
Energy not supplied ENS (MWh/year)	1,183.6	200.3
Interruption cost IC (1,000 USD/year)	5,545.6	1,088.4

DPs are negligible compared to these two. Note that the indices are annualized as the analysis is performed for the peak load situation only.

Delivery point 3 is expected to experience almost 7 interruptions per year. This number is influenced by outage of either line 1 or line 6 causing overload on the other line due to low voltage, as well as combinations of outages of lines or generators. The expected number of interruptions for DP 6 is equal to 1.0 dominated by the single outage of line no 9. The IC for DP 3 sums up to about 5.5 million USD per year. This DP serves large industrial users and some commercial services, while DP 6 serves an industrial farm.

Case studies are provided in Chap. 8 to demonstrate the approach described in this chapter.

7.7 Conclusions

This chapter has described an approach to quantitative risk analysis of electricity supply which can be used in a detailed analysis for instance as input to cascade diagrams (cf. Chap. 4) in the risk analysis of cascading failures and interdependencies with other infrastructures. The risk analysis approach is based on the analytical contingency enumeration approach which consists of three main steps combining contingency and reliability analysis. The results are presented as reliability indices describing risk of electricity interruptions for different DPs in the electricity system serving for instance societal critical functions or other infrastructures.

The contingency and reliability analysis need input data of network (electrical) topology and power flow models, in addition to component reliability data, DP data and so on. This risk analysis approach requires a rather profound knowledge of the electricity system, detailed computer models and specialized computer tools.

The contingency enumeration approach combining contingency and reliability analysis can be used to derive annual indices suitable for planning purposes or it can be used to assess the consequences and risk related to a specific undesired event (contingency) in the electricity system.

The models and methods for risk analysis of electricity supply are utilized in some case studies demonstrating the use of the risk analysis approach. The case studies are described in Chap. 8 comprising a study of two DPs in the main grid both supplying major industrial sites, a study of the loss of supply to Oslo central Station (cf. Chap. 4) in the distribution grid as well as a risk and vulnerability analysis including extraordinary events.

References

1. Doorman, G., Uhlen, K., Kjølle, G.H., Huse, E.S. (2006). Vulnerability analysis of the Nordic power system. *IEEE Transactions on Power Systems*, *21*(1).
2. NordSecurEl (2009). Risk and vulnerability assessments for contingency planning and training in the Nordic electricity system. Final report, statens energimyndighet, EU EPCIP, Eskilstuna March 2009.
3. Billinton, R. (1989). Composite system adequacy assessment—the contingency enumeration approach. IEEE Tutorial Course Reliability assessment of composite generation and transmission systems, course text 90EH0311-1-PWR, paper no 5.
4. Samdal, K., Kjølle, G.H., Gjerde, O., Heggset, J., Holen, A.T. (2006). Requirement specification for reliability analysis in meshed power networks. Report TR A6429 SINTEF Energy Research, Trondheim December 2006.
5. Billinton, R., & Allan, R. N. (1992). *Reliability evaluation of engineering systems. Concepts and techniques* (2nd ed.). New York: Plenum Press.
6. Kjølle, G. H., & Holen, A. T. (1998). Reliability and interruption cost prediction using time dependent failure rates and interruption costs. *Quality and Reliability Engineering International Journal, 14*, 159–165.
7. Billinton, R., Kumar, S., Chowdhury, N., Chu, K., Debnath, K., Goel, L., Khan, E., Kos, P., Nourbakhsh, G., Oteng-Adjei, J. (1989). A reliability test system for educational purposes—basic data. *IEEE Transactions on Power Systems*, *4*(3).

Chapter 8
Risk of Electricity Supply Interruptions

Oddbjørn Gjerde and Gerd Kjølle

Abstract This chapter presents three case studies using the models and methods for risk analysis of electricity supply described in Chap. 7, as well as the basic concepts and interdependency modelling of Chaps. 2 and 4. The case studies comprise analyses of the reliability of supply for delivery points in the transmission and distribution grid, and a risk and vulnerability analysis including extraordinary events in the electricity system.

8.1 Introduction

The electricity system consists of power plants for electricity generation, delivery points serving loads and power grids connecting the power plants and loads. The power grids consist of overhead lines and underground cables and can be divided into the national transmission grid (or main grid), regional grids and local medium-voltage and low-voltage distribution grids . Grids at different levels are connected by transformer stations. The power plants are mainly connected to the main transmission grid and regional grid levels.

The case studies presented in this chapter comprise (1) a study of the reliability of supply for two delivery points in the transmission grid supplying major industrial sites, (2) a study of the loss of supply to Oslo Central Station which is located in the distribution grid and (3) a risk and vulnerability analysis including extraordinary events.

O. Gjerde (✉) · G. Kjølle
SINTEF Energy Research, Trondheim, Norway
e-mail: Oddbjorn.Gjerde@sintef.no

P. Hokstad et al. (eds.), *Risk and Interdependencies in Critical Infrastructures*, Springer Series in Reliability Engineering, DOI: 10.1007/978-1-4471-4661-2_8,

8.2 Case 1: Reliability of Delivery Points in the Transmission Grid

In this case study, as described in [1], the reliability of supply is analysed for two different delivery points in the 420 kV Norwegian transmission grid: both supplying major industrial sites. One point is situated more or less in the centre of the transmission grid and the other at the end of a line with single-sided supply.

The methods for risk analysis of electricity supply described in Chap. 7 are integrated with market models for the selection of operating scenarios as input to the contingency analysis. This is depicted in Fig. 8.1 where the contingency analysis and reliability analysis are marked with a dotted line in the middle of the Figure.

Since the electricity generation and loads vary during the year, the contingency analysis should ideally be carried out for a set of operating scenarios regarded to be representative for a year (*cf*. Chap. 7). The reliability-constrained power market analysis in the upper part of the Figure represents the part where the power market solutions are combined to produce a set of operating scenarios. An operating scenario is defined as a system state valid for a period of time, characterized by load and generation composition including the electrical topological state (breaker positions etc.) and import/export to neighbouring areas.

The combination of contingency analysis and reliability analysis in Fig. 8.1 represents the contingency enumeration approach for composite generation and transmission system reliability analysis. A contingency is here defined as an event composed by outages of one or more components due to failures, which may have technical-, human- or nature-related causes. As explained in Sect. 7.2, the contingency enumeration approach comprises three main steps:

1. Selection of contingencies
2. Consequence analysis of contingencies
3. Reliability assessment and accumulation of reliability indices.

The two first steps are combined in the contingency analysis depicted in Fig. 8.1, and the third step is achieved by adding reliability information in the reliability analysis (Fig. 8.1).

The studied delivery points L1 (centrally located) and L2 (with single-sided supply) are situated in the middle of Norway, represented by area “10” in the power market model shown in Fig. 8.2. This Figure only shows the areas and the connections between areas included in the market model which gives the operating scenarios used as input to the contingency and reliability analyses. For this purpose, detailed information about the network and components is needed. This is restricted information, and the physical lines within the different areas are not shown.

The Norwegian electricity system is dominated by hydro power generation (about 95 %). Total annual electricity consumption in Norway is about 125 TWh, the maximum electricity generation about 140 TWh and the maximum load

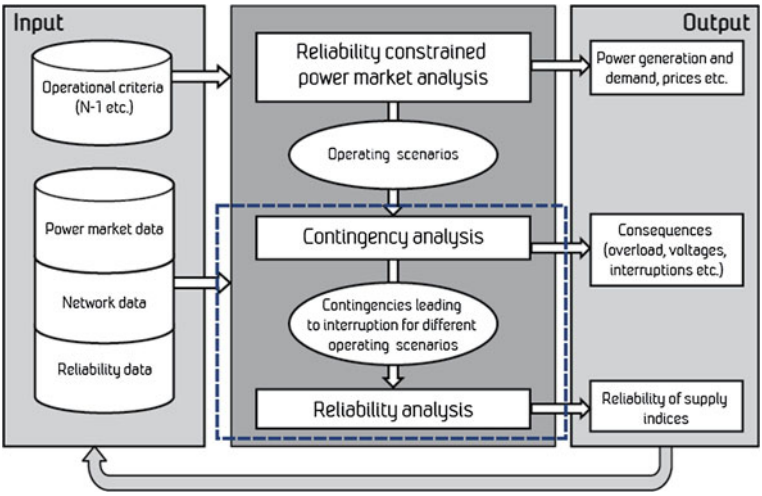

Fig. 8.1 Framework of integrated methodology for reliability of supply analysis based on [1]

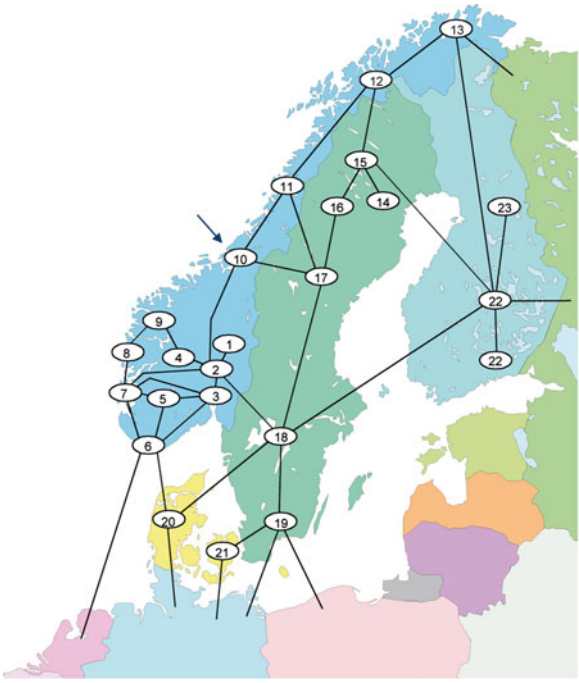

Fig. 8.2 Power market model and division of areas (from SINTEF energy research)

approximately 24,000 MW. The generation and loads may vary significantly throughout the year. For simplicity, the system in the middle of Norway has been analysed using three different operating scenarios from the market model to represent the year; these were the weeks 4, 16 and 30. Week 4 represents a heavy

load situation, week 16 represents a still quite heavy load situation (but less than week 4) and hydro reservoirs running out of water, while week 30 represents light load. Power flow and market models for the year 2010 have been used as a basis with constant loads of 650 MW in L1 and 220 MW in L2.

8.2.1 Power Market Simulations

The first analysis step was to initialize the three operating scenarios through interaction between the market model and the power flow model in a reliability-constrained power market analysis. In the estimation of transmission capacities to the neighbouring areas, the system constraints related to voltages and loading of lines must be taken into account. In this case, the voltage level turned out to be the limiting factor. The market model was updated with the transmission capacities in the different operating scenarios.

8.2.2 Contingency Analysis

In this case, the Siemens TPLAN tool[1] was used for screening of the system providing a list of single contingencies to be analysed. Double contingencies (outages of two components) were defined manually.

A total of 330 single and 46 double contingencies were analysed. For each of the 376 contingencies, the system consequence was found. This implied to decide whether or not the contingency would lead to interruption of electricity supply for the studied delivery points. Voltages and loads were checked, and it was revealed whether or not the system was within its defined operating limits. The consequence analysis led to lists of contingencies causing interruptions for delivery points L1 and L2 in the different operating scenarios represented by weeks 4, 16 and 30. The interruptions were due to network separation, overload or voltage deviations. No blackout situations (*i.e.* interruption for the entire system) were revealed for the chosen operating scenarios.

8.2.3 Reliability Analysis

The last step was to calculate the reliability of supply indices. A number of 4–6 minimal cuts (as defined in Chap. 7) were identified for both L1 and L2, depending

[1] PSS®E Siemens TPLAN-module http://www.energy.siemens.com/us/en/services/power-transmission-distribution/power-technologies-international/software-solutions/pss-e.htm.

Table 8.1 Reliability analysis input data, component failures [source Statnett (Norwegian TSO)]

Component	Voltage (kV)	Failure rate (1/year)	MTBF[a] (years)	Average outage time[b] (h)
Overhead line (1 km)	420	0.0104	96.2	2.2
Bus bar		0.0118	84.7	0.25
Power transformer		0.0645	15.5	360
Circuit breaker		0.0035	285.7	0.25
Distance protection		0.0543	18.4	0.25
Overhead line (1 km)	300	0.0088	113.6	5.9
Bus bar		0.0146	68.5	0.25
Power transformer		0.0283	35.3	430
Circuit breaker		0.0035	256.4	0.25
Distance protection		0.0549	18.2	0.25
Overhead line (1 km)	132	0.0118	84.7	6.9
Bus bar		0.0044	227.3	0.25
Power transformer		0.0106	94.3	245
Circuit breaker		0.0019	526.3	0.25
Distance protection		0.0231	43.3	0.25

[a] Mean time between failure
[b] Expected reconnection time is used for bus bar, circuit breaker and protection

on the operating scenario. Only, first- and second-order cuts (*i.e.* single and double outages) were taken into account. Inputs to the reliability analysis were information about the protection configuration, failure statistics and specific interruption costs. The main reliability input data are listed in Tables 8.1 and 8.2. For each delivery point and operating scenario, interruption frequency and duration were calculated by summing up the contributions from the different minimal cut sets. The indices were then weighted according to the probability of the different operating scenarios to obtain annual indices. The results are listed in Table 8.3.

This example shows that the expected number of interruptions is much higher for delivery point L2 compared with L1. This is as expected since L2 has single-sided supply, and the single outages are decisive for the reliability of supply indices. The expected mean time between interruptions is more than 30 years for L1, while L2 will experience an interruption more than once per year on average, resulting in an interruption cost of about 4.3 million euro per year. For L1, only double outages contribute. These are dependent outages, mainly arising from the dependencies related to the protection system of missing and undesired operation of the breakers (see Sect. 7.5).

The reliability indices neglecting any dependencies related to the protection system are shown in Table 8.4. A comparison between the tables shows that protection system dependencies only have a relatively small influence on L2, while the reliability of supply would have been practically 100 % for L1 if protection had not been taken into consideration since only second- or higher-order independent outages contribute.

Table 8.2 Reliability analysis input data, dependent protection failures (source Statnett)

Component	Voltage [kV]	Missing operation p(missing)[a]	Undesired operation p(undesired)[b]
Distance protection	420/300	0.0009	0.01412
Circuit breaker	420/300		–

[a] Probability of missing operation of circuit breaker
[b] Probability of undesired operation of circuit breaker

Table 8.3 Reliability of supply indices for the 420 kV delivery points

	λ [No. of interruptions per year]	U [Annual interruption duration (hrs/year)]	ENS [Energy not supplied (MWh/year)]	IC [Cost of energy not supplied (€/year)] (approx.)
L1 (650 MW)	0.03	0.007	4.78	8,000
L2 (220 MW)	1.36	2.37	521	4.30 million

Table 8.4 Reliability of supply indices neglecting protection system dependencies

	λ [No. of interruptions per year]	U [Annual interruption duration (hrs/year)]	ENS [Energy not supplied (MWh/year)]	IC [Cost of energy not supplied (€/year)] (approx.)
L1 (650 MW)	0	0	0	0
L2 (220 MW)	1.34	2.36	520	4.29 million

8.3 Case 2: Loss of Electricity Supply to Oslo Central Station

This case study uses the event at Oslo Central Station (Oslo S) in 2007 ("the culvert case" in Chap. 4) as a starting point. The event started as a minor fire in an 11 kV cable in the distribution network, caused by digging in the area around the central station. The fire led to the evacuation of the station. Several communication systems were interrupted, including train operation services, Internet and phone services. It took 16 h before the electricity supply was restored and another 4–5 h before the central station was reopened for the public and the train traffic resumed. The consequences for the society were thus severe, even if the interrupted power was rather limited. The case is also described in [2] and is a result from a study of serious events in several infrastructures in Oslo, covering events of technical character, malicious acts, as well as natural hazards. The study was in principle carried out according to the steps described in Chap. 4, mainly focusing on the detailed quantitative analysis.

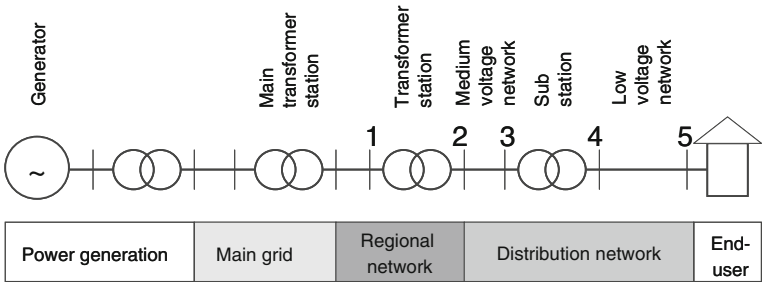

Fig. 8.3 Stylized overview of the power system (value chain) from power generation to demand (*Source* Hafslund Nett)

8.3.1 Loss of Electricity Supply and Hazardous Events

Figure 8.3 gives a stylized overview of the electricity system in Oslo. The voltage level of the main grid supplying Oslo is 300 kV, while there are three voltage levels in the regional network in the city: 132, 47 and 33 kV. These are mostly underground cable networks, but there are also overhead lines. The distribution network mainly consists of 11 kV underground cables.

According to the network company's interruption statistics for the period 2001–2007, the end-users of Hafslund Nett (the network company) will experience an interruption on average every second year (0.5 per year) with an expected duration of 18 min per interruption, *that is,* 9 min per year, due to failures in the regional network (down to level 2 in Fig. 8.3). Including failures in the distribution network (level 3 and 4 in Fig. 8.3), the number of interruptions increases to 0.8 per year with an expected annual duration of 40 min per year. Thus, the regional network contributes to about 60 % of the frequency of interruptions and stands for about 23 % of the total interruption duration.

In the same period, there have been three major events in the electricity system in Oslo affecting larger parts of the city. Two of these events (in 2005 and 2007) involved multiple failures and cascading events in the main grid (300 kV), causing loss of one or more main transformer stations and interruption to a major portion of the electricity end-users. Both these events lasted for less than one hour. The third event is the Oslo S event as mentioned above. All three undesired (hazardous) events are plotted in the consequence diagram in Fig. 8.4.

Figure 8.4 shows that the two 300 kV events (in the main grid, Fig. 8.3) were large in terms of disconnected load, but caused relatively short interruption duration and thus limited consequences for dependent infrastructures. The event at Oslo S caused low disconnected load, *that is,* interrupted power, but considerably longer duration of the loss of electricity supply to the central station. The consequence classes in Fig. 8.4 are scaled compared to Fig. 7.1 to better fit the size of the electricity system in Oslo and to provide an illustration of the criticality of events. This is not an official classification used by Hafslund Nett. In accordance

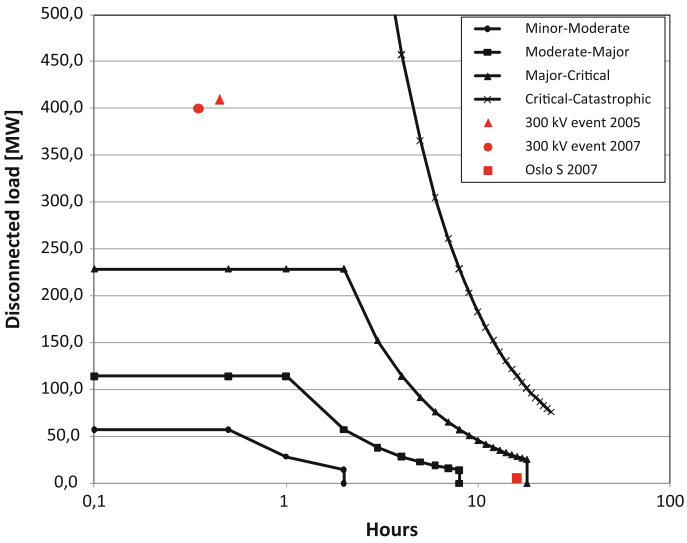

Fig. 8.4 Consequence diagram for three hazardous events in the electricity supply in Oslo

with Fig. 8.4, the three events can be considered to range from major to critical. However, the Oslo S event (11 kV distribution network) was very different from the two events in the main grid (300 kV).

The event "loss of electricity supply to Oslo Central Station (Oslo S)" at Oslo S was selected because the other infrastructures depend to a large extent on electricity supply. In a cross-sector risk analysis, it is necessary to identify interdependencies between infrastructures and consequences for these infrastructures if the electricity supply is interrupted.

8.3.2 Consequences of Hazardous Events for the Electricity Supply

Based on the risk analysis methodology described in Chap. 7, it is possible to calculate reliability indices, such as frequency and duration of electricity supply interruptions to different delivery points, the amount of interrupted load, energy not supplied (ENS) and the corresponding interruption cost (here denoted CENS), as well as area or number of electricity end-users affected. In Norway, the network companies' revenue caps are adjusted in accordance with the customers' interruption costs, CENS [3]. In this arrangement, the individual end-user consequences are represented by average cost rates per customer category [4]. CENS represents an estimate of the societal costs of electricity supply interruptions, however, only considering the end-users' costs. Consequences when loss of electricity supply results in unavailability of dependent infrastructures, public services etc. are not included in CENS.

Table 8.5 Reliability indices for 33 kV delivery points, including single line and transformer outages and common mode

Delivery point	Number of interruptions per year	Duration in hours	Energy not supplied (ENS) MWh/year
Station A	3.0	71	2,340
Station B	0.12	371	292

No reconfiguration possibilities included in the analysis

8.3.3 Consequences of Loss of Electricity Supply for Other Infrastructures

It is a challenge for network companies to have detailed knowledge about the different end-users behind each delivery point. Consequences of electricity supply interruptions to other infrastructures need to be investigated by focusing on interdependencies, involving the stakeholders responsible for the operation of the dependent infrastructures. The contingency enumeration approach was used to calculate how often an undesired event will occur (frequency of electricity supply interruptions) and the consequences in terms of interruption duration and energy not supplied. This kind of information can be useful to operators of the dependent infrastructures in their evaluations of consequences and emergency preparedness planning.

The undesired event "loss of electricity supply to Oslo Central Station (Oslo S)" may be caused by outage of transformer stations and/or power lines in the main transmission grid and regional network in Oslo (Fig. 8.3). The event is critical if it occurs in heavy load situations, usually in cold winter periods. In such situations, the reserve electricity capacity is limited. Electricity supply interruptions may also be critical to dependent infrastructures, such as railway transportation and banking services (*cf.* Step 2–identifying interdependencies in Chap. 4).

Table 8.5 shows the result from a reliability analysis for the heavy load situation for two different transformer stations in the 33 kV network in the inner parts of Oslo. This result includes common mode failures, such as cables in the same culvert or underneath a road bridge (geographical dependency).

Oslo S is supplied from Station B while Station A serves some societal critical functions, for instance a hospital. Thus, the consequences of loss of electricity supply and dependencies to other infrastructures and critical functions should be further investigated. Since the results in Table 8.5 are based on the heavy load situation only, the reliability indices are annualized, *that is*, the frequency of interruptions and energy not supplied presented in the Table are given in units per year as if the heavy load situation lasts for the whole year. One should keep in mind that the heavy load situation is regarded as the worst case, but this situation only lasts for a small portion of the year. However, for the emergency preparedness of other critical infrastructures, it is important to consider the worst case outcome of interrupted electricity supply.

In the case presented in Table 8.5, reserve connection possibilities are not considered. This is the main reason for the very large average outage duration for each of the transformer stations. The reliability data are taken from the national statistics, using the expectation (average) values including all failure causes, while there are large dispersions in outage times. For instance, it will take about 1 h for the operator to perform reconfigurations from the control centre. In practice, the network company has various possibilities for provisional restoration of supply to the delivery points, depending on local conditions. Different measures take different time. As an example, it may take 4–24 h to connect reserve supply from underlying distribution network and up to 4 days to move transformers. It is rather complicated to model and take into consideration all such possibilities and procedures in the reliability assessment and the various tools represent reconfiguration and restoration aspects to a varying degree.

Keeping in mind the assumptions and premises for the analysis described above, the results presented in Table 8.5 are not realistic for the actual electricity supply to Oslo S. The results should be regarded as examples of typical results that can be provided from the current reliability and risk assessment methodology presented in Chap. 7. This kind of information may be important when pursuing interdependencies and consequences for other critical infrastructures.

The simplified cascade diagram in Fig. 8.5 shows the possible consequences the losses of electricity supply may have for the major railway station in Oslo (Oslo S). A general loss of electricity supply will mainly cause consequences due to functional interdependencies, shown in the cascade diagram (*cf.* the semi-quantitative risk analysis in Chap. 4).

The actual consequences of this event at Oslo S in 2007 are summarized in Table 8.6, according to available information in [5].

The event at Oslo S, which started in the electricity system, caused rather limited consequences for the electricity supply in terms of disconnected load. Even if the electricity supply interruption lasted for 16 h, the CENS cost was calculated to 4.5 MNOK only. This is the cost seen by the network company. In railway transportation, a delay is often valued in the range of 3 NOK per passenger minutes lost [6]. Assuming that all the 80,000 passengers were delayed for 20 h, this results in a societal cost of passenger minutes lost of approximately 300 MNOK, which is nearly 70 times higher than the CENS cost. In addition, there are societal costs related to the loss of Internet services for 25,000 users for 10 h, as well as other direct and indirect consequences, such as increased road traffic, closed shops, etc.

The risk analysis of the electricity supply and the further investigation of interdependencies and consequences for other critical infrastructures can be used to assess the need for risk-reducing measures, for example in the electricity supply system itself or with respect to back-up solutions or redundancy in other infrastructures (*e.g.* the railway traffic centre at Oslo S in Fig. 8.5). The different cost estimates visualize the challenges in cost-benefit analysis when risk assessments only deal with one infrastructure and demonstrate the importance of a cross-sector risk analysis approach including consequences arising in dependent infrastructures.

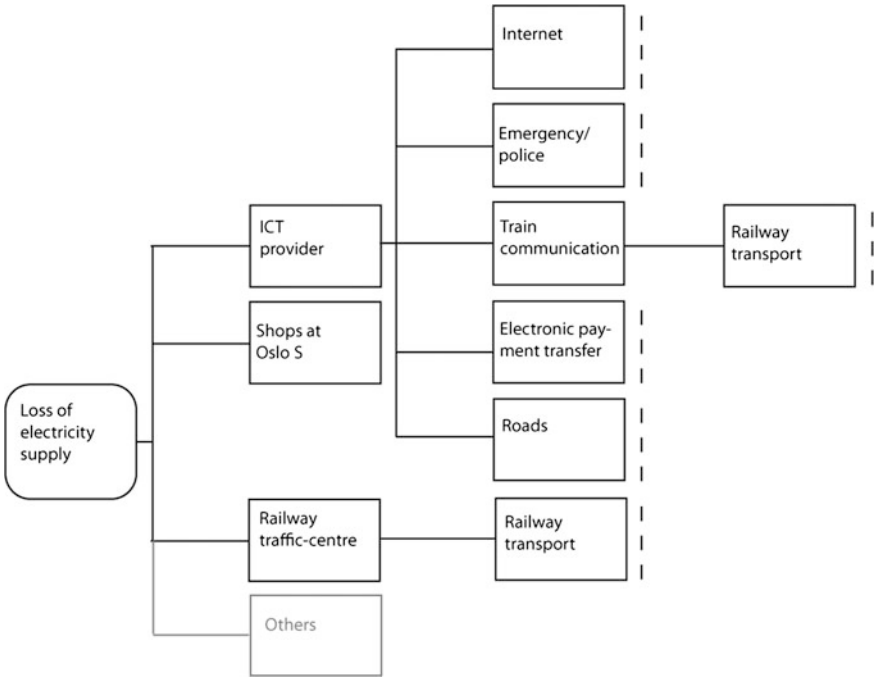

Fig. 8.5 Simplified cascade diagram for loss of electricity supply for the Oslo central station, based on [6], *cf.* Chap. 4

Table 8.6 Cross-infrastructure consequences of loss of electricity supply to Oslo central station, based on DSB [5]

Infrastructure	Consequence
Electricity supply	Loss of 5.6 MW load, interruption duration 16 h, CENS = 4.5 MNOK
Railway transport	80,000 passengers delayed for 20 h, cost ≈300 MNOK (see below)
Internet	25,000 users without services for 10 h
Traffic control centre	Loss of control centre for some (unspecified) time

8.4 Case 3: Risk and Vulnerability Analysis of Electricity Supply Including Extraordinary Events

In this case study, the risk and vulnerability of extraordinary events in a 420 kV transmission system were analysed, [7]. The studied area is connected to neighbouring areas via one AC connection and two DC connections as shown in Fig. 8.6. The physical network is not included for confidentiality reasons.

Power system failures are considered in this case study, whereas the energy and capacity balance are indirectly represented as a part of the power system operation, *that is,* the operating scenario. The analyses were carried out by combining

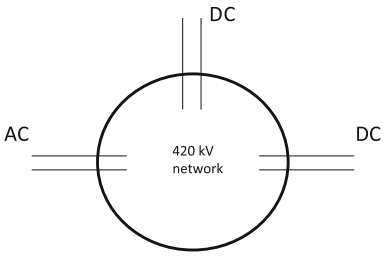

Fig. 8.6 Studied network: connection to other areas, from [7]

qualitative and quantitative techniques through the different steps described in Chap. 3 with emphasis on detailed analyses [7]:

- Identification of threats and undesired events
- Description of causes and probabilities (causal analysis)
- Classification of consequences (consequence analysis)
- Risk and vulnerability evaluation.

The bow-tie model (*cf.* Sect. 2.5) was used as a framework to describe the relations between the main causes and consequences of an undesired event [7]. An example is given in Fig. 8.7. The main undesired events to be considered here are power system failures and the consequences in terms of wide-area interruptions or blackouts . This is shown in the Figure together with major categories of hazards, including natural hazard (*e.g.* a major storm), technical/operational hazards, human errors and antagonistic causes, such as terror or sabotage.

The hazards might lead to power system failure(s) through a chain of events and a set of causes, and the failure(s) might lead to minor or severe consequences through a set of circumstances. As indicated in Fig. 8.7, a number of barriers exist to avoid hazards to develop into undesired events and to prevent or reduce the consequences. A system is more vulnerable towards the relevant hazards if the barriers are weak or malfunctioning.

In risk and vulnerability analysis of electricity systems, a major challenge is to identify chains of events that could lead to wide-area interruptions. The vulnerability approach presented in Chap. 6 is one way of dealing with this challenge. It is necessary to have knowledge about the underlying causes and to determine and evaluate the consequences of these events. The analyses are described in the following sections.

8.4.1 Identification of Threats and Undesired Events

In the case study, undesired events and corresponding hazards that might lead to the undesired events in certain operating scenarios were identified through brainstorming and interviews with personnel at the transmission system operators (TSOs) control centre and planning department, as well as by the use of power

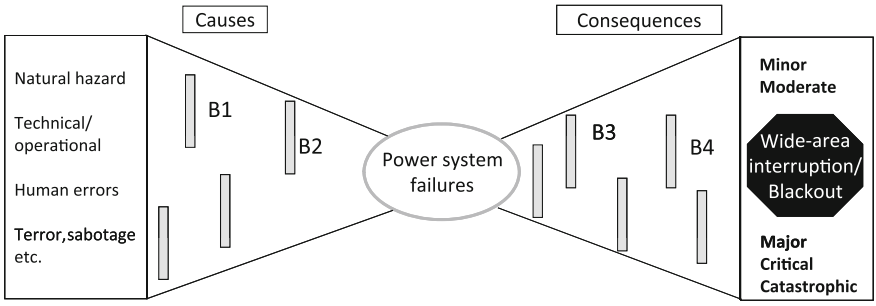

Fig. 8.7 Threats, undesired (extraordinary) event, consequences and barriers, from [7]

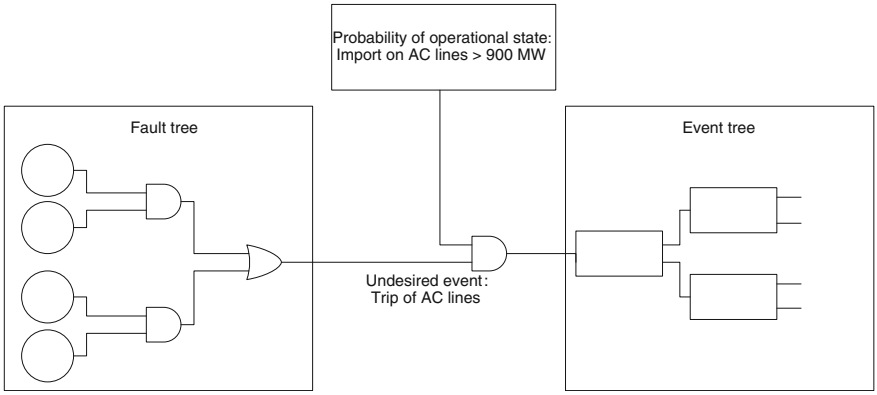

Fig. 8.8 Bow-tie model for the selected undesired event in the transmission system, based on [7]

flow simulations. For the studied area, three different *undesired events,* considered to be extraordinary, were identified. It was difficult to find potentially severe events in the system, since both long-term and operational planning follow the (N-1) criterion and ensure that all *likely* events can be dealt with. The remainder of this chapter focuses on one of the undesired events.

According to experts at the transmission system operator (TSO), it is likely that the system will not withstand any loss of the AC connection when import on the AC lines is higher than 900 MW. The undesired event is therefore defined as "loss of both AC lines if import on AC lines is >900 MW". See the corresponding bow-tie model in Fig. 8.8 using fault tree and event tree for the causal and consequence analyses, respectively (*cf.* Sect. 3.4).

The following hazards and causes, leading to loss of both AC lines, are identified through discussions with experts:

- Undesired non-selective breaker tripping
- Thunderstorm
- Sabotage

- Transportation accident
- Earth line breakage
- Galloping lines
- Station fault
- Power outage at feeding end.

These causes do not normally lead to extraordinary events individually, but combined with a critical operating scenario (>900 MW import on AC lines) and the fact that both lines are lost; the result might develop into an extraordinary event.

8.4.2 Causal Analysis

The fault tree for "loss of both AC lines" is shown in Fig. 8.9. The basic events are based on the identified hazards or causes and grouped as shown in the figure. All input data are based on combining failure statistics with expert judgment. Barriers on the "causal side" are not explicitly analysed, but taken into account in the expert evaluation when estimating the frequency of the event. The resulting frequency for the loss of both AC lines is calculated to 0.13 per year. Based on historical data, the probability of the critical operating scenario is 1.4 %. By combining this information, a frequency of the event "loss of both AC lines if import on AC lines is >900 MW" of 0.00182 per year corresponding to a return period of 550 years is derived.

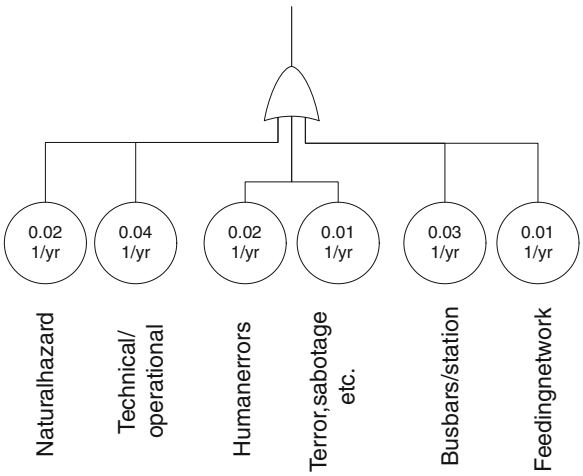

Fig. 8.9 Fault tree for the selected undesired event in the transmission system, with estimated frequencies of basic events, from [7]

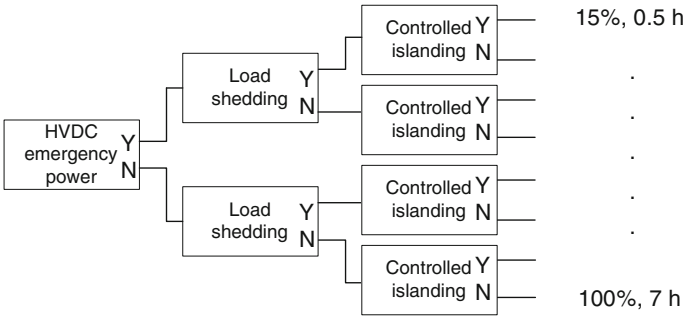

Fig. 8.10 Event tree for the selected undesired event in the transmission system, based on [7]

8.4.3 Consequence Analysis

The consequence analysis for the undesired event "loss of both AC lines if import on AC lines is >900 MW" is carried out by using the TSO experts in qualitative evaluations in combination with quantitative analyses using power flow and dynamic analyses. If there were no barriers on the event side of the bow-tie, the loss of 900 MW could not be handled by the system and a total blackout would be inevitable. Even if all barriers are successful, there will still be a partial interruption (15 % of total load). The resulting event tree is shown in Fig. 8.10 with the following barriers:

- HVDC emergency power
- Load shedding
- Controlled islanding

Both HVDC emergency power and load shedding aim at reducing the unbalance between generation and load to avoid that the frequency becomes too low, while controlled islanding is needed due to the loss of all AC connections.

The different consequences for this event are shown to the right in terms of load shedding and duration, from 15 % when all barriers are successful to blackout (100 %) when all barriers fail. The frequency of blackout is calculated to 0.0012 per year corresponding to a return period of more than 800 years.

The results from the consequence analysis are shown in the consequence diagram in Fig. 8.11 and in risk diagram in Fig. 8.12 for three undesired events. "Event 3" corresponds to the one described above.

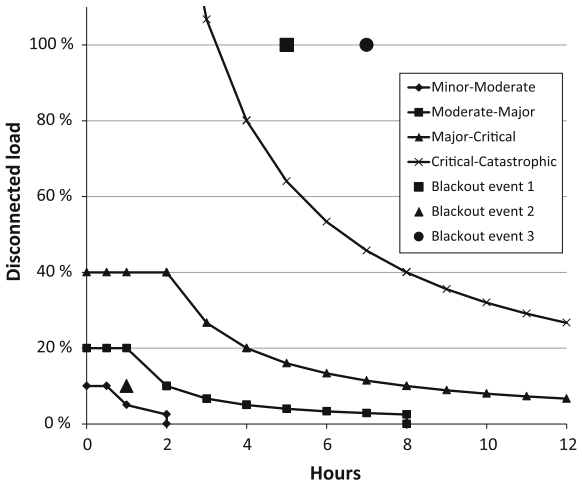

Fig. 8.11 Consequences of identified undesired events, from [7]

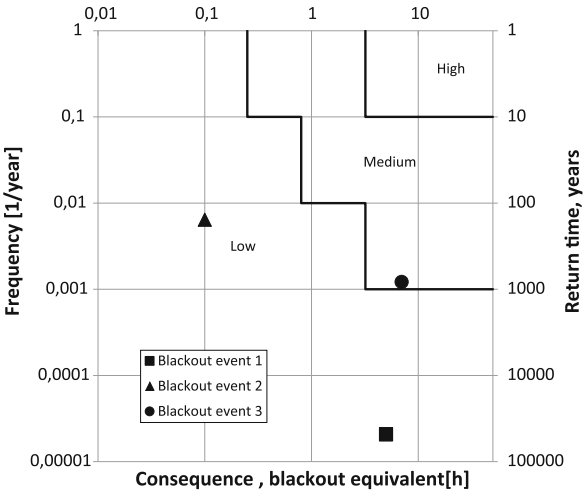

Fig. 8.12 Risk diagram of identified undesired events, from [7]

8.4.4 Risk and Vulnerability Evaluation

Two of the identified undesired events have consequences considered by the TSO to be "catastrophic", while the third is "moderate". Note that the disconnected load is given in percentage in the consequence diagram in Fig. 8.11. Due to very low expected frequency, the risk is categorized as medium or low for all three events. In the risk diagram, the consequences in Fig. 8.12 are represented by a "blackout equivalent", calculated as the equivalent number of hours with interruption of 100 % of the load.

This case study clearly illustrates the "high societal impact and low probability" nature of extraordinary events. Nevertheless, if the consequences are unacceptable, the extraordinary event must be taken into consideration, even if the risk is small.

References

1. Kjølle, G., & Gjerde, O. (2010a). Integrated approach for security of electricity supply analysis. *International Journal of Systems Assurance Engineering and Management, 1*(2), 163–169.
2. Kjølle, G., & Utne, I. B. (2010b). Critical infrastructures and risk analysis of electricity supply. In ESREL Conference proceedings. London: Taylor & Francis Group.
3. Langset, T., Trengereid, F., Samdal, K., & Heggset, J. (2001). Quality adjusted revenue caps—a model for quality of supply regulation. Proceedings of the international conference and exhibition on electricity distribution (CIRED), Amsterdam.
4. Kjølle, G., Samdal, K., Singh, B., & Kvitastein, O. (2008). Customer costs related to interruptions and voltage problems: Methodology and results. *IEEE Transactions on Power Systems, 23*(3), 1030–1038.
5. DSB. (2007). Fire in cable culvert. Oslo central station (in Norwegian: Brann i kabelkulvert. Oslo sentralstasjon). Tønsberg: Directorate for Civil Protection and Emergency Planning (DSB).
6. Utne, I. B., Hokstad, P., & Vatn, J. (2011). A method for risk modeling of interdependencies in critical infrastructures. *Reliability Engineering & System Safety, 96*, 671–678.
7. Gjerde, O., Kjølle, G. H., Detlefsen, N. K., & Brønmo, G. (2011). Risk and vulnerability analysis of power systems including extraordinary events. Proceedings of IEEE PES Trondheim Powertech.

Chapter 9
Integrated Urban Water System

Rita Ugarelli and Jon Røstum

Abstract This chapter presents the challenges faced by the water utilities to provide safe, secure and reliable service to meet the Water Framework Directives 2000/60/EC and the water safety plan (WHO [16]). These directives among others will form framing conditions for the risk and vulnerability analysis to be conducted. The analysis approach follows standard methodology for risk and vulnerability described in Chap. 3 of this book. In order to structure the analysis, it is common to split the system into the various water cycle components. For each of these components, hazards and threats are identified, probability and consequences assessed, and finally, the total risk picture presented. Practical examples from the Oslo case study are presented to support the approach.

9.1 Outline of the Method and Description of the Main Water Cycle Components

The analysis method applied for integrated urban water systems follows the general approach for risk and vulnerability analysis outlined in Chap. 3. In the step 1—*analysis preparation,* water system–specific conditions are emphasized related to management and system breakdown. In step 2—*Coarse risk analysis,* it is demonstrated how historical events may support the hazard identification process. In step 3—*Detailed analyses,* the fault tree method is used to demonstrate how a critical system like the water pumping station may be analysed. In order to get an overview of the various elements of a typical water and wastewater system,

R. Ugarelli (✉) · J. Røstum
SINTEF Building and Infrastructure, Trondheim, Norway
e-mail: rita.ugarelli@sintef.no

P. Hokstad et al. (eds.), *Risk and Interdependencies in Critical Infrastructures*, Springer Series in Reliability Engineering, DOI: 10.1007/978-1-4471-4661-2_9,

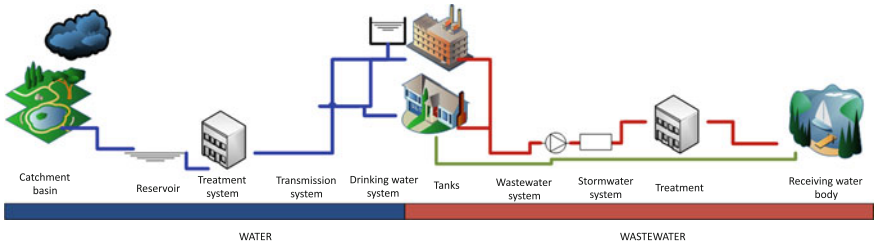

Fig. 9.1 Illustration water and wastewater systems

Fig. 9.1 illustrate the main components/elements. These elements are also often used as a basis for structuring the risk and vulnerability analysis.

The water and wastewater systems follow the urban water cycle from catchment and reservoir for water supply to recipient for the effluent from wastewater treatment plant. The following list elaborates slightly more on the various elements:

- Catchment basin—surface water catchment; groundwater catchment.
- Reservoir—surface water reservoir; groundwater reservoir including abstraction system; groundwater recharge.
- Treatment system—water treatment plant.
- Transmission system—transmission pipelines including valves, pumping stations, sensors.
- Drinking water system—distribution network including pipes, valves, pumping stations, sensors and plumbing systems.
- Tanks—storage or distribution reservoirs.
- Wastewater system—wastewater collection network; interceptor system; combined sewer overflows; pumping stations; storage structures; infiltration systems; outfalls.
- Storm water system—storm water collection network; infiltration systems; storm water overflows; pumping stations; storage structures.
- Treatment—wastewater and storm water treatment.
- Receiving water body—river; estuary; lake; coastal water.

The water cycle system includes infrastructure assets (e.g. pipes, storage, tanks) and equipment (e.g. valves, pumping stations, measurement tools, processes) and important communication systems and control systems to the most critical components (wireless, SCADA, sensors).

Due to pressing factors such as ageing, climate changes, population growth, increasing expectation on the service quality and availability, energy restrictions, etc., it will in the future be even more important to monitor and control the performance and conditions of all the components of the water cycle to prevent undesired events and to act properly in case an event occurs.

To achieve a sustainable water service, efficiency for the whole water cycle management is required. Integrated water management is a strategy that brings

together all facets of the water cycle—water supply, sewage management, water treatment and storm water management—to achieve strong triple bottom line benefits in addition to guarantee technical performances with respect to government requirements. This means that only with an integrated approach, including optimized storm water management to use all the available capacity of the drainage system, efficient wastewater treatment, safe and environmental safeguard of natural resources, adequate treatment solutions and safe and healthy delivery, the ultimate goal of delivering safe, secure and reliable service is attained.

9.2 Analysis Preparation

This section emphasizes important aspect of the analysis preparation including standard elements described in Chap. 3, but water and wastewater-specific issues are specially considered.

9.2.1 Standard and Directives

The general methodology for risk and vulnerability outlined in Chap. 3 of this book does not explicit points to standards and directives. In the preparation of the risk analysis, it is important to state whether such standards and directives exist, and to which extent they are mandatory. In this section, a brief description of standards, directives and approaches that apply for water and wastewater are briefly described.

The application of the risk management framework (ISO 31000) at the water cycle should start with the identification of the aims of the analysis with regard to safety and health, environmental protection and security.

The level of acceptance of risk for each aim of the risk analysis has to be defined, and often, standards and directives are taken as reference.

Overall, directions for water utilities and other stakeholders included in the ISO and EN standards (ISO 24511:2007, ISO 24512:2007 and EN 752:2008) cover aspects such as:

- Protection of public health;
- Safeguard public safety;
- Protection of surface and groundwater;
- Sustainable use of resources (water, energy…);
- Continuity of service;
- Fulfil needs and expectations of consumers and other users;
- Sustainability of the service.

Furthermore, relevant EU Directives have to be taken into account, namely:

- **Water Framework Directive** (2000/60/EC) which aims at protecting European water resources (rivers, lakes, groundwater, estuaries and coastal waters). It requires Member States to achieve "good ecological and chemical status" in all water bodies by 2015, by preventing water pollution and deterioration of water quality and to ensure that the achieved status does not deteriorate. In terms of quantity, the Directive restricts abstraction of water from water sources to a quantity that corresponds to the portion of the overall recharge not needed by the ecology.
- **Drinking Water Directive** 98/83/EC (revision in progress) whose objective is the protection of the consumers' health by guarantying the quality of drinking water. It sets quality standards for drinking water at the tap (microbiological, chemical and organoleptic parameters) and the general obligation that drinking water must be wholesome and clean.
- **Urban Waste Water Treatment Directive** (91/271/EC) whose objective is to protect the environment from the adverse effects of urban waste water discharges and discharges from some industrial sectors. It sets requirements in terms of level of wastewater treatment and limits for pollutants in the treated wastewater.
- **Bathing Water Directive** (2006/7/EC) which aims to ensure good bathing water quality. It sets quality standards for bathing waters by establishing limits for physical, chemical and microbiological parameters.
- **Groundwater Directive** (2006/118/EC) whose aim is the protection of groundwater from pollution to deterioration. It sets groundwater quality standards (at present, the maximum limits for pollutant concentrations have been set for nitrate and pesticides) and introduces measures to prevent inputs of pollutants into groundwater.
- **Floods Directive** (2007/60/EC) that promotes the assessment and management of flood risks considering climate change aspects. It requires Member States to identify water courses and coast lines at risk from flooding, to map the flood extent and assets and humans at risk in these areas and to implement control measures to reduce the flood risk.

Other documents to take into account include:

- **EU Communication on Water Scarcity and Drought** (COM 2007/414) that addresses the challenge of water scarcity and droughts in the European Union. It promotes, among other measures, the development of drought risk management plans.
- **EU Thematic Strategy for Soil Protection** (COM 2006/231) that addresses the protection and sustainable use of soil, based on guiding principles including preventing further soil degradation and preserving its functions and restoring degraded soils to a level of functionality consistent at least with current and intended use.
- **EU Proposal for a Directive of the European Parliament and of the Council establishing a framework for the protection of soil and amending Directive 2004/35/EC** (COM 2006/232).

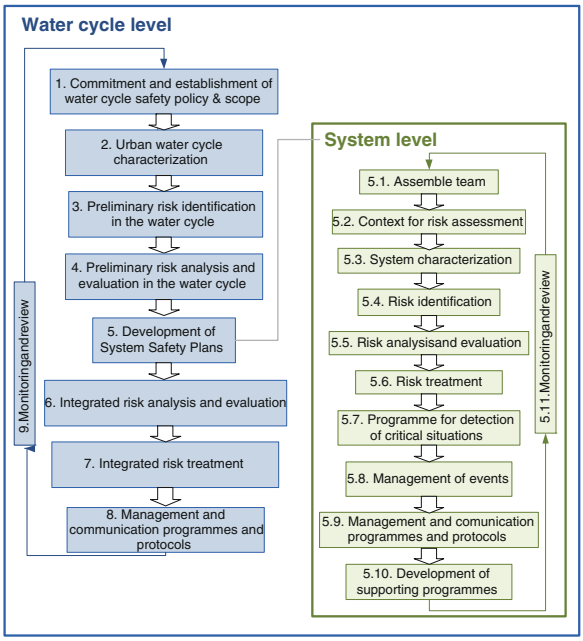

Fig. 9.2 WCSP framework [1]

Other important aspects to take into consideration include efficiency in the use of resources and minimization of greenhouse gases (GHG). Widening scope of safety plans implies multiple primary aims when looking at the water cycle. Therefore, the envisaged scope of the water cycle safety plans comprises the *protection of public health* but also the *public safety* and the *protection of the environment*.

9.2.2 Risk Management in the Water Cycle Safety Plan

In the 7th framework programme project PREPARED (www.prepared-fp7.eu), the risk management framework, as from ISO 31000, has been adapted to the water cycle management [1]. The project deals with adaptation to climate changes, therefore risks related to climate changes are the main interest of study. The work builds on the EU project Techneau [13] where a framework for risk analysis of drinking water systems from source to tap was developed [6]. The aims of the risk management presented are the ones of the Water safety Plan [16] but applied to the whole water cycle, health and safety, security and environment. The analysis is described at both the integrated and/or the system level. At the integrated level, issues are dealt with at a macro scale, and interactions between cycle components are considered. Detailed analysis is carried out at the system level. At both levels,

safety plans should be produced, one for the water cycle and as many system plans as the existing number of organizations managing water systems, see Fig. 9.2.

WCSP developed in PREPARED is specific to water systems and focuses on risks related to human health and safety, security and environment. Conversely, the «Risk Management Process», RMP, approach is broader, applicable to any field and can be used to manage any type of risk. One main difference between the RMP and WCSP is that the risk evaluation step in RMP is not included in WCSP. According to Rosen et al. [13], this is probably due to the fact that the WCSP work, as the WCSP, is guided by health-based targets and decisions about tolerable risk are made when the targets are compiled. However, to deal with risks that cannot be controlled using predetermined targets, the risk tolerability decision should be included as part of the work.

9.2.3 Objectives, Stakeholders and the Challenges for Managing the Urban Water Systems

UWCS are required to supply water for the various urban water usages to ensure that the wastewater produced is adequately handled and that the rainwater is also well managed. These objectives have to be achieved while ensuring the WCSP aims: protection of public health but also the public safety and the protection of the environment. Standards and directives presented in Sect. 9.2.1 are used as references to set the level of acceptance of risk in a WCSP.

Every water and wastewater system is unique case study with its own unique organization, driven by governmental policies and regulations, demand from consumers to expected levels of service, therefore describing the system, understanding the expectations of the different stakeholders, and identifying the present and future challenges is of primary importance to implement the WCSP.

The practical outcome of the analysis is the choice and design of different elements of the urban water infrastructure, as well as their operation, maintenance and development.

The main challenges of the system are the ageing of infrastructure, increase of demand or different water uses, and impacts of climate changes.

Ageing infrastructure (physical) assets deteriorate in efficiency and need to be overhauled and rehabilitated, and parallel to this, population growth complemented by a rise in purchasing power may call for an increase in demand for services. Together, this may lead to greater stress on the infrastructure assets, accelerated wear and tear, capacity constraints, customer (or consumer) dissatisfaction and a general reduction in welfare levels.

Changing demands, society, industry and agriculture influence the uses of water. By varying these human uses, the water and sanitation services in the future will be influenced and will need to adapt. However, changes in water use will not act alone. Climate changes will affect, directly or indirectly, the whole water cycle,

including all its components. It is thus essential to identify which water cycle components (and their associated subsystems) will be affected, how they will affect and with what magnitude; it is also important to take into account potential cascade effects. The water cycle is expected to be affected by both acute and slow developing climate change effects: the acute deals with acute events like flooding, whereas the slow developing leaves signs that something is happening, such as change in water colour. Both types of events will influence practice and methodologies to manage and operate the systems. The acute events should be faced and mitigated at planning and crisis management level, while the slow developing events should be dealt with at planning level.

9.2.4 System Boundaries and Consequence Categories

The illustration of a water and wastewater system in Fig. 9.1 forms the basis for defining the system boundaries in terms of which components are involved. In addition to the physical delimitation, it is also important to emphasize organizational factors and other forces that will influence the system performance. A starting point for such delimitation is shown in Fig. 9.2.

In the Oslo case study presented in Sect. 9.3, both probabilities and consequences were assessed on a four point scale. For the probability dimension, it has been found efficient to use qualitative criteria when assessing the probabilities. The probability categories with corresponding criteria are shown in Table 9.1.

Altogether, five dimensions were found necessary in order to get a reasonable complete picture to assess the consequences. The categories used for consequences are shown in Table 9.2.

Table 9.1 Categories of probability (Oslo case study)

Probability category	Criteria
P1: small	a. The event not known within the water industry b. The event cannot be totally excluded c. Safety evaluation indicates low probability
P2: medium	a. The event has occurred within the water industry the last 5 years b. Professional and precautionary evaluations indicate that the incident might be able to happen within the next 10–50 years c. Safety evaluation indicates medium probability
P3: high	a. The event occurs every year within the water industry b. The water company has observed some events or the events nearly happened c. Professional and precautionary evaluations indicate that the incident might happen within the next 1–10 years d. Safety evaluation indicates high probability
P4: very high	a. The event is regularly observed within the water company b. Safety evaluation indicates very high probability

Table 9.2 Categories of consequences with corresponding description for each consequence dimension

Categories of consequence	Consequence dimension				
	Health/ Life quality	Unavailability/ Capacity	Reputation	Economic	Environmental
C1—Low	Intangible damage to population	Insignificant impact on the service	Reputation not threatened	Economic loss less than 5 % of yearly costs	Minor environmental damage restored within a few days
C2—Medium	1 injury in need of medical attention	Short terms (h) of effect on the service	Reputation threatened	Economic loss less 5–10 % of yearly costs	Major environmental damage restored within weeks
C3—Large	Several cases requiring medical attention/hospital	Medium term (d) of effect on the service	Short term loss of reputation	Economic loss less 10–20 % of yearly costs	Sever environmental damage restored within months
C4—Very large	Several cases requiring medical attention/hospital at least 1 invalidation	Long term (>1 week) of effect on the service	Long term loss of reputation	Economic loss less greater than 20 % of yearly costs	Critical environmental damage requiring years to restore

The most important consequence dimensions in the Oslo case study was health/life/quality, unavailability/capacity and reputation.

9.3 Coarse Risk Analysis: Oslo Case Study

SINTEF has carried out a risk and vulnerability study for the water and wastewater company in the Norwegian capital Oslo [15]. The analysis covers the complete urban water cycle from drinking water catchment to wastewater treatment plant and main findings will be presented in the following. An important aspect of the work has been on identifying undesired events both for all individual subsystems (e.g. water treatment plan, water distribution) but with attention also at the borderland between the different disciplines. Special focus has also been on potential critical links to other infrastructures like telecommunication and electricity. The work included traditional techniques for risk identification and risk evaluation (e.g. risk matrixes), but also more in-depth analysis like Fault Tree Analysis (FTA) of a large pumping station for both water and wastewater systems. The FTA proved to be a powerful tool for identifying critical events and was also used for evaluating different risk-reducing measures (e.g. improved maintenance routines). Several types of thematic maps were also produced serving as a basis for the risk identification.

9.3.1 Risk Identification in the Case Study of Oslo

In order to reveal hazards and threats to the water and waste water system, the starting point is the water and wastewater cycle illustrated in Fig. 9.1. It is essential that not only the generic elements are considered, but that one follows the flow of the water through the water cycle and analyses what can go wrong for each component. The identification process follows the procedure shown in Fig. 9.2.

In the actual study, the system was classified in different systems, subsystems and components and undesired events for each of them have been listed. For the wastewater part, for instance, the urban drainage system has the following subsystems (bold) and components (in brackets):

- **Storm water network** (big pipe, medium pipe, small pipe, tunnel, manhole, overflow structure, valves, culvert, siphon, pump, storm water detention)
- **Sanitary network** (big pipe, medium pipe, small pipe, tunnel, manhole, overflow structure, valves, culvert, siphon, pump)
- **Combined network** (big pipe, medium pipe, small pipe, tunnel, manhole, overflow structure, valves, culvert, siphon, pump)

Similar was done for all other urban water cycle subsystems and components.

In general, historical (past) events form an important input to the process of identifying undesired events and threats to the water cycle systems. To maintain a list of critical events serving as a check list in the identification process is therefore important. Both events experienced for the actual utility company as well as critical events from other places should be systemized in such a check list. Below some examples of events are given for both water quality issues (microbiological contamination, chemical contamination) and water quantity issues. This list also serves as an inspiration list for the water company when looking for "black swans", that is, rare events that not have been considered before but which have happened elsewhere.

9.3.1.1 Selected Events from Literature Related to Contamination of Drinking Water

Milwaukee, US (1993): Suboptimal design and operation of water treatment plant (coagulating and filtration) causes a waterborne outbreak of cryptosporidiosis. A total of 400,000 got sick and 69 died. One of the contributing factors for the event to happen was reuse of water used for backflow from filters [3].

NW London/Hertfortshire, England (1997): A total of 345 persons confirmed sick caused by *Cryptosporidium* contamination of a groundwater well. Cause of the event not defined, but prior to the event there was a long-lasting drought followed by heavy rain. A total of 746,000 inhabitants boiled the water. Afterwards, water treatment using membranes has been implemented for removing parasites. (Three valleys water, 2006).

Walkerton, Canada (2000): A total of 2,300 got sick and 7 died caused by *E.coli* O157:H7 and *campylobacter jejuni*. The reason for the outbreak was run off from cow manure into a groundwater well. Long-lasting negative health effects observed after the outbreak, [3] and [6].

Bergen, Norway (2004): Waterborne outbreak where 4,000–6,000 persons got giardiasis. The parasite Giardia was found in the surface water reservoir Svartediket. (www.bergenvann.no)

Nokia, Finland (2007): Large waterborne outbreak where 8,000 person got sick and most likely 3 persons died caused by the outbreak. A total of 450,000 L of "treated" wastewater flowed into the drinking water network due to a non-functioning backflow prevention valves/system. It took more than 3 mon to clean the drinking water network afterwards [5].

Northampton, UK (2008): Waterborne outbreak of cryptosporidiosis. A boiling water notice was issued for 250,000 persons lasting for 10 days. 22 persons got sick. Genotyping of contaminated water showed that the source of the contamination was rabbit. A dead rabbit was found in the clean water tank after the water treatment plant. Chlorine disinfection did not inactivate Cryptosporidium. The outbreak was detected by a continuously water sampling system [5].

Østersund, Sweden (2010): Waterborne outbreak where 12,000 persons reported themselves on the webpage to be infected. The parasite Cryptosporidium was

found in the surface water reservoir. The water had to be boiled from 27 November 2010 to 19 February 2011. The raw water source was a large lake, and within the storm water system, several cross-connections with the sewer system were detected. The water treatment was not adequate for removing or disinfection of the parasite. Afterwards, UV-disinfection has been implemented (www.ostersund.se).

Camelford, UK (1988): A total of 20 t of aluminium sulphate delivered to a chlorine tank. Instead of disinfection, the water with chlorine aluminium sulphate was pumped into the water flow. After the event there has been media focus on the increased risk of Alzheimer disease resulting from the high aluminium doses [3].

Boston (US) (2010): A pipe break on a large 3,000 mm diameter pipe only 7 years after installation. A previously used water source with poor water treatment was used as alternative supply. A boiling water notice was issued for 2 million persons lasting for 3 days [6].

Bergen, Norway (2010): Long period without rainfall/snow melting combined with higher water consumption due to frost tapping (open taps for avoiding frost in plumbing system). Backup source without required multiple barriers in treatment. 20,000 persons got water witch only had been chlorinated. Boling notice was issued, in the relevant period. Bergen water has afterwards installed UV-disinfection also for this backup supply if to be used in the future (www.bergenvann.no).

Severn Trent, UK (2007): The water treatment plan was flooded from the rivers Severn and Trent. The treatment plant was located on the bank of the river. 300,000 persons without water supply for 17 days. During the event, bottled water/tanks was provided on a large scale and military was also involved. Critical equipment was sent for dehumidification. Flood defences have been erected by Severn Trent Water following this event to provide some level of protection should another such event occur (DWI 2007).

9.3.2 Risk Assessment and Presentation of the Risk Picture in the Case Study of Oslo

Each risk event has been recorded in a risk matrix according to the level of probability and of consequence. Green boxes show the events at low risk, yellow the ones at medium risk and red the ones at high risk. The most critical events (green events not shown) relevant to drinking water are shown in Fig. 9.3.

For instance, some of the identified possible events related to drinking water in Oslo were (numbers refer to the circles in Fig. 9.3):

- Event 2: Contamination of drinking water in water tanks
- Event 8: Long-lasting drought will lead to water scarcity problem in Oslo
- Event 10: Failure at critical pumping station
- Event 13: Virus or hacking of SCADA system at water treatment plants

Resulting from the analysis, different risk-reducing measures are being implemented. The most important one is the establishment of a new alternative

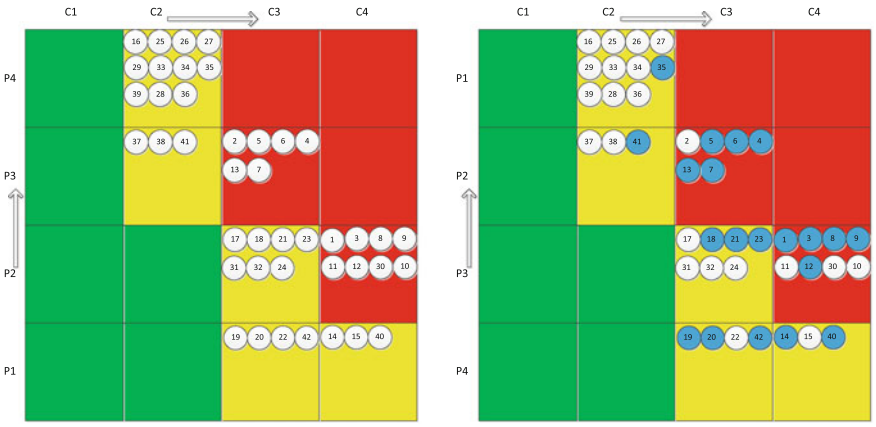

Fig. 9.3 Example of risk matrix for the OSLO case study, each *circle* represents a specific event relevant for water supply (only *yellow* and *red* events shown). Right part shows the effect of implementing a new alternative water supply source and which of the events this has an effect on (in *blue*)

water source and corresponding water treatment plant. These measures alone will remove most of the critical events identified as indicated with blue circles in Fig. 9.3.

9.4 Detailed Analysis: Fault Tree Analysis of a Water Pumping Station in Oslo

The coarse risk analysis described in Sect. 9.3 gives a rough overview of the risk picture but will not be detailed enough to get a proper understanding of the real challenges and to what extent a risk-reducing measure will actually influence the risk. The objective of the detailed analysis is therefore to get a better understanding of the causes behind each undesired event identified in the coarse risk analysis. Oslo has more than 30 pumping stations for water, and some of these are more critical than others. One of the new pumping stations feeding the western part of Oslo was selected a case study for a detailed analysis with a fault tree analysis (FTA).

It is recognized that careful planning in advance of an emergency gives a water utility a far better chance to successfully handle a major failure. It also provides more and better services while reducing lost revenue and recovery costs. Defining the role and abilities of the maintenance and engineering department in emergency preparedness must start in the planning process, which helps avoid a reactionary, run-to-failure approach. For failure of technical systems like the pumping station, the natural risk analysis technique to apply is the FTA. In the case study of Oslo, a detailed FTA was therefore carried out for the major water supply and wastewater

pumping stations. As example, the FTA of a specific water pumping station is presented in the following.

The analysis showed which elements of the water pumping station contribute most to the development of the selected undesired events that may cause interruptions in the operation of the pumping station. Although today's water pumping station is reliable, the provision to customers will be interrupted, in case of its unavailability, if the time to repair will last longer than the time to empty the connected compensation tank. The detailed analysis with FTA helped to identify new actions that will further increase the reliability of the water pumping station. The measures are in terms of simple measures and changes in operating and maintenance procedures. The main measures proposed are increased access security, installation of automatic fire extinguishing system, improved/new procedures for periodic maintenance (i.e. periodic testing of the sensors in the pump stations).

For building the fault tree of the pumping station, the following steps were followed:

- Obtain an understanding of the system
- Identify the *objective* for the FTA and define the top event
- Construct the fault tree and collect data
- Assess input data for different types of events.

9.4.1 Obtain an Understanding of the System

All available information about the system and its environment should be studied. A teamwork analysis and brainstorming with the water utility of Oslo proved to be a helpful exercise in determining the necessary information.

9.4.2 Identify the Objective for the FTA and Define the Top Event

When creating a FT, a basic requirement is to define the objective of the FTA. To be successful, the objective should be phrased in terms of a failure of the system to be analysed. Once, the objective is defined in this way then the top event of the FT is also defined. A so-called top event is a critical event in the system being analysed, and the main objective of the FTA is to find causes leading up to the top event and eventually quantify the probability of the top event to occur. In order to define the top event, three questions are asked, What, Where and When? The "what" question is representing what our concern is about, and here, this would be TOP = The pumping station fails. The "where" question is used to specify the location, and here, it is therefore required to specify which pumping station that is being assessed. The "when" question typically addresses operational modus, for

example, whether this is under normal operation or under a major revision of the station. It might also be necessary to be more specific with respect to what a failure is, for example is it total loss of pumping capacity, or only reduced capacity?

9.4.3 Fault Tree Construction

The construction of the FT consists in defining, for each event that is analysed, the most closely related events that result in the event itself, that is, identify the possible causes that contribute to the top event, that is, the pumping station fails to function. Possible causes for such an event to happen are (see also [13]):

- Inflow stop
- Pumps failure
- Control system failure
- Presence of water in the floor
- Sabotage
- Operator failure
- Failure at the electrical cabinet.

Logic symbols are used in the fault tree to represent the relationships between events.

The contributors are connected to the TOP EVENT with an OR gate, that means in order to stop the station at least one of those contributor events has to happen. The transfer symbols (P1–P10) following each event in Fig. 9.4 indicate that for each causes a FTA is built. The transfer symbols are actually pointers to separate pages in the fault tree. For example, Fig. 9.5 shows page P3 with a system with 4 pumps in parallel. 2 pumps at a time are continuously working to satisfy the demand in the zone. In order to have the station not functioning, 3 over 4 pumps have to be out of order at the same time, since 1 pump only would not be able to satisfy the water demand.

9.4.4 Reliability Data for the Basic Events

In the current analysis, the basic event essentially represent component failures. The reliability of each component is determined by the failure rate and downtime given that a failure occurs. The failure rate is the reciprocal of the mean time to failure (MTTF), whereas downtime is described by the mean time to repair (MTTR). The average fraction of time the component is not able to fulfil its function (unreliability) is given by the ratio MTTR/MTTF. The reliability data for the basic events are shown in Table 9.3.

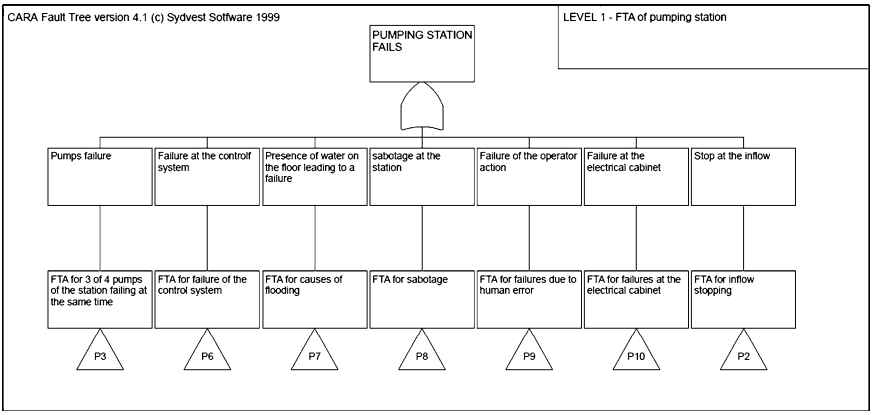

Fig. 9.4 Fault Tree of a pumping station: first level of contributors

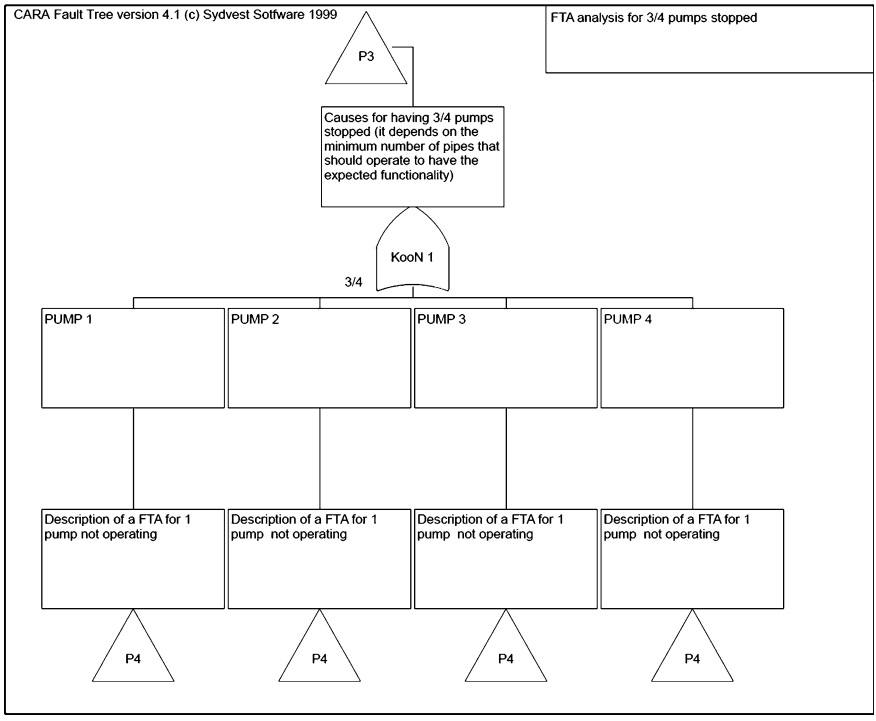

Fig. 9.5 Page P3 where the use of KooN gate is illustrated

Table 9.3 Reliability data for the basic events

Event number	Description	MTTF (years)	MTTR (h)
Basic 1	Electrical failure inflow valve	50	360
Basic 2	Total failure electrical cabinet	20	2,160
Basic 3	Water on the floor, gully blockage	50	1
Basic 4	Sabotage	50	1,440
Basic 5	Pipe break inside the station leading to low pressure	50	8
Basic 6	Low pressure at the inlet of station	30	3
Basic 7	Low pressure from supplying pumping station leading to no flow entering the station	50	2
Basic 8	Low pressure from pipe break leading to no flow entering the station	20	12
Basic 9	Cable failure due to external digging leading to failure of 1 pump	10	24
Basic 10	Transform failure leading to failure of 1 pump	500	8
Basic 11	External electricity failure	1	4
Basic 13	Engine mechanical failure in 1 pipe leading to failure of 1 pump	20	72
Basic 14	Starting system failure leading to failure of 1 pump	50	1
Basic 15	Frequency control: over current leading to failure of 1 pump	10	96
Basic 16	Unbalanced rotating wheel due to sabotage in the pump leading to failure of 1 pump	100	720
Basic 17	Failure engine shaft leading to failure of 1 pump	10	720
Basic 18	Vibration leading to failure of 1 pump	20	1
Basic 19	Lightening failure leading to main switcher failure and then 1 pump failure	6	24
Basic 20	Overvoltage leading to main switcher failure and then 1 pump failure	20	1
Basic 21	Electrical motor failure leading to main switcher failure and then 1 pump failure	20	72
Basic 22	Sensor failure due to over voltage leading to a failure of the control	20	360
Basic 23	Sabotage: data hacking leading to a failure	50	24
Basic 24	Pressure switches failure leading to a failure of the control system to stop the pumping station	10	1
Basic 25	Set to maximum speed for pumps leading to a failure of the control system to stop the pumping station	50	1
Basic 26	Control system failure due to lack of power leading to a failure of the control system to stop the pumping station	3	1

(continued)

Table 9.3 (continued)

Event number	Description	MTTF (years)	MTTR (h)
Basic 27	Control system failure (single component) due to overvoltage peaks leading to a failure of the control system to stop the pumping station	20	1
Basic 28	Water on the floor due to failure of the sensor system leading stop the pumping station: if level over 5 cm	20	24
Basic 29	Operator failure leading stop the pumping station	4	1
Basic 30	Failure (single component) at switched cabinet #1 producing failure to electrical cabinet and leading stop the pumping station	20	72
Basic 32	Failure (single component) at switched cabinet #2 producing failure to electrical cabinet and leading stop the pumping station	20	72
Basic 33	Failure at the main cabinet leading to failure at the electrical cabinet	20–30	72
Basic 34	Fire leading to failure at the electrical cabinet	30	720
Basic 36	Change of phase due to external leading to failure at cabinets and to stop the pumping station	30	1
Basic 37	Change of phase due to internal failure leading to failure at cabinets and to stop the pumping station	30	1
Basic 38	Inflow valve failure due to electrical problem leading to no flow in the station	50	24
Basic 39	External electricity grid failure leading to failure of 1 pump	5	24
Basic 40	Control system failure (all the system) due to overvoltage peaks leading to a failure of the control system to stop the pumping station	20	24
Basic 41	Indirect sabotage leading stop of pumping station	20	24
Basic 42	Cable failure (e.g. rats) leading to stop of pumping station	50	4
Basic 43	Failure at switched cabinet #1 leading to stop of pumping station	20	2,160

Table 9.4 Most important events contributing to failure of the pumping station

Event number	Description	Birnbaums measure
Basic 4	Sabotage	9.86911e−001
Basic 34	Fire leading to failure at the electrical cabinet	9.65002e−001
Basic 22	Sensor failure due to over voltage leading to a failure of the control	9.64343e−001
Basic 17	Failure engine shaft leading to failure of 1 pump	9.64084e−001
Basic 15	Frequency control: over current leading to failure of 1 pump	9.63420e−001

9.4.5 Minimal Cut Set Listing

A minimal cut set in a fault tree is a set of components where the failure of the components in the set ensures that the system will fail (top event occurrence). A cut set hence represent a set of components having the ability to "kill the system". A cut set of only one components means that a single failure will cause the system to fail, whereas a cut set with two components will require two components to fail in order to kill the system.

For the pumping stations, 36 first-order cut sets and 4 s-order cut sets were identified.

9.4.6 Quantitative Results

The most important quantitative result from a FTA is the top event probability, or, in a semi-quantitative analysis, the frequency of the top event occurrence. A quantitative FTA may also list the importance of each basic event which is a measure of each component's contribution to the failure of the system. The probability of the top event is calculated to 0.018 and the system availability 0.9742. The unavailability of the pumping station is thus 1–0.9742 = 0.0258 years, that is, 226 h/year. However, due to the fact that there is also a water tank in the zone, failures lasting for less than 24 h will have no consequences. The five most important events according to Birnbaums importance measure (i.e. the rate of change in the top event probability as a result of the change in the probability of a given event) for the water pumping station are shown in Table 9.4.

9.4.7 Lessons Learned from the FTA of a Pumping Station in Oslo

From the perspective of Oslo Water, the FTA has proved to be a very powerful tool for identifying possible causes of failures for the pumping station. Drawing the fault tree and defining the input values (i.e. failure data and repair data) was in itself a useful exercise, but the identification of the most critical events and the identification of efficient risk-reducing measures proved to be very useful for the company.

Possible risk-reducing measures for these events have been identified. For example for event number 34, "Fire in electrical cabinets" the following efficient measures has been identified:

- Installation of fire extinguishing system (e.g. CO_2)
- Increase frequency of periodic thermal photographing main cabinets from once a year to twice a year. This should be considered for the most for the most critical pumping stations
- Installation of systems for emergency power.

References

1. Almeida, M. C., Ugarelli, R., Leitão, J. P., & Vieira P. (2011). Risk identification. Supporting document definition of contents and data structure. Report D. 2.2.1—PREPARED Project. En 752:2008—Drain and sewer systems outside buildings.
2. Hrudey, E., Og Hrudey, E,. (2004). *Safe drinking water Lessons from recent outbreaks in affluent nations*. London: IWA Publishing.
3. Hamilton, P. D., Paul, G & Simon J. T. Pollarda (2006). A commentary on recent water safety initiatives in the context of water utility risk management. Environment International, 32(8), 958–966.
4. Health Stream. (2008) Public health newsletter newsletter of water quality research Australia. Issue 49 March 2008 (8TUhttp://www.wqra.com.au/hs/hscurrent.htmU8T).
5. Health Stream. (2010) Public health newsletter newsletter of water quality research Australia. Issue 58 December 2010 (8TUhttp://www.wqra.com.au/hs/hscurrent.htmU8T).
6. Hokstad, P., Røstum, J., Sklet, S., Rosén, L., Pettersson, T. J. R., Linde, A. et al. (2009). Methods for risk analysis of drinking water systems from source to tap—Guidance report on risk analysis. Available from http://www.techneau.org/index.php?id=124.
7. ISO. (2009). ISO 31 000:2009 Risk management. Principles and guidelines. International Standards Organization.
8. ISO. (2009). ISO 31 010:2009 Risk management. Risk assessment techniques. International Standards Organization.
9. ISO (2009). ISO Guide 73:2009 Risk management. Vocabulary. International Standards Organization.NHMRC. (2008). *Guidelines for managing risks in recreational water*. Australia: National Health and Medical research Council.
10. ISO 24511:2007—Activities relating to drinking water and wastewater services—Guidelines for the management of wastewater utilities and for the assessment of wastewater services.
11. ISO 24512:2007—Activities relating to drinking water and wastewater services—Guidelines for the management of drinking water utilities and for the assessment of drinking water services.
12. Rausand, M., & Høyland, A. (2004). *System reliability theory; models, statistical methods and applications* (2nd ed.). New York: Wiley. (ISBN 0-471-47133-X).
13. Rosen, L., Hokstad, P., Lindhe, A., Sklet, S., & Rostum, J. (2009). *Generic framework and methods for integrated risk management in water safety plans*. Germany: Techneau Report.
14. Røstum, J., Ugarelli, R. Selseth, I. (2011). Risikovurdering av vanndistribusjon som en del av ROS VAV prosjektet. SINTEF rapport SBF 2011 0052.
15. Røstum, J. (2011). Risiko—og sårbarhetsanalyse (ROS) i Vann- og avløpsetaten.—Sammendragsrapport. SINTEF report SBF2011F0053.
16. WHO. (2009). *Water safety plan manual*. Geneva: Step-by-step risk management for drinking-water suppliers.

Chapter 10
Information and Communication Technology: Enabling and Challenging Critical Infrastructure

Maria B. Line and Inger Anne Tøndel

Abstract Information and communication technology (ICT) is increasingly becoming a part of all critical infrastructures, and thus, there is an increasing need to include ICT in all risk assessments. This chapter explains the dependencies between ICT and other infrastructures and provides an overview of the threats and risks associated with ICT. The chapter also gives an introduction to modelling techniques that is of particular use when performing risk analyses of ICT systems. The chapter ends with recommendations on how to include the ICT aspects in risk assessments of other infrastructures.

10.1 Introduction

The capacities of information and communication Technology (ICT) have evolved enormously over the latest decades. A study of the developments from 1986 to 2007 [1] shows an annual increase of 58 % in the general-purpose computing capacities, a growth of bidirectional telecommunication capacity of 28 % per year and a 23 % annual increase in globally stored information. ICT infrastructure now includes a variety of solutions offering communication, storage and processing of information, consisting of equipment and software targeted at highly different user groups. Individuals utilize ICT infrastructure for a high number of tasks, including entertainment, communication and business. ICT infrastructure is also used for controlling critical processes in other infrastructures, e.g., through process control systems. ICT is thus a critical infrastructure in itself, at the same time it is an

M. B. Line (✉) · I. A. Tøndel
SINTEF ICT, Trondheim, Norway
e-mail: maria.b.line@sintef.no

P. Hokstad et al. (eds.), *Risk and Interdependencies in Critical Infrastructures*, Springer Series in Reliability Engineering, DOI: 10.1007/978-1-4471-4661-2_10,

important component of other critical infrastructures, such as power supply, water supply and transportation.

This chapter addresses the dependencies between ICT and other critical infrastructures and explains the main threats towards ICT systems. It also provides an overview of common ways to perform risk analyses with respect to ICT. The chapter does not focus on the traditional ICT infrastructure, such as the telecom network, but rather on ICT systems that are an integrated part of other infrastructures. Recommendations are also provided on how to include ICT when risk analyses of critical infrastructures that utilize ICT are performed.

10.2 Dependencies between ICT and other Infrastructures

The increased dependence on ICT in a number of critical infrastructures results in a need to properly address the interdependencies that exist between these infrastructures and the ICT systems. Whereas the traditional ICT systems used in such infrastructures were proprietary and not connected to the outside world, the recent trends towards more general-purpose solutions, software and increased networking have radically changed the benefits and risks involved. The progress in ICT has been important to achieve cost savings. Utilizing the Internet for communication related to operation and management of remote processes and production systems increases efficiency and cooperation and saves time and money in localization and correction of faults and errors. Using commercial off-the-shelf (COTS) components, such as MS Windows, in control systems further reduces costs. However, though the gain is obvious, there is also a downside when it comes to information security issues. The increased use of publicly available ICT systems instead of proprietary solutions, and the increased connectivity between different types of networks, make formerly isolated ICT systems vulnerable to a set of threats and risks they have not been exposed to before. This poses new challenges to communities who have not been used to operate such ICT systems before, and ICT can be a source of failures to other infrastructures. However, ICT also usually plays a crucial role in emergency management, and the dependencies between ICT and other infrastructures are exemplified below.

In the oil and gas industry, the advances in ICT made it possible to introduce integrated operations (IO) as means to run offshore facilities more efficiently. IO implied a change of technology from proprietary stand-alone systems in closed or physically separated networks to standardized COTS systems integrated in communication networks. In other words, “traditional” ICT components were included in the process control networks, and logical network connections were established between process control and administrative/office networks. Before, there were no such connections; those two different networks were physically separated with no means of reaching one of them electronically from the other. Now, with the logical connection, although well protected, it is possible to reach control systems offshore from all over the world over the Internet. So, even though the development of IO

makes remote control and support possible and results in savings in both time and money, since few persons simultaneously can monitor a large set of installations, it also increases the dependencies on ICT and opens up for a great number of new information security threats.

The same kind of development also takes place in the power industry, with the Smart Grid vision, which is a close relative to IO. Smart Grids is about introducing ICT components into the power distribution grid: sensors for monitoring and control, smart meters and two-way communication. Smart Grids connects power plants and system control centres with all households, businesses and buildings all over the country—and abroad. The power industry is thus moving towards a situation where the power distribution depends on ICT, while the ICT infrastructure itself depends on power.

Such an evolution within critical infrastructures makes ICT an integrated part of all other industries. It is thus not possible to make a clear separation between the ICT systems and the industry that utilize these systems. Take the Smart Grid vision; the ICT systems are a part of the power distribution, monitoring and influencing the whole service delivery. As a result, it is rather obsolete to make a clear separation between ICT and oil/gas, ICT and power, ICT and water distribution and so on. All infrastructures are based on ICT, and specific ICT competence is therefore necessary in operation and management, in addition to competence related to the core business of the specific infrastructure.

10.3 Information Security

Within the ICT disciplines, a lot of effort is put into protecting the ICT systems. A central part of ICT is the information processed by the system (note the "I" in ICT), and the work on protecting the ICT systems is usually denoted by information security.

The most common definition of information security comprises the properties of confidentiality, integrity and availability [2], where

- *Confidentiality* means that the information is not made available or disclosed to unauthorized individuals, entities or processes.
- *Integrity* means safeguarding the accuracy and completeness of assets that no unauthorized modification can be made to the information or the system that handles the information.
- *Availability* means that information shall be accessible and usable upon demand by an authorized entity.

In an extended definition of the term information security, the following aspects could also be included:

- *Authentication*: determining whether someone or something is who or what it is declared to be.

- *Non-repudiation*: ensuring that a party cannot deny the authenticity of their signature on a document or the sending of a message that they originated.
- *Traceability*: it should be possible to see which changes are performed to information, who did it and when.
- *Privacy*: ensuring that each individual can control their own information and what it is used for.

When addressing information security aspects of an ICT system, there is a need to consider malicious actions directed at the system as well as errors and accidents that can result in security breaches. Information security is also not purely a technical matter, but is highly dependent on the people and the organization surrounding the system.

Note that one will never be able to claim that a system is 100 % secure. Due to the extensive investments needed, achieving close to 100 % should not be the goal either. The most important and indeed challenging task is to choose the right level of security balanced with an acceptable level of risk. Implementing security mechanisms can be costly, but so can also the consequences of not implementing them; however, documenting the financial gain of security mechanisms is difficult.

10.4 Threats and Vulnerabilities

In general, the evolution of ICT systems and its use within critical infrastructures has radically changed the threats to such infrastructures. Proprietary systems off-line have traditionally had an attack surface close to zero, as an attacker would have to be geographically at the same place as the target system and have detailed technical knowledge about the system in order to be able to do harm. When connecting these proprietary systems to the outside world through ICT networks, this is no longer the case as they can be reached from anywhere. In addition, the increased use of COTS systems results in production systems being easier targets. Although detailed technical knowledge is still required, there are far more experts of COTS systems worldwide than there are experts of proprietary systems. Thus, the introduction of ICT results in an increased need to consider incidents caused by attackers and not only failures that occur by accident.

Threats towards ICT systems can be divided into three main categories: (1) *unintentional incidents* that are possible due to weaknesses in the ICT system, unfortunate employees or external incidents; (2) *general attacks* that are not directly aimed at a particular ICT system, but rather attack ICT systems in general; and (3) *targeted attacks* that are directed towards a particular enterprise or system.

Unintentional incidents happen by sheer accident. Examples can be lightning, power failures, fire, disc crashes, communication failures, erroneous backups and mistakes made by employees. To limit the risk associated with such threats, it is important to consider both the technical and human side of ICT systems. On the technical part, measures can be made to assure that the loss of one individual

component does not result in failure of the whole system (single point of failure). On the human side, it is important to remember and take into account that the users of ICT systems and those building and maintaining ICT systems can make mistakes or use the system in unintended ways. Any lack of competence on how the systems should be used, and also the reliance on key personnel, can be a potential vulnerability.

General attacks are not aimed at a particular ICT system, but rather target a number of different ICT systems. Obvious examples are the high number of general malicious software found on the Internet. These may, for instance, aim to get access to computer resources, or get hold of personal information, like usernames/passwords, credit card number and so on. Although they are not targeted directly at a system, they can still do a lot of harm. The risk from general attacks increases as COTS components are used in the systems and as connectivity increases. Typical high-risk activities include employees surfing on the Internet from systems with critical functionality (e.g. production systems), remote access to control systems and connecting portable units (e.g. laptops, USB sticks) to critical systems.

Targeted attacks are performed with the motivation of harming one particular system or organization. They can be anything from physical attacks, for example, in form of burglary or vandalism, to attacks performed via the Internet. In the last case, the perpetrators may be located far away, but it is also possible for insiders to attack via the ICT systems. Physical attacks can also be combined with online attacks. Some attacks will only be possible if the attackers have detailed knowledge of the ICT systems and will thus require skilled and dedicated attackers. Such attacks may be rather unlikely, but may still have huge impact. Thus, they should still be assessed. Examples of targeted attacks include

- The injection of malicious software (malware) into the company's network, e.g., in form of a backdoor that enables an attacker to login remotely. Malware can be used to search for personal or confidential information, or to track everything that is typed on a keyboard.
- The use of social engineering techniques to trick users into providing inside information.
- Disruption of the availability of ICT services by performing a distributed denial-of-service (DDoS) attack, where large amounts of network traffic flood the service.
- Performing a break into the SCADA system, taking control of production processes, for example through a backdoor installed earlier by malware.

Several problems related to the security of ICT systems are rooted in the quality of the existing solutions. Experience shows that software contains a lot of vulnerabilities, of which some can be used by attackers to perform general untargeted attacks. A rich variety of malware has been detected during the last few years, and the amount is exponentially increasing. A number of tools exist that utilize malware and perform attacks automatically, and little knowledge is required to use these tools. Malware comes in the forms of viruses, worms, Trojan horses,

spyware, backdoors, key loggers and many others, but the main principle is the same; it is a piece of code that performs actions that the user has no control of; and usually with unfortunate consequences for the user and/or his computer system/network. The goal of attacking with malware may be several:

- To access certain computers for obtaining confidential/personal information
- To harvest personal information for sale and use for fraud
- To access computer resources, to use the computer as part of a larger attack
- To monitor emails and other correspondence related to certain persons of interest
- To obtain user names and passwords to a number of Internet services, e.g., by the use of key logging
- To log a user's activities on the Internet in order to create a marketing profile
- To encrypt files and demand payment for decryption: blackmailing
- To take control of production systems in order to do harm to a company or society: power supply, water supply, oil production, nuclear plants, traffic signals, etc.

A key to improved information security is to perform patching, i.e., install fixes to known vulnerabilities as soon as they are available. Patching is, however, problematic in some settings, as it takes time, may result in downtime and may affect system stability. Not installing patches is also risky as it leaves the system more vulnerable to attacks.

Recognizing a security incident is difficult if one is not used to it. Again, experiences from the oil and gas industry show that a computer may be unstable for days and weeks without anyone recognizing it as a possible virus infection [13]. Ensuring that such an incident is detected and responded to is an organizational and cultural challenge just as much as a technical. An ICT security incident does not necessarily lead to an unavailable system that, at best, shuts down gracefully or enters a safe mode. In fact, such a consequence would be advantageous, because it would mean that the incident is detected quite quickly. A much worse, and just as probable, consequence is that the ICT system slightly changes its behaviour, or does not change at all, which makes the incident hard to detect. It seems like everything is running like normal, but someone is wiretapping the communication, or someone is copying confidential information, or someone is injecting slightly justified values into the control system or the processor is used for spam distribution in addition to its real mission.

A number of real-life attacks towards the ICT system have had big consequences for critical infrastructures. Some examples are

- **Stuxnet**: In July 2010, a new and an advanced piece of malware; Stuxnet; was detected. This was the first occurrence of malware specifically targeted at industrial control systems. Its goal was to reprogram systems of a specific type and hide any changes. It exploited vulnerabilities in a Windows-based software program used in industrial settings. Most Stuxnet infections were detected in Iran; five organizations were specifically targeted. But since Stuxnet was able to

self-replicate, it also infected computers outside the target organizations and all over the world. Stuxnet is thus an example of a targeted attack that also resulted in a general attack. Stuxnet also demonstrated that it is possible to attack critical infrastructure, even infrastructure that is not connected to the Internet [3, 4].

- **Night Dragon**: In November 2009, an attack targeted at the energy sector (oil, power and petrochemical companies) was identified, which seemed to be originating from China and was given the name Night Dragon. The goal seemed to be to collect information related to competitive proprietary operations and financial details regarding field bids and operations [5].
- **Power outage** caused by hackers: In January 2008, several cities experienced power outage which was caused by hackers breaking into computer systems related to power supply. Little information about this incident is disclosed, such as in which regions the power outage happened, but the motive is said to be extortion [6].
- **Slammer**: The Slammer worm occurred in 2003 as a piece of malware exploiting a vulnerability in Windows Internet Information Server. Slammer infected a computer network at a nuclear power plant in Ohio, disabling a safety monitoring system for nearly five hours. At this power plant, they believed to have a firewall protecting against such types of attacks, which turned out not to be true. Fortunately, this incident did not cause any damage, because the plant actually was offline. But this was an early warning for what was, and is, yet to come [7].

10.5 Risk Analysis of ICT Infrastructure

Risk analysis is an important activity for those responsible for the security of ICT infrastructures. In the following, we provide some comments on the standard risk analysis applied to ICT before we describe a couple of methods for detailed analyses of ICT threats: *misuse case diag*rams and *attack trees*. Both these techniques are useful in risk assessments for identifying threats, but also for studying a potential incident in more detail. They improve understanding of the likelihood and consequences associated with a threat and help determine what types of countermeasures are most valuable. Similar types of modelling diagrams are used for other types of infrastructures, but misuse case diagrams and attack trees reflect the information security focus within ICT; they are concerned with protection of the ICT system, and their focus lies on deliberate attackers.

10.5.1 Standard Risk Assessment

There are standards available on how to perform risk assessments of ICT systems. One example is the ISO/IEC 27001-2005 standard [2] that provides guidelines for

Table 10.1 Issues to be addressed during a risk assessment of ICT—a checklist

External requirements	Organizational matters	Technical matters
Laws and regulations	ICT security policy	Access control
Standards	Responsibilities and authorities	Network architecture
Service level agreements with customers	Service level agreements with suppliers	Password policies
	System documentation	Physical security
	ICT security management	Remote access
	Security awareness	Patching
	Audit	Redundancy

information security risk management. The principles for risk assessments of ICT systems are similar to those of other infrastructures (cf. Chap. 3).

A risk assessment entails identifying the most important unwanted incidents corresponding to an organization's assets and determining the probability and consequences of each incident. Risks are often documented in a risk matrix, as described in Chap. 3. If the organization does not know which assets should be protected and from what, it is impossible to prioritize and design the appropriate security measures. This makes periodic risk assessment one of the most important activities related to information security. To ensure that all relevant risks to ICT systems are identified, it is important to engage the various actors who work with these systems in the risk assessment process (cf. Chap. 14). Table 10.1 provides a checklist that can be used during risk assessment to ensure inclusion of important aspects.

A risk assessment should at least include considerations on all issues mentioned in this checklist. Questions like "Do we have this in place? Is it up to date? How does it work in practice? Which threats apply? Does it cover our needs?" could be asked for each issue. Some issues might not apply, but such a fact should also be stated in the assessment report.

A common weakness of a risk assessment is that one only looks for expected vulnerabilities and threats. A way of mitigating this problem is by including personnel not working with ICT on a daily basis, in order to get some new perspectives. This could also be the best way to identify so-called black swans; incidents with quite low probability, almost out of the question, which will have severe consequences if they, against all odds, should actually occur.

10.5.2 Misuse Case Diagram

Both misuse case diagrams and attack trees can be used to study possible threats and attacks towards systems. They do not require any specific tools, and evaluations show that they are both quite easy to learn and use [8]. The modeller

however, will benefit from knowledge of typical ICT attacks, and thus, the best results are expected when information security experts are involved in the modelling.

Misuse case diagrams [9] are built based on knowledge of the functionality of the system. In the unified modelling language (UML), this functionality can be expressed as use cases; both in textual form and visually in use case diagrams. Use case diagrams visualize the main functionality of the system and the users of this functionality and are useful in getting an overview of the main workings of an ICT system. Misuse case diagrams add to this and also show how this functionality can be misused or attacked and who can be the source of such misuse (the attacker). Creating a misuse case diagram is in many ways a creative task where the security expert tries to "think like an attacker" and envision main ways that attackers may use the functionality of the system to their own advantage. The main steps are [9]:

- To identify the critical assets of the system (e.g. information or functionality of the systems) and their value
- To identify stakeholders that may intentionally harm the system and its assets, assess their motivation for performing an attack and identify the main steps needed to achieve their goals
- To identify potential countermeasures that can help prevent the attackers in achieving their goals

The modelling process is cyclical, in that the threats identified and the countermeasures used to prevent them can result in new assets that need to be protected. A simple example is the use of encryption to protect messages during transmission. This results in new assets; the encryption keys — that also are vulnerable and can be a potential attacker goal.

Figure 10.1 shows an example of a misuse case diagram that shows potential threats towards an ICT system that can be used to monitor offshore equipment and send electronic messages. The actor named "Operator" and the three white ovals constitute the use case diagrams used as a basis for the misuse case diagram. The use case diagram visualizes the main functionality and the main users of this functionality; in this case, it shows that the system is used by operators to monitor offshore equipment, and to send electronic messages, and also emphasizes that the messages are encrypted during transmission. In a misuse case diagram, the potential system abuse is added, in form of attackers (actors shown in black) and the abusive behaviour (black ovals). In this case, the diagram describes the following attacker goals: to disrupt monitoring, to send fake messages and to get access to messages. The above example is simple, and a real misuse case diagram for a real system is likely to include more users, describe more types of functionality, have more than one type of attackers identified and also describe more potential for misuse. Readers who would like to start using misuse case diagrams should look to a textbook or online resource on UML for descriptions of how to create use case diagrams. Then, the specifics of misuse cases are described best by [9]—the inventors of the misuse case extension.

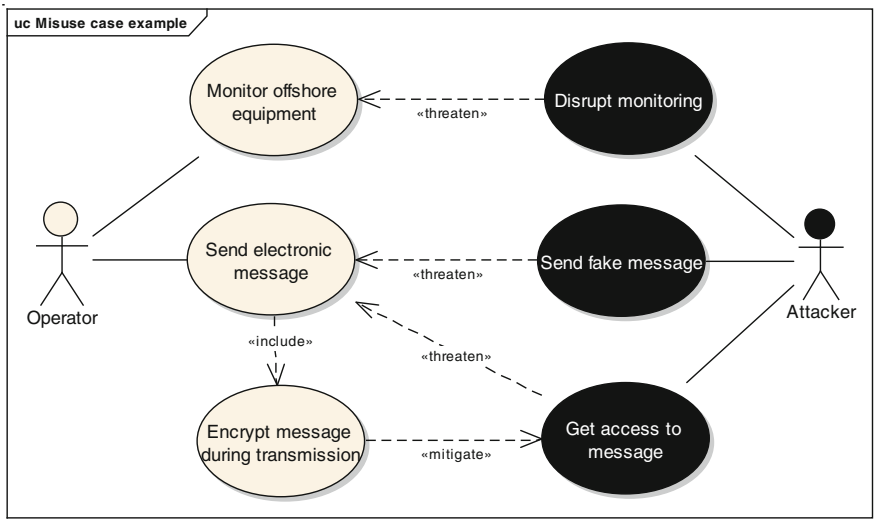

Fig. 10.1 Misuse case example

With misuse case diagrams, it is possible to visualize potential threats towards a system in a concrete way and show how the threats relate to the functionality of the system. It can also show how functionality of the system can reduce the risk associated with a specific type of attack; in Fig. 10.1, such mitigation comes in the form of message encryption that makes it harder for an outsider to get access to the message content. The strength of the misuse case diagrams lies in this close connection between system functionality and potential attacks. They are, however, best suited to describe systems and attacks at a high level, where the granularity of functionality and attacks does not result in too many "ovals" and "arrows".

10.5.3 Attack Tree

If there is a need to go into more details about how an attacker may go about in order to achieve an attack goal, it is better to use attack trees, as proposed by [10].

Attack trees aim at modelling security threats by focusing on the attackers and the different ways they may try to attack systems. An example attack tree is found in Fig. 10.2 showing how an attacker may try to make a network unavailable. In attack trees, attacks against a system are represented in a tree structure where the root node represents the attack goal. Branches in the tree represent the different paths an attacker can follow to achieve his or her goal. OR-nodes represent alternatives, while AND-nodes represent sub-goals where all must be fulfilled in order for the attack to be successful; note that in Fig. 10.2, the different branches are considered alternatives (OR-nodes) unless otherwise specified. The trees can be shown graphically or be written in textual form.

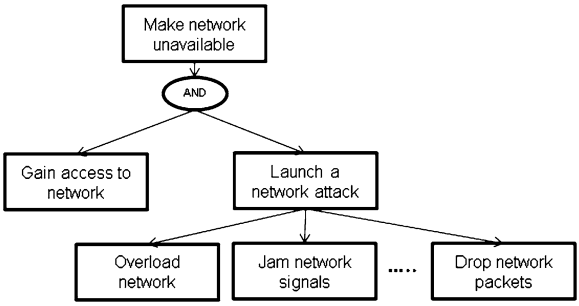

Fig. 10.2 Attack tree example

When constructing attack trees for a given system, one always starts with identifying attack goals. This can, e.g., be done through modelling misuse case diagrams or through identifying main assets of the system and potential attacks towards these assets. Each attack goal forms the root node of own attack tree. Then, the modeller tries to think about all ways an attacker can achieve these goals and adds them to the trees. As there is no way to ensure that all possible attack paths are covered, it is in general recommended that the resulting attack trees are given to someone else and that this/these person(s) continue to modify the trees. It is also possible to add more information to the nodes of the trees, e.g., by indicating whether an attack is possible or impossible or by assigning costs to each leaf node.

Attack trees are very similar to fault trees (cf. references in Appendix C), but have differences in notation and focus due to their use in different fields and for different purposes. Where fault trees aim at analysing failures to better understand their probabilities, attack trees are used to analyse the possible attack scenarios and identify the easiest ways into a system for an attacker.

10.6 Challenges when ICT is included in Risk Assessments of an Infrastructure

Even though the risk analysis methods used for ICT and other infrastructures are quite similar, there are some characteristics of ICT that typically complicate matters when ICT is included in cross-sectorial risk analyses. In the following, a few common challenges are discussed.

Information security aims to protect the ICT system itself, and the confidentiality, integrity and availability of the data that it contains. The consequences of information security incidents can therefore be perceived as less concrete than what is typically found with respect to safety (damage to life, health and the natural environment caused by the system) or reliability (loss of service), [11]. But this does not necessarily mean that the information security incidents are not important. Their importance, however, relies on what happens next, how the incident is handled and what are the motivations and skills of the attacker.

Determining the likelihood of information security incidents is commonly difficult due to a number of factors, including:

- Rapid changes in technology and threats
- Intentional acts
- Lack of available statistical data

The traditional risk analyses have been developed and used, e.g., in the nuclear power and the petroleum industry, to assess frequencies that are based on statistics and consequences of technical failures [11]. For ICT, such statistics are rarely available, and if they were, there would be good reasons to question their relevance. ICT has so far been characterized by rapid changes, both in technology and threats. Thus, historical data may be of little value. Also, security, as opposed to safety, fights a malicious attacker, and the motivation and skills of the attacker will have a major influence on whether an attack succeeds [11]. To further complicate matters, motivation may change overnight, e.g., due to political decisions. One example is the attacks [12] on the website of the Norwegian Nobel Committee after its decision in 2010 to grant the Peace Prize to the Chinese dissident Liu Xiaobo. Likelihood is thus really hard to predict. Usually, its approximate value is determined based on expert opinions, considering, e.g., the motivation and capabilities of attackers and current controls in place. But the likelihood estimates are usually at a lower level of precision than what may be expected within other infrastructures.

These challenges mainly represent problems that appear due to the nature of ICT systems and probably also their lack of maturity. The way that ICT is deeply integrated into other infrastructures is the main reason why several known techniques for addressing dependencies between the ICT and the infrastructures utilizing ICT may not work.

10.7 Recommendations for Inclusion of ICT in Cross-Sectorial Risk Analyses

To address the above-mentioned challenges of consequence comparison the following actions are recommended:

- Increased cross-domain cooperation during risk identification and estimation of consequences.
- Create an overview of the role of ICT in the value chain.

Since information security incidents often are at a different level than critical infrastructure disruptions, it is important that people with information security expertise and domain experts with safety or reliability expertise work together to identify ICT's role in the total risk picture (cf. Chap. 14). When potential critical infrastructure failures have been identified, information security experts should be

asked if ICT can be a contributing factor. The same way, when information security incidents have been identified, domain experts should be asked whether this may cause critical infrastructure failures (cf. Chap. 14). However, to be able to understand how ICT incidents can influence the environment, it is necessary to create overviews of the role of ICT, showing how the information and functionality of ICT is used and for what purposes.

When it comes to likelihood estimations, it is important to create an understanding of the relevance (or irrelevance) of historical data when it comes to ICT incidents. The importance of ICT should not be considered low due to lack of historical evidence of serious incidents with a root in ICT systems. Still, information security experts should be required to provide arguments for their likelihood estimates.

10.8 Conclusion

ICT has become an integral part of critical infrastructure. As a consequence, it is of paramount importance that the role of ICT is understood and taken into account when managing risk of such infrastructure. A key success factor in this respect is to increase cooperation between experts on ICT and experts on the technologies that utilize ICT for provision of critical services.

References

1. Hilbert, M., & López, P. (2011). The world's technological capacity to store, communicate, and compute information. *Science*, *332,* pp. 60–65. http://www.sciencemag.org/content/332/6025/60.abstract.
2. ISO/IEC. (2005). *Information security management systems–requirements*. ISO/IEC 27001: 2005.
3. Albright, D., Brannan, P., & Walrond, C. (2010). Did stuxnet take out 1000 centrifuges at the Natanz enrichment plant? *Institute for Science and International Security*, 22 Dec 2010. http://isis-online.org/uploads/isis-reports/documents/stuxnet_FEP_22Dec2010.pdf.
4. Albright, D., Brannan, P., & Walrond, C. (2011). *Stuxnet Malware and Natanz: Update of ISIS 22 Dec 2010 report*. Institute for Science and International Security, 15 Feb 2011 http://isis-online.org/uploads/isis-reports/documents/stuxnet_update_15Feb2011.pdf.
5. McAfee® Foundstone®. (2011). *Professional Services and McAfee Labs™ (2011) Global Energy Cyberattacks:* "*Night Dragon*", 10 Feb 2011. Available at: http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf.
6. Computerworld. (2008). *CIA says hackers pulled plug on power grid*, 18 Jan 2008 http://www.computerworld.com/s/article/9057999/CIA_says_hackers_pulled_plug_on_power_grid.
7. Poulsen, K. (2003). *Slammer worm crashed Ohio nuke plant network, SecurityFocus*, 19 Aug 2003 http://www.securityfocus.com/news/6767.
8. Meland, P. H., Tøndel, I. A., & Jensen, J. (2010). Idea: Reusability of threat models–two approaches with an experimental evaluation. Lecture Notes in Computer Science, 2010, Vols. 5965/2010, pp. 114–122.

9. Sindre, G., & Opdahl, A. L. (2005). Eliciting security requirements with misuse cases. *Requirements Engineering, 10*(1), 34–44.
10. Schneier, B. (Dec 1999). "Attack Trees". *Dr Dobb's Journal*, 24(12). Archived from the original on 6 August 2007. http://www.schneier.com/paper-attacktrees-ddj-ft.html. Retrieved 2007-08-16.
11. Line, M. B., Nordland, O., Røstad, L., & Tøndel, I. A. (2006). *Safety vs. security? In Proceedings from Probabilistic Safety Assessment and Management* (*PSAM*), New Orleans. ISBN 0-7918-0245-0.
12. The Register. (2010). *Hackers plant firefox 0-day on Nobel peace prize website*, Oct 26, 2010. http://www.theregister.co.uk/2010/10/26/firefox_0day_report/.
13. Jaatun, M. G., Albrechtsen, E., Line, M. B., Tøndel, I. A., & Longva, O. H. (2009). A framework for incident response management in the petroleum industry. *International Journal of Critical Infrastructure Protection, 2*, 26–37.

Chapter 11
Risk-Based Design of Maritime Transport Systems

Bjørn Egil Asbjørnslett, Inge Norstad and Øyvind Berle

Abstract This chapter provides an approach to modelling and analysis of supply chain vulnerabilities due to physical and functional interdependencies in maritime transport systems. The results of the analysis are risk of supply breaches of the commodities transported by the system. The risk analysis is set into the context of development of infrastructure for maritime transport systems, where industrial shipping systems are used as an example. The risk analysis is used to balance the scale of the system's infrastructure against an assessment of the requirements and vulnerabilities of the system's dependents. The maritime transport system is here regarded as a critical infrastructure for supply of required commodities into a region.

11.1 Introduction

The maritime transport system is the backbone of international trade and supply chains, moving approximately 80 % of global trade measured in tons [1]. Therefore, interruptions in the maritime transport system have the potential to create disturbances in many dependent supply and distribution chains covering industrial and societal demands.

A challenge in design of most major systems, including critical infrastructure systems, is to make the best use of the system resources in producing the product or services that is required in an industrial or societal context. For transport systems, this means to optimize the system structure, scale of resources and operational use of

B. E. Asbjørnslett (✉) · Ø. Berle
Department of Marine Technology, NTNU, Trondheim, Norway
e-mail: bjorn.e.asbjornslett@ntnu.no

I. Norstad
MARINTEK, Trondheim, Norway

P. Hokstad et al. (eds.), *Risk and Interdependencies in Critical Infrastructures*, Springer Series in Reliability Engineering, DOI: 10.1007/978-1-4471-4661-2_11,

the resources so that they are best fit to cover the required demand for transport work services, without undue use (waste) of transport infrastructure and resources. This could be achieved through optimization-based analysis and planning approaches, with a cost minimizing objective function. However, due consideration should be taken to contingencies that could affect the system and how interdependencies within the system and with other systems have affected. The approach presented here addresses this.

Some parts of maritime transport system infrastructure are part of other supply chains, for instance fairways, ports and terminals. Vessels could also be part of several supply chains. Lack of access to such infrastructure due to contingencies in other types of shipping is an example of geographical interdependencies found in maritime transport systems. If optimization of the system design and system resources is done uncritically, overlooking the risks that could make the optimized system design fail under given conditions or events, the result could be cascading effects throughout a wide range of supply chains, affecting several industrial and societal dependents.

Risk in cargo transport chains, and the related vulnerability of industries and societies, was brought up by the World Economic Forum as an emerging global risk [2] and restated as an area needing further attention [3]. Hence, optimization as a measure to improve cost effectiveness of transport resources such as vessels, ports, terminals and storage could become a design-based hazard for risk and vulnerabilities that affect larger systems due to functional interdependency and should be "stress-tested" against such scenarios [4].

11.2 Maritime Transport Systems

Maritime transport systems can be grouped into three types of shipping systems: tramp shipping, liner shipping and industrial shipping. In tramp shipping, the vessels sail and transport cargo in a not pre-defined order, based on a mix of contractual and spot cargo. In liner shipping, the vessels sail and transport cargo in pre-defined routes with pre-defined schedules. In industrial shipping, the vessels are part of a specific industrial development, as part of the supply and distribution chain infrastructure. An example of industrial shipping is for instance liquefied natural gas (LNG) carriers transporting LNG from the liquefaction plant to customers at given geographical locations. Such LNG transport is part of regional energy supply and hence regional energy security. The focus in this chapter will mainly be on industrial shipping.

A maritime transport system is a network-based system built up of nodes of ports and terminals, with sea transport as the transport mode between the network of ports and with other transport modes covering the hinterland transport behind each port and terminal. As such, a maritime transport system stretches from the hinterland behind the loading port (export) to the hinterland behind the unloading port (import).

Due to the increasing globalization of industries, supply chains has grown longer, with several transfer points between modes and with several possible choke points,

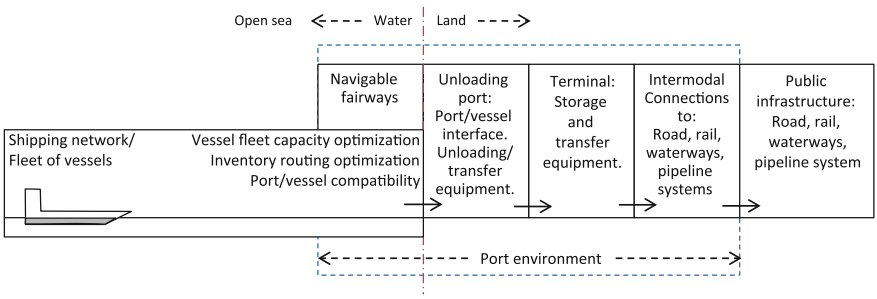

Fig. 11.1 A port vessel interface model, where the interface is optimized with respect to vessel usage and inventory routing in keeping a balanced inventory between outbound and inbound cargo inventories

both on land and at sea. On land, the port infrastructure itself is a choke point that may get reduced throughput capacity due to several failure modes [5], but also hinterland logistics may be sources of reduced throughput capacity from sea to land, for instance, if there are few alternative transport channels into the port and one of them are choked. At sea, navigable waterways into the port often go through narrow fairways, often with dense vessel traffic, and narrow straits and canals can become choke points due to physical restrictions or, as seen lately, due to man-made malign actions as piracy. As such, the choke points in a maritime transport system can become scarce resources for the total transport work capacity of the system.

Some terms and concepts related to maritime transport systems can be found in [6]; a cargo is a set of goods shipped together from a single origin to a single destination; a load is the set of cargoes that is on the ship at any given point in time—a load is considered a full shipload when it consists of a single cargo that for practical and/or contractual reasons cannot be carried with other cargoes; a loading port is a pickup location (corresponds to a pickup node); an unloading port is a delivery location (corresponds to a delivery node). In this chapter, we will address cargo shipments from loading port to unloading port, without emphasizing whether the load being multiple cargoes or full shiploads.

Figure 11.1 illustrates a general interface between sea and land in a maritime transport system. The focus is set on the functions that must be available for the vessel port interface to support the cargo transport function of a maritime transport system. The vessel port interface is optimized with respect to utilization of the vessel fleet and securing the inventory balance in outbound and inbound storages.

11.2.1 Annual Delivery Plan in Industrial Shipping

Figure 11.2 illustrates a general industrial shipping network with a single loading port and several unloading ports. This is a typical example of an industrial shipping system where there is one producer in the system and a set of demand points

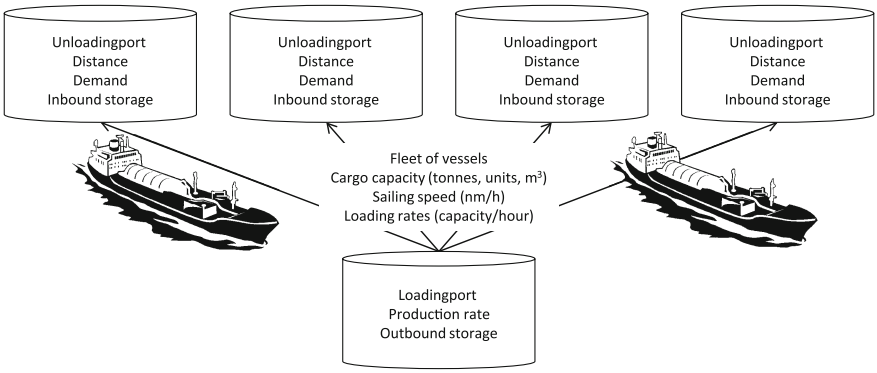

Fig. 11.2 A network structure of an industrial maritime transport system with a single port of loading (POL), several ports of discharge (POD) and a fleet of vessels transporting cargo from the POL to the PODs

(customers) being supplied with cargo by the industrial shipping system. In general, this is a network model with one supply node and several consumption nodes, and a fleet of vessels servicing the nodes securing that the balance between supply and demand is kept intact.

An industrial shipping system is often planned and optimized to realize an annual delivery plan (ADP) at minimum cost, under the constraints that the outbound storage in the loading port is not filled up so that production have to be reduced or stopped, or that the inbound storages in the unloading ports do not run empty.

A risk analysis should be part of this assessment to secure that the system infrastructure design is not optimized in a way so that contingencies would result in underperformance versus the ADP and lead to supply breach–related vulnerabilities for the system dependents.

11.3 Risk Analysis Approach

The scope of the maritime transport system's risk analysis is to assess the system's ability to keep up the throughput of cargo from outbound hinterland area, through loading port, via the sea transport leg, and through unloading port into the inbound hinterland area. The risk approach is as such primarily taken from an industrial or societal point of view which is the vulnerability of having supply shortage of required input factors. A flow chart of the risk analysis process is shown in Fig. 11.3, with a description of each step.

The risk analysis approach is based on four steps, with two alternative routes through the risk analysis flow chart. Choice of route is dependent on whether analytical tools for transport system optimization and routing and scheduling will be used or not. Optimization and simulation tools applied for such analysis are seldom directly commercially available. The basic software may be available, but the

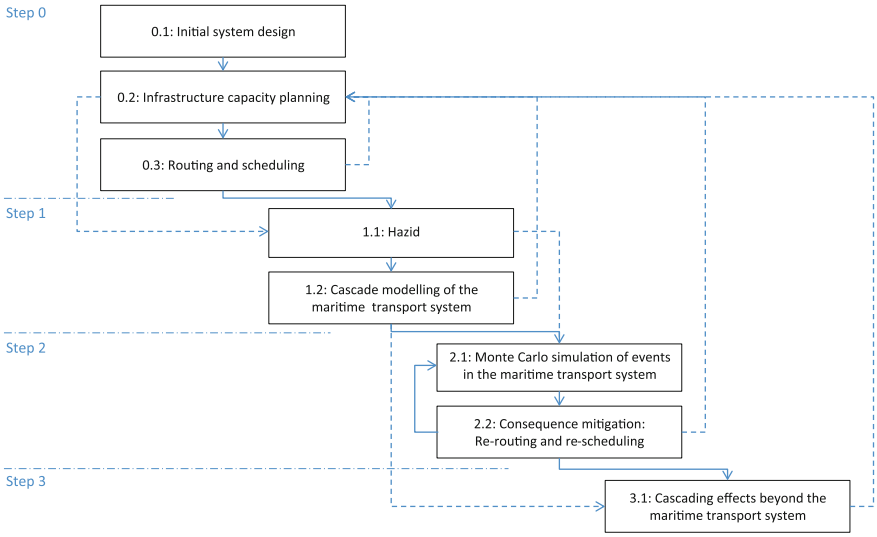

Fig. 11.3 Flowchart of the maritime transport system design risk analysis approach

specific analysis model will have to be modelled and programmed in the analysis software. Such software will often have rather strict user requirements. The software applied in these studies is TurboRouter for vessel routing and scheduling, with the Invent add-on if inventory routing is required. All steps have feedback loops to '0.2 Infrastructure capacity planning' for infrastructure configuration adjustments.

Step 0 is an initial system design step, where the scale of the system's infrastructure, for instance number of vessels and capacities of loading equipment and storages is determined based on a deterministic assessment. The non-optimization-based route will after Step 0.2 proceed directly to the hazard identification in Step 1.1. The output from Step 0 is the system's deterministic supply capacity.

Step 1 is the preliminary hazard analysis phase and rough risk assessment, with the cascade modelling approach as presented in Chap. 4 as a starting point for the supply risk assessment. If a detailed, optimization-based risk assessment is wanted or required, the cascade modelling in Step 1.2 can be omitted, and one can proceed directly from the hazard identification in Step 1.1 to the simulation in Step 2.1. Omitting the cascade modelling step is something that we do not recommend, as the cascade modelling will contribute to better insight into the relationships and interdependencies of the transport system and could in an iterative process support the hazard identification. The cascade modelling should therefore be conducted through the qualitative interdependency modelling. The depth of the cascade modelling into a full quantitative assessment may be restricted if a detailed simulation and optimization study shall be performed in Step 2. If Step 2 is omitted, then a quantitative cascade modelling according to the principles described in Chap. 4 should be performed. The output of Step 1 is a rough to semi-detailed assessment of the risk of supply breaches from the maritime supply system.

Step 2 is a detailed risk assessment of supply breaches of the maritime transport system. The Monte Carlo simulation in Step 2.1 is based on the likelihood of given contingencies defined in Step 1.1 maturing, and the impact these contingencies will have on the total transport system is given by the system interdependencies as modelled in the routing and scheduling optimization model. The objective function is set to maximize the delivered quantity of the commodity transported through the transport system. When a contingency matures, Step 2.2 will dynamically perform mitigating actions by re-routing and rescheduling vessels, so that the system seeks to maximize the throughput of cargo given the contingency. The simulation continues based on the new situation after the mitigating actions. The output from Step 2 is a detailed assessment of the risk of supply breaches from the maritime transport system, given different configurations of the system scale.

Step 3 is a vulnerability analysis where the focus is the vulnerability of the dependents of the maritime transport system, due to risk of supply breaches in the transport system. The cascade modelling approach is a good candidate to use for such assessment or alternatively a vulnerability analysis as presented in [7].

Adjustment of the scale of critical infrastructure in the maritime transport system could be made as a result of Step 0.3, Step 2.2 or Step 3.1.

11.3.1 Step 0: System Design and Infrastructure Capacity

A good transport system is a resource effective transport system, which means that waste of resources is minimized. This requires that all design and improvement efforts of a transport system have structure and resource optimization as part of the improvement approach. This starts with seeking to minimize the infrastructure required, for instance, vessel resources and storage capacities to meet the defined demand for transport work in the transport system.

The first step is the system design stage, including strategic capacity optimization of the vessel fleet, storage infrastructure and loading equipment. The output from the first step is a deterministically optimal or feasible start capacity of system infrastructure consisting of outbound and inbound storage capacities, loading and unloading capacities, and size and mix of vessels in the vessel fleet. Fleet size and mix problems are deciding which given types and numbers of vessels are best fitted for a given scope of transport work.

The result from this step is a feasible maritime transport infrastructure adapted to perform the required transport work in a cost effective way. The optimization part of this step could also be omitted, and an iterative approach where the starting point of infrastructure could have been a given, feasible fleet of vessels and storage capacities and where the infrastructure are adjusted based on the resulting probability for supply breaches after steps 1.2, 2.2 or 3.1 of the analysis.

When a fleet of vessels are defined, either by a fleet size and mix optimization approach or by starting with an established fleet of vessels, the vessels must be assigned to routes and set into a schedule. Routing is the assignment of a sequence

of ports to a vessel, while scheduling is assigning times or time windows to the various port calls on a ship's route [6].

In an industrial shipping system as presented in Fig. 11.2, the storage and inventory management requirements must be taken into account. This requires an inventory routing approach, meaning that the routing should be optimized to achieve a minimum level of operational costs, without breaching storage constraints. A more thorough description of an inventory routing model for an industrial shipping system can be found in [8], describing a set of transport system internal interdependencies in a four-stage model: (1) routing—the objective function with cost minimization to assign given vessel to given routes, (2) loading and unloading—securing that loading and unloading are being performed in a correct order, (3) scheduling—control the scheduling on given routes and prevent overlap of vessels in port and (4) inventory management—securing that the inventory level in each port is kept within upper and lower limits.

The resource planning step performs an inventory routing routine to optimize the assignment of vessels to routes and scheduling of the vessels so that the supply capacity of cargo through the system is maximized, without breaching the upper– and lower-level bounds of the outbound and inbound storage requirements. The objective function for the system optimization is therefore seeking to maximize the system's transport of cargo from the supply side (loading port) to the demand side (the set of unloading ports).

However, optimization contribute to moving a system's characteristics, as well as operational requirements in a way that make the system couplings more tight and the system interactions—to secure best system throughput, more complex. That should be acknowledged and dealt with, before inherent contingencies mature into incidents for which the system is vulnerable and which have cascading consequences beyond the system limits. The inventory routing optimization of the vessel fleet given the cargo storage requirements will result in less slack and tighter coupling which could be seen as a type of spatial interconnectedness, with inherent dynamic interdependencies.

The output from Step 0.3 is a check of whether the fleet of vessels found in Step 0.2 is capable of meeting the demand for transport work, when set into the detailed system context with all system requirements. If it is not feasible to produce the transport service with the initial resource configuration set in Step 0.2, adjustments should be made of the system resource configuration.

11.3.2 Step 1: Hazard Identification and Interdependency Modelling

Given that we now have checked that our maritime transport infrastructure deterministically is capable of producing the required transport services, it is time to list potential contingencies that could be related to the transport system infrastructure and lead to breaches in the production of transport work, violate the ADP

and mature vulnerabilities for the system's dependents. A supply chain–focused hazard identification and scenario development process as described in [7] could be used for this hazard identification process.

A maritime transport system is a coupled system where a set of infrastructure elements either store or transfer cargo along a supply chain. Interdependencies among these infrastructure elements affect the transport system's ability to secure the transfer of cargo along the supply chain given contingencies related to the transport system infrastructure.

When a vessel arrives in loading port, it requires access to a berth where it can dock. Then, the cargo loading equipment in berth must be available to hook-up to the vessel so that the cargo transfer process can commence. Further, for the cargo transfer to begin, the commodity must be available in the outbound storage in a minimum quantity to fill up the cargo holds of the vessel. When the vessel is loaded, the loading equipment can be uncoupled and the vessel is ready to navigate out of port of loading into a navigable fairway towards the unloading port. A navigable fairway is the "road on water" where a given vessel can navigate safely. When the vessel reaches the unloading port, it needs to await access to a berth to be able to dock. Then, the unloading equipment in the berth must be in operation, and there must be inbound storage available to store the cargo from the vessel. Finally, the vessel itself should be considered a critical infrastructure in such a transport system. The vessel is an infrastructure that is exposed to hazards and threats of both internal and external origin and could itself be a hazard both to its own system and to other systems.

Below a further description of contingencies related to loading port, navigable fairways, unloading port and the vessel is presented.

Loading port: A main issue in POL is the throughput mechanism of transferring cargo from land to sea. In a system set-up as described here, the loading port will often be a bottleneck, and capacity lost in a bottleneck is capacity lost for the system as a whole. As such, the loading port and the processes managing it must secure a balanced out-take from the outbound storage against the inflow of cargo to the outbound storage. This requires a steady ordering of vessels into loading port so that no available berth space—physical and time related—is wasted as capacity to transfer cargo.

Navigable fairway: A navigable fairway can become a non-navigable fairway if there is a blockage of or hindrance in the fairway. A blockage or hindrance could be due to several causes. First, an object that is placed in the fairway in such a way that it is not possible to navigate around the object or that the capacity of the fairway is strongly restricted due to extra navigation required around the object or sailing another fairway. The most likely situation of such temporary objects blocking or hindering the passage of a fairway would be related to a vessel that is stuck in the fairway after a vessel-related accident, as for instance the Port Arthur accident in Texas in 2010. Another case could be fairways that are non-physically blocked, but where the functional consequence would be the same. Examples of such could be regulatory or politically based closures of fairways, or even war-related closure, of which the best known example is the closure of the Suez Canal.

Table 11.1 Contingencies in maritime a transport system

Part	Description
Loading port	Contingencies mainly related to input to the port, for instance reduced production to feed the port storage, reduced cargo in storage in the port, berth unavailability, loading equipment not functioning or access to port restricted
Sea transport	Contingencies mainly related to fairway bottlenecks as for instance blocked canals, piracy or vessel-related events like breakdown in vessel systems or maritime accidents setting the vessel out of service temporarily or permanently
Unloading port	Contingencies mainly related to port access restricted, berth unavailability, loading gear not functioning, storage unavailable or hinterland transport capacity restricted

In addition, piracy has again become a threat that has led many ship owners to abandon shortest route fairways to sail longer-distance fairways with no or lower piracy activity—leading to reduction in transport work capacity.

Unloading port: The unloading port is the regional access point for the supply chain. As such could any event related to blocking or capacity restrictions in the navigable fairway into unloading port, the port itself or the berths, the unloading equipment or the inbound storage, and even the hinterland transport systems lead to breaches in cargo supply capacity. The United States west coast port worker strike and lockout in 2002 is an example of a contingency affecting and blocking a whole network of ports.

Vessel: The port systems are fixed systems for which restrictions in their throughput capacity or capability of cargo could have major regional impacts. For the shipping networks, there is flexibility to charter in additional vessels in case of shortage of transport capacity, or re-routing to cover changes in supply–demand relations. However, this flexibility differs between different shipping systems, vessel types and cargo types, and especially for some types of industrial shipping systems of dedicated cargo types, there could be limited flexibility.

The contingencies in maritime transport systems could be summarized as in Table 11.1.

11.3.2.1 Cascade Modelling

Hazard identification is a starting point for further interdependency risk modelling. The cascade modelling approach (cf. Chap. 4) has the benefit of enabling rather swift modelling and assessment of risk in a maritime transport system's supply capability and at the same time contributes to enhance the understanding of system interdependencies, all in a transparent way.

Cascade modelling of maritime transport system interdependencies could in general be explained through the process presented in Fig. 11.4. Any maritime transport chain has contingencies related to the outbound infrastructure, the vessels, the fairway infrastructure, the network of ports, the inbound infrastructure and the interdependencies among these infrastructure elements. The outbound

infrastructure would cover for instance outbound storage, cargo trans-loading equipment, berths and port access. The vessel itself as an autonomous construction and operation could be affected by contingencies within itself, as for instance unplanned maintenance need, or of external origin as for instance collision with another vessel. Fairway contingencies should also be seen in relationship with the vessel. The inbound contingencies will be equal to the outbound contingencies.

Cascade modelling and analysis of the maritime transport system, from cargo export to loading port, until effect on supply capacity (cargo import) in unloading port could be described as follows. To assess the total risk for the cargo supply capacity into the set of unloading ports from a "cargo export" contingency, we first move from left to right in the cascade diagram to estimate the contingent probabilities for succeeding events, based on the extent and duration of the preceding event. Both the extent and duration of a cargo export event would increase the probability of events related to the other outbound infrastructure such as storage, loading gear, berths and other port systems. Restrictions in "cargo export" would lead to queuing of vessels within the port area, and an increasing extent of vessel queuing would lead to increased risk for vessel–vessel encounters (collisions). The loading equipment would after mitigation of the "cargo export" event be required to be used more intensively to recover from the lost time and could hence be more prone to technical failure due to "over-use".

There is one event box in Fig. 11.4 that requires specific attention and that is the "Environment" box. A vessel could be part of contingencies for all parts of the infrastructure, and when a vessel is involved, for instance in a collision in port, there could be spills of bunker oil or cargo that could lead to environmental consequences. If such spills/environmental consequences are present, the transport capacity consequences of the contingency will be higher, due to additional required time to clean-up the spill.

Given now that we have the probability for "cargo import" (supply) breaches, due to the starting "cargo export" event, we can calculate backwards through the cascade diagram to find the total risk for the transport system from the "cargo

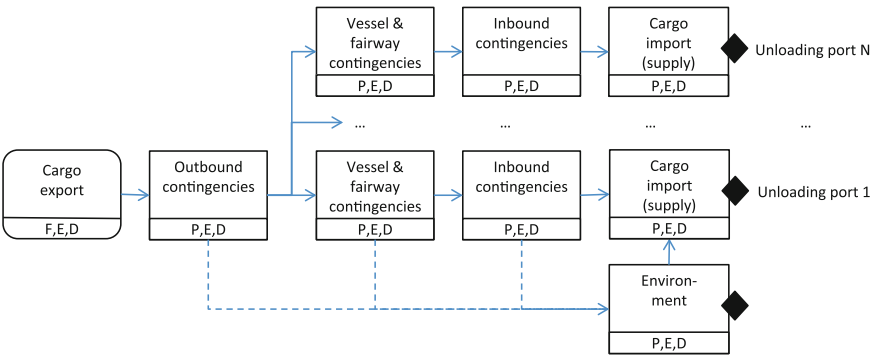

Fig. 11.4 A generalized cascade diagram for a maritime transport system, with one loading port and a number of N unloading ports

export" event. This could then be repeated with the succeeding stages of the supply chain as starting point for the cascade modelling, hence establishing a full risk picture for the transport system.

The total risk for the transport system calculated through the cascade model could then be assessed for different infrastructure configurations to find an acceptable risk level for supply breaches for the transport system and hence support a rough risk-levelled configuration of the transport system infrastructure.

Several vessels call at a port, so that from an outbound port several vessels will sail to several inbound ports. Hence, the earlier in the chain a contingency matures, the more global the consequences will be. This is illustrated in the cascade diagram where several "vessel/fairway" paths towards several unloading ports are following from the "outbound contingencies" box.

Hence, the cascade modelling approach could be used both qualitatively to gain understating about relationships and interdependencies in the transport system and quantitatively to make a semi-detailed risk picture of the transport system's transport capacity risk. However, there is one aspect that the cascade model will not be able to capture, and that is the internal interdependencies among the vessels and network of ports in the transport system, and even more so if there is a question of storage requirements to adhere to. To be able to make full account of such internal interdependencies, a simulation set-up around a vessel routing or inventory routing model has to be used. This is addressed in Step 2.

11.3.3 Step 2: Contingency Analysis—Simulation and Dynamic Mitigation

The fourth step performs an integrated risk assessment and risk mitigation procedure, based on simulation of an ADP for the transport system. As input to the process, the hazard identification from the previous step is used to define contingencies that could threaten the supply robustness of the transport system. The contingencies are given as input into a routing and scheduling model, and a Monte Carlo simulation process is performed.

Mitigation measures could be found in two ways:

1. Adding more resources to the infrastructure, making it more robust.
2. Using in-built flexibility in the system.

In the simulation process, both of these measures for mitigation of supply breaches could be applied. To test the mitigating effect of added resources, the simulation can be performed with a set of different system infrastructure configurations. For a maritime transport system, such could be different number of vessels, or the size or speed of the vessels, different cargo loading and unloading rates between port storage and vessel, as well as different storage capacities in loading and/or unloading port.

A more interesting mitigation feature is to understand how the in-built flexibility in a system could be exploited to hedge supply breaches. Maritime transport systems are based on the use of vessels as primary transport mode, and vessels are a quite flexible infrastructure element, as vessels can sail wherever there are navigable fairways, and call any port with which the vessel is compatible. Compatibility in this sense means that the vessel has physical characteristics—such as overall length, width or draft that the port can handle, and suitable cargo trans-loading equipment.

During the simulation, flexibility measures are exploited by re-routing and rescheduling the vessels whenever a contingency matures. The simulation process is performed so that whenever a contingency occurs, the procedure in the simulation set-up is that the system will be asked to check whether the consequences of reduction in transport capacity due to the contingency can be mitigated by re-routing and rescheduling the vessels for the remaining period of the ADP taking the contingency into account.

The output of the third stage is therefore a simulated distribution of system supply capacity for alternative system infrastructure configurations, for the system as a whole and per unloading port for an ADP.

11.3.4 Step 3: Interdependencies and Vulnerabilities Beyond the Maritime Transport System

The focus of this interdependency risk analysis is the transport system's mission to keep up the transport capacity and meet the demand requirements in each unloading port, so that the cascading effects of maturing contingencies in the transport system do not breach the annual cargo delivery commitments and mature vulnerabilities for the dependents of the transport system.

The cascade diagram with the approach described in Chap. 4 could be used both as an overall starting point for a transport system interdependency study and as a concluding phase of a study. For the latter, the cascade modelling approach could take the results from for instance a simulation study as presented here and utilize the results to estimate cascading effects for industrial and societal dependents of the transport system.

The analysis has this far established an estimated distribution of cargo throughput capacity. Hence, we should now assess the risk of the dependents of the transport system, due to restrictions in inbound cargo supply. Figure 11.5 illustrates this.

The hinterland transport and user context are more linear than the vessel/port network context of the maritime transport system, so the cascade modelling approach would be a better approach in this part of the supply chain than in the network dependent maritime transport system. The modelling approach should follow the principles as presented in Chap. 4.

The ultimate consequence of reduction in cargo supply is that both industries and societal functions could be affected due to lack of input factors. The effect will

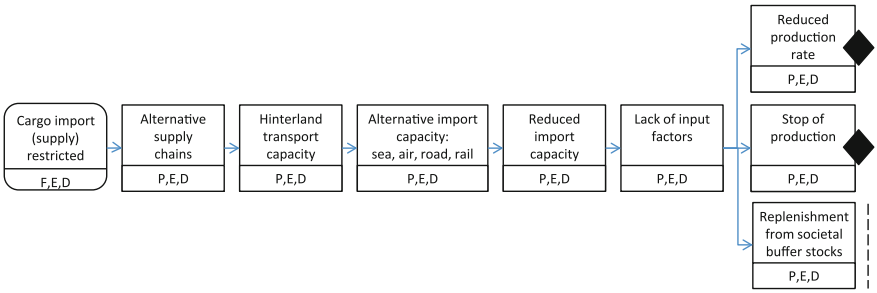

Fig. 11.5 A cascade diagram illustrating the interdependence between restrictions in cargo import and societal vulnerability, under the presence of alternative transport channels

be dependent on feasibility and availability of the set of alternative supply chains that could mitigate the lapse of a supply chain. Whether an alternative supply chain is a feasible mitigation alternative is dependent on the hinterland transport capacity and the capability and capacity of connecting to alternative import sites. To assess such a chain of interdependent events is fit for the cascade modelling approach.

11.4 Conclusions

This chapter has suggested an approach to bringing risk analysis into the infrastructure design process of maritime transport systems. This contribute to a risk-based assessment of the configuration of the transport system infrastructure, hopefully making it more robust to cope with contingencies that could lead to serious supply breaches if not dealt with properly in the design phase. Industrial shipping systems are for instance an example of a type of system design that would benefit from such an approach for proactive treatment of system-based risk.

Combining the interdependency modelling and the cascade approach provided in Chap. 4, with in-depth simulation and analysis would meet the demand for treatment of risk. Mitigating measures could take both infrastructure configuration and flexibility measures through event-based re-planning into account.

Hence, most importantly, both the cascade modelling approach and the simulation and optimization approach could be used to make a risk-based assessment of the configuration of the transport system infrastructure against the vulnerability exposure for the transport system's dependents. The main question is about the level of detail that is required and the requirement to assess the inherent and dynamic interdependencies in the vessel and port network configuration. If the latter is important, then a vessel routing and scheduling model would be required.

Chapter 12 provides an example of the described approach for a maritime transport system for LNG.

References

1. UNCTAD. (2011). Review of maritime transport, UNCTAD/RMT/2011, United Nations Publication, ISBN 978-92-1-112841-3, Geneva.
2. WEF. (2008). Global risks 2008: A global risk network report, Geneva, Switzerland: World economic forum.
3. WEF. (2012). Global risks 2012: A global risk network report, Geneva, Switzerland: World economic forum.
4. Berle, Ø., Asbjørnslett, B. E., & Rice, J. B. (2011a). Formal vulnerability assessment of a maritime transportation system. *Reliability Engineering and System Safety, 96*, 696–705.
5. Berle, Ø., Rice, J. B., & Asbjørnslett, B. E. (2011b). Failure modes in the maritime transport system: a functional approach to throughput vulnerability. *Maritime Policy and Management, 38*(6), 605–632.
6. Christiansen, M., Fagerholt, K., Nygreen, B., & Ronen, D. (2007). Maritime transportation. In C. Barnhart & G. Laporte (Eds.), *Transportation, handbooks in operations research and management science* (Vol. 14, pp. 189–284). Amsterdam: Elsevier Science.
7. Asbjørnslett, B. E. (2008). Assessing the vulnerability of supply chains, in supply chain risk: A handbook of assessment, management, and performance, G.A. Zsidisin & B. Ritchie (eds.), pp.15–33, Springer.
8. Christiansen, M., & Fagerholt, K. (2009). Maritime inventory routing problems. In: C. A. Floudas & P. Pardalos (Eds.), Encyclopedia of optimization (2nd ed.), pp. 1947–1955, Heidelberg, Springer.

Chapter 12
Risk of Supply Breaches in Maritime LNG Transport

Bjørn Egil Asbjørnslett, Inge Norstad and Øyvind Berle

Abstract This chapter presents a case study based on the approach described in Chap. 11. The case is a maritime transport system for distribution of liquefied natural gas, liquefied natural gas (LNG), from a producer to a set of receiving terminals in different geographical regions. The objective is to provide an example of modelling and analysis of interdependency risk in maritime transport infrastructure and potential-related vulnerabilities, where the transport system is part of a tightly coupled energy supply system. The main focus is given to the interdependency risk assessment of supply breaches of LNG based on detailed inventory routing–based simulations. Interdependency modelling and assessment based on the cascade model presented in Chap. 4 is discussed at the end.

12.1 Introduction

Sea transport plays an important part in the global energy market, transporting major energy carriers, such as crude oil, coal and natural and petroleum gases. Some of these maritime transport systems are highly market based, for instance crude oil and coal, with high liquidity in both vessel markets and production and consumption markets. Other maritime energy transport systems are industrial, meaning that they are designed as part of a specific industrial development, for instance maritime transport systems for liquefied natural gas (LNG). In natural gas

B. E. Asbjørnslett (✉) · Ø. Berle
Department of Marine Technology, NTNU, Trondheim, Norway
e-mail: bjorn.e.asbjornslett@ntnu.no

I. Norstad
MARINTEK, Trondheim, Norway

P. Hokstad et al. (eds.), *Risk and Interdependencies in Critical Infrastructures*, Springer Series in Reliability Engineering, DOI: 10.1007/978-1-4471-4661-2_12,

distribution terms, sea transport of LNG could be seen as a floating pipeline system continuously replenishing a consumer with natural gas. However, the infrastructure of the LNG supply chain is costly, so there is a considerable potential for cost-effectiveness in optimizing the supply chain infrastructure investments.

This chapter presents a case study based on the approach described in Chap. 11. The case has relevance both for modelling and analysis of industrial maritime transport systems in general, as well as for intermodal supply chains where maritime transport is one of several transport modes.

The chapter proceeds with a description of the maritime LNG transport system, followed by a nominal and a deterministic assessment of infrastructure capacity, before transport system infrastructure contingencies are addressed and a risk-based assessment of system capacity is made for a set of transport system infrastructure configurations. Finally, a comment about the interdependency cascade modelling in such systems is made, with a discussion of the results obtained.

12.2 The LNG Maritime Transport System

LNG is first and foremost a storage and transport mode of natural gas. The LNG supply chain requires use of a maritime transportation system to bring the liquefied gas from producer to consumer. After the liquefaction process, the produced LNG is transferred into outbound storage. The outbound storage capacity is a physical limitation in the system, which eventually stops the production of LNG if the storage is not "emptied" periodically requiring a steady inflow of empty LNG vessels to load. From the outbound LNG storage, the LNG is brought through pipeline systems and loading equipment in loading port onto LNG vessels docked at berths in port. Thereafter, the LNG vessels transport the LNG through a navigable fairway to unloading port. When the arriving LNG vessel is given access to a berth, the vessel can berth and hook-up to the loading equipment to start discharging her LNG cargo. The LNG is then transferred to inbound storage. The LNG supply process from production site to consumption market is outlined in Table 12.1.

Figure 12.1 shows a typical network structure of a LNG maritime transport system. LNG is exported from a single production facility at loading port, to a set of receiving terminals at unloading ports. In the case illustrated in Fig. 12.1, there are four regionally located LNG terminals, with differing annual demand for LNG and differing sailing distances. To transport the LNG from the production facility at loading port, to the receiving terminals at the unloading ports, a fleet of LNG vessels is required. The fleet of LNG vessels will either be designed of vessels of similar design, capacities and capabilities, or a set of different designs. An important compatibility issue is that the vessel port interface and trans-loading technology design is similar across the fleet so that all vessels as far as possible can call all ports in the shipping network. On the contrary, if the vessels of the fleet have differing vessel port interfaces, so that not all vessels can call all ports in the

Table 12.1 Components of the LNG supply chain

Components	Description	Characteristics	Goals/Challenges
Feed gas	Natural gas from fields	Transported in pipelines	Steady usage
Liquefaction plant	Cleans and cools gas to liquid state at −162 °C	High investment and operational cost	Maximize utilization without interruption
Outbound LNG storage	Storage of LNG before loading	High investment cost	Minimize required capacity
Loading	Moving LNG to ship	Specialized infrastructure; load rates	Safe loading, maximize throughput capacity
Port/vessel interface	Scheduling and coordination of vessels	Port and berth infrastructure; potential bottleneck	Need for frequent loading, long planning horizon, maximize utilization
Shipping network	Owned, chartered and spot vessels	Decisions on utilization of owned and chartered fleet	Maximize capacity utilization and minimize costs, recourse action for deviation management
Port/vessel interface	Scheduling and coordination of vessels	Agreed delivery of gas; port and berth infrastructure; potential bottleneck	Limited capacity, long planning horizon, maximize capacity utilization
Unloading	Moving LNG from ship	Specialized infrastructure; load rates	Safe unloading, maximize throughput capacity
Inbound LNG storage	Storage of LNG	High investment cost	Minimize capacity requirement
Regasification	Evaporating LNG to natural gas	Moderate investment	Meet gas demand without interruption
Gas consumption/ gas storage	Use of gas, gas to transportation system, gas to storage	Variability in demand with stochastic uncertainty	Meet gas demand

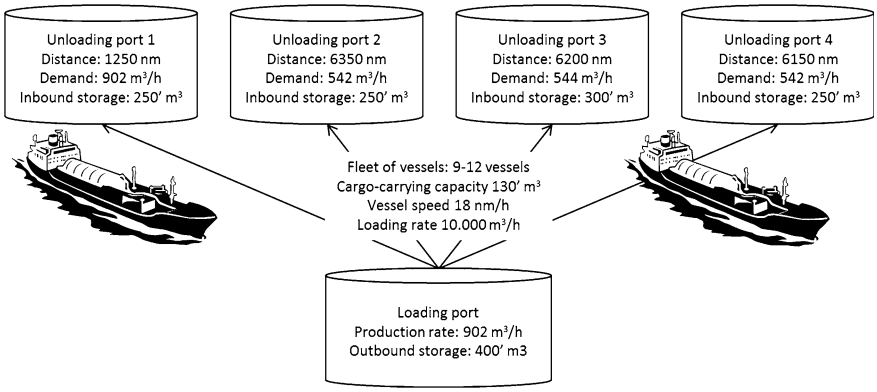

Fig. 12.1 A generic network structure of a LNG transport system structure

shipping network, then the consequences of a vessel shortfall in the fleet would have more severe consequences with higher reduction in replenishment of LNG regionally.

12.3 Infrastructure Capacity Design

Data required in transport and logistics system modelling should first and foremost describe the demand/supply relationships, and capacity influencing parameters, such as distances, speed and cargo capacity of transport means or load units. Table 12.2 shows examples of input data and output in modelling of maritime transport systems.

The starting point for the infrastructure capacity design is the availability of LNG, measured by the production rate. The gross demand for LNG in the system is measured as the sum of the demand rates at each unloading port. The baseline

Table 12.2 Input and output data in modelling of maritime transport systems

Input	Output
Demand requirements	Scale of transport infrastructure
Network structure—locations and distances	Supply or replenishment capacities
	Reduction in replenishment capacities
Capacities of transport equipment	Resource configuration to maximize system throughput or minimize
	Effect of loss of system capacity
Speed of vessels	Other
Fairway restrictions	
Sequence constraints	
Vessel port compatibility	

production capacity and hence the maximum theoretical demand that may be covered is 2,530 m^3/h or 22.16 million m^3/year. The case-specific production rate in loading port and the sum of the corresponding demand rates in each unloading port are balanced, see Table 12.3.

Table 12.3 does also provide other information about the infrastructure of the LNG maritime transport system. The distance column gives the distance between loading port and each unloading port, respectively, in nautical miles (nm). In a deep-sea LNG shipping case like this, there will be full shiploads that are delivered, while in a general industrial shipping case where partial shiploads could be delivered at unloading port, the sailing distances between all pairs of unloading ports would be required. The production rate in loading port and the demand rates in each unloading port is given in cubic metres per hour (m^3/h). A berth is the physical parking space for a vessel within the port, and as such, a capacity restriction in the port infrastructure, measured in number of berths (#). The storage capacity in each port is given in units of 1,000 m^3. The loading rate between storage and vessel is also given for each port in units of 1,000 m^3/h. The capacity of the storages is set so that they cover more than a shipload and is also related to number of berths in the port.

Based upon the volumes of LNG to be transported and the sailing distances between port of loading and each unloading port, respectively, *a* nominal estimate over number of vessels can be made. As a starting point we assume a homogeneous fleet of LNG vessels with a cargo-carrying capacity of 130,000 m^3/LNG, a sailing speed of 18 knots [nautical miles per hour, (nm/h)] and full vessel/port compatibility which means that all vessels can call all ports, in all loading conditions. The nominal estimation of required fleet of vessels is given in Table 12.4.

The estimation presented in Table 12.4 takes the gross demand in each unloading port as a starting point. By dividing the gross demand with the vessel's cargo-carrying capacity, one finds the required number of port calls per year. Knowing the distance between loading port and unloading port, the vessel speed and capacity, and the loading rate, the round-trip duration in hours can be estimated. Then the feasible number of round trips per vessel per year can be estimated. Comparing the required port calls per year with the feasible round trips per vessel per year for each unloading port, the number of vessels required to service each unloading port is given. Summarizing this for all unloading ports give the minimum required number of vessels to balance the supply and demand for LNG

Table 12.3 Initial design of fixed infrastructure

Port	Distance (nm)	Production rate/ demand rate (m^3/h)	Berths (#)	Storage capacity ('000 m^3)	Loading rate ('000 m^3/h)
Loading	0	2,530	6	400	10
Unload 1	1,250	902	2	250	10
Unload 2	6,350	542	2	250	10
Unload 3	6,200	544	2	300	10
Unload 4	6,150	542	2	250	10

Table 12.4 Nominal estimation of required fleet of vessels

Port	Unload 1	Unload 2	Unload 3	Unload 4
Gross demand ('000 m^3/year)	7,902	4,748	4,765	4,748
Required port calls per year (#/year)	61	37	37	37
Distance (nm)	1,250	6,350	6,200	6,150
Loading rate ('000 m^3/h)	10	10	10	10
Duration round trip (hours)	165	732	715	709
Round trips per vessel per year (#/year)	53	12	12	12
Vessels required per unload port (#/year)	1.1	3.1	3.0	3.0
Total number of vessels required (#/year)				10.1

within the system. The estimation states that 10.1 vessels are required to transport the LNG between loading port and unloading ports. Vessels come only in integer numbers, but a requirement for a 0.1 vessel could be chartered in a vessel market.

No seasonal influences with bad weather requiring longer sailing distance or reduced speed or fairway restrictions, for instance like missing a Suez convoy is taken into account here. Neither is queuing problems in port, cargo availability, loading restrictions, or similar taken into account in this nominal estimation.

12.4 Deterministic Routing and Scheduling

A deterministic simulation of vessel infrastructure capacities can be made with a routing and scheduling tool. The LNG maritime transport system is optimized as an inventory routing problem. Christiansen et al. [1] give a good description of inventory routing problems as part of routing and scheduling in maritime supply chains. A modelling approach to an inventory routing problem based on four stages can be found in Christiansen and Fagerholt [2]. The four stages are as follows:

1. *Routing of vessels*, seeking to minimize the total cost of deploying vessels to given routes in the network of ports.
2. *Loading and unloading*, securing that the capacity constraints of the vessels are not breached when scheduling the order of port calls in the vessel's schedules.
3. *Scheduling*, taking time elements such as sailing time, queuing time into port, and loading and unloading time in port along a route into account when scheduling the vessels port calls, as well as securing that two vessels are not allowed to enter the same berth at the same time and that one vessel must finish its service at berth in a port before the next vessel is allowed to berth.
4. *Inventory management*, securing that minimum and maximum inventory levels in each port are not breached, so that the scheduling of vessels secures that a vessel calls a loading port before the outbound inventory becomes full and that a vessel calls an unloading port before the inventory becomes empty.

The inventory routing approach is here performed with the TurboRouter fleet scheduling system, with the Invent inventory routing add-on to TurboRouter. Both

the TurboRouter fleet scheduling system and the Invent inventory routing add-on are commercial software systems, but requires adaptation to the given fleet, sea transport system or supply chain context. For this study, a specific simulation module is built for the purpose of utilizing the TurboRouter and Invent inventory routing and scheduling systems as the core in the simulation system.

As additional input to the simulation, the available volume of LNG in outbound and inbound storage at start of the simulation is given. Queuing problems, cargo availability and such is now taken into account, but effect of season, fairway restrictions, or other events reducing the capacity or capability of the transport system infrastructure is not taken into account. The deterministic transport capacity is simulated with four vessel configurations, 9, 10, 11 and 12 vessels of same type; 130,000 m^3 cargo capacity and 18 knots speed. The simulation performed simulates an annual delivery plan.

Andersson et al. [3] present two planning problems related to transport planning and inventory management in an LNG transport system, as seen from both the side of a producer as well as a vertically integrated company. Rakke et al. [4] describes a rolling horizon heuristics for creating an annual delivery plan for LNG transport systems. Both Andersson et al. [3] and Rakke et al. [4] are sources that will support the understanding of the problem presented in this chapter. The result of the deterministic routing and scheduling for different vessel configurations is shown in Table 12.5.

The simulation result shows that with the given configuration of transport system infrastructure; storage capacities, load rates, and number of berths, the system is not able to fully meet the theoretical throughput, with a 0.3 % or half a shipload underperformance. We can also see that 9 and 10 vessels reach approximately what should be expected based on the estimated vessel requirement, being 11.4 %, respectively, and 1.5 % short of the theoretical maximum, which converts to approximately 1.1 vessels and 0.1 vessels short in capacity. We have now taken the infrastructure interdependencies such as storage capacities, minimum and maximum inventory, vessel cargo capacities, vessel sailing and service times, queuing of vessels into port, berth constraints and loading constraints into account. All these infrastructure interdependencies are presented and described more in detail in the four-staged inventory routing approach presented in Christiansen and Fagerholt [2].

So far, these interdependencies have been treated in a deterministic way without assessing the impact of contingencies. Contingencies are addressed next.

Table 12.5 Deterministic throughput capacity of LNG, dependent on number of vessels

	Number of vessels				
	Max.	9	10	11	12
Throughput volume, 1,000 m^3	22,163	19,630	21,840	22,100	22,100
Deviation from theoretical maximum	–	−11.4 %	−1.5 %	−0.3 %	−0.3 %

Numbers are in 1,000 m^3 LNG

Table 12.6 Identified contingencies—expert judgment

Generated scenarios	Description	Probability per day
Production	LNG production rate down 50 % for 48 h	0.01
Loading port	Loading port unavailable for 48 h	0.003
Unloading port	One unloading port unavailable for 96 h	0.003
Tank capacity	Loading port storage tank capacity down to 24 h production for 7 days	0.005
Loading rates	Loading rates is down 50 % for 7 days	0.001
Berth availability—loading?	Only 4 of 6 loading berths are available for 5 days	0.005
Unloading rates	Unloading rate in one unloading port down 50 % for 14 days	0.001
Berth availability—unload?	Only 1 of 2 unloading berths available for 14 days	0.001
Extra-ordinary dry-dock schedule	Maintenance need removes 1 vessel for 14 days outside of schedule, plus repositioning to the Far East for yard	0.002

12.5 Identification of Contingencies Based on Expert Judgement

Transport system infrastructure–related contingencies that could be a risk for the capacity and capability of the transport system should be identified and addressed. Based on input from experts working with design and management of LNG transport systems, a list of contingencies with corresponding probabilities presented in Table 12.6 were developed.

Four out of the identified contingencies were included in the simulations performed in the next section: production, loading port, unloading port and extraordinary dry-dock schedule. These four were chosen as they represent contingencies in all steps of the transport system infrastructure, i.e., in the production infrastructure, export infrastructure, shipping network and import infrastructure. These four are marked with grey shading in Table 12.6.

12.6 Mitigating Infrastructure Measures

Mitigation of risk in a transport system could in general be achieved by two means: robustness or flexibility. Mitigation through robustness is achieved by increasing the scale of the infrastructure to have excess capacity to cope with contingencies, while mitigation through flexibility is achieved by reconfiguration of the system resources to adapt to new situations.

In the contingency simulation a set of infrastructure configurations are tested, where the effect of robustness is assessed through the change in infrastructure configuration. The infrastructure configurations are presented in Table 12.7.

Table 12.7 Infrastructure configurations

Infrastructure configuration	Outbound storage ('000 m^3)	Load rate ('000 m^3/h)	Number of vessels (#)	Unload rate ('000 m^3/h)	Inbound storage ('000 m^3)
1	400	10	9	10	250–300
2	400	10	10	10	250–300
3	400	10	11	10	250–300
4	400	10	12	10	250–300
5	800	10	9	10	250–300
6	800	10	10	10	250–300
7	800	10	11	10	250–300
8	800	10	12	10	250–300
9	400	10	9	10	500–600
10	400	10	10	10	500–600
11	400	10	11	10	500–600
12	400	10	12	10	500–600
13	400	20	9	10	250–300
14	400	20	10	10	250–300
15	400	20	11	10	250–300
16	400	20	12	10	250–300
17	400	10	9	20	250–300
18	400	10	10	20	250–300
19	400	10	11	20	250–300
20	400	10	12	20	250–300

The effect of flexibility is implicitly taken into the simulation in the way that whenever a contingency matures, the simulation model will seek to re-route and reschedule all vessel resources to improve the remaining transport capacity after the contingency has matured. Mitigation through flexibility is not explicitly accounted for in the simulations, but could be achieved with an alternative set-up of the simulator that in parallel measures the results if no rerouting and rescheduling of the vessel resources are performed after a contingency has matured.

12.7 Alternative Infrastructure Configurations

The infrastructure capacity configurations are based upon changes in five of the LNG transport system's infrastructure elements:

- outbound storage volume in loading port
- loading rate in loading port
- number of vessels employed
- unloading rate in unloading ports
- inbound storage volume in unloading ports.

There are 20 different infrastructure configurations in total, as shown in Table 12.7. If we use infrastructure configuration number 1 as an example,

Table 12.7 can be read like this: Infrastructure configuration 1 has an outbound storage volume of 400,000 m^3 of LNG, a load rate from outbound storage onto a vessel of 10,000 m^3 LNG per hour, use nine vessels, has an unload rate from vessel to inbound storage of 10,000 m^3 /h and has an inbound storage capacity of 250,000 or 300,000 m^3 LNG dependent on which unloading port the vessel calls.

12.8 Contingency Simulation with Dynamic Re-planning

The simulations are performed with an objective function to maximize the throughput of LNG in an annual delivery programme. As such, the simulation set-up tests how much throughput of LNG the maritime transport system is able to achieve given the transport system infrastructure configuration. Each simulation will simulate the operations in the transport system over a year, with the given probabilities as presented in Table 12.6 for the contingencies that could impact the infrastructure to mature. Each simulation will be a unique scenario, where the simulator will note how many and which contingencies that matured in the simulation, as well as which day of the year a specific contingency matured.

A set of 1,000 simulations were performed, which are too few to get stable results, but nevertheless is enough to exemplify the effect of interdependency risk in a maritime transport system. Running a simulation series of 1,000 simulation for the 20 infrastructure configurations took approximately 80 h with a 2.2 Ghz Intel core 2 processor with 8 GB RAM.

The results from the contingency-based simulation show that the throughput found in the nominal estimation and supported by the deterministic routing and scheduling is only a theoretical number, which is "impossible" to achieve. Hence, the effect of infrastructure and interdependency risk in transport system design should be taken into account when assessing the throughput performance of the system and the demand the system is capable of meeting to a defined level: "in the best scenario", "on average" or "as a minimum in 95 % of the scenarios".

Simulation results for a set of the infrastructure configurations are presented in Table 12.8 to highlight the main results. The cases are ranked according to their 95th percentile throughput volumes of LNG. The infrastructure configuration with the best 95th percentile is "18" with 16.36 million m^3 LNG. The infrastructure configuration with the best average is "8" with 18.60 million m^3 LNG on supplied on average. The infrastructure configuration with the highest "disruption-free" volume is some 11 and 12 vessel configurations, for instance "2", "7" and "15", with a disruption-free throughput of 22.23 million m^3 of LNG. This is more than the annual production rate, which states that the year-end outbound storage level is lower than the year-start outbound storage level. The infrastructure configurations with the lowest throughput volumes were all the nine vessel configurations. The "Deviation average of maximum volume" and "Deviation 95th percentile of maximum volume" state the percentage reduction in transport volume of LNG in the average and 95th percentile compared to the disruption-free volume.

Table 12.8 Simulation results, ordered by 95th percentile volumes. Not all cases are shown

Infrastructure configuration	Average volume ('000 m^3)	95th percentile ('000 m^3)	Disruption-free volume ('000 m^3)	Deviation average of max. volume (%)	Deviation 95th percentile of max. volume (%)
18	18,388	16,361	21,710	−15	−25
6	18,412	16,250	21,840	−16	−26
7	18,472	16,250	22,230	−17	−27
15	18,358	16,120	22,230	−17	−27
8	18,600	16,120	22,100	−16	−27
20	18,467	15,990	22,230	−17	−28
17	17,477	15,470	20,150	−13	−23

Figure 12.2 shows the simulated distribution for the three infrastructure configurations: "18" with 10 vessels and doubled unloading rate from vessel to inbound storage, which had the highest simulated 95th percentile volume; "7" with 11 vessels and doubled capacity of inbound storage, which had the highest simulated average volume; and "8" with 12 vessels and doubled capacity of inbound storage, which had the highest disruption-free volume.

Although the three infrastructure configurations represent 10, 11 and 12 vessels, respectively, the distribution of transported volume of LNG do not differ substantially. In Fig. 12.3, we take a closer look at the 5–95th percentile span and the 30–70th percentile span. The distribution in Fig. 12.2 and the 5–95th percentile span in Fig. 12.3 show that the 11 and 12 vessel infrastructure configurations have a higher likelihood of supplying higher volumes of LNG. However, one additional

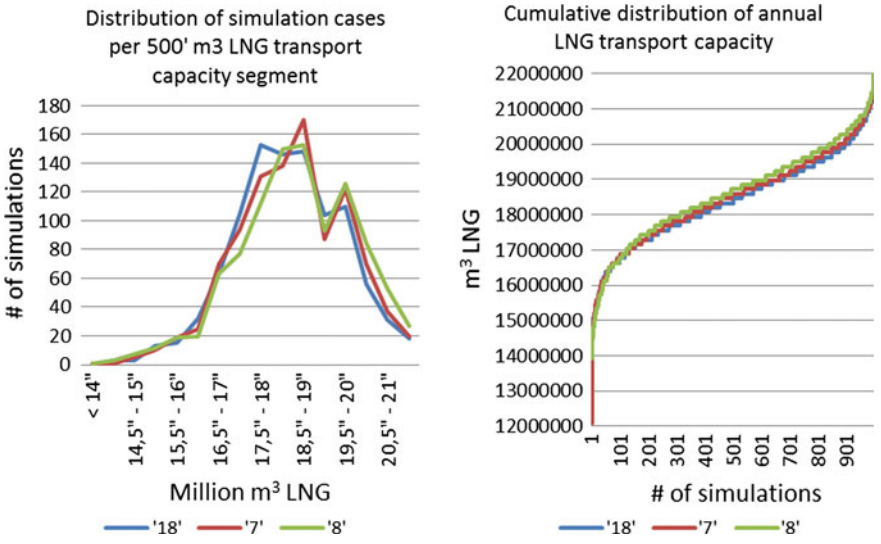

Fig. 12.2 The distribution and cumulative distribution of simulations results for three infrastructure configuration scenarios

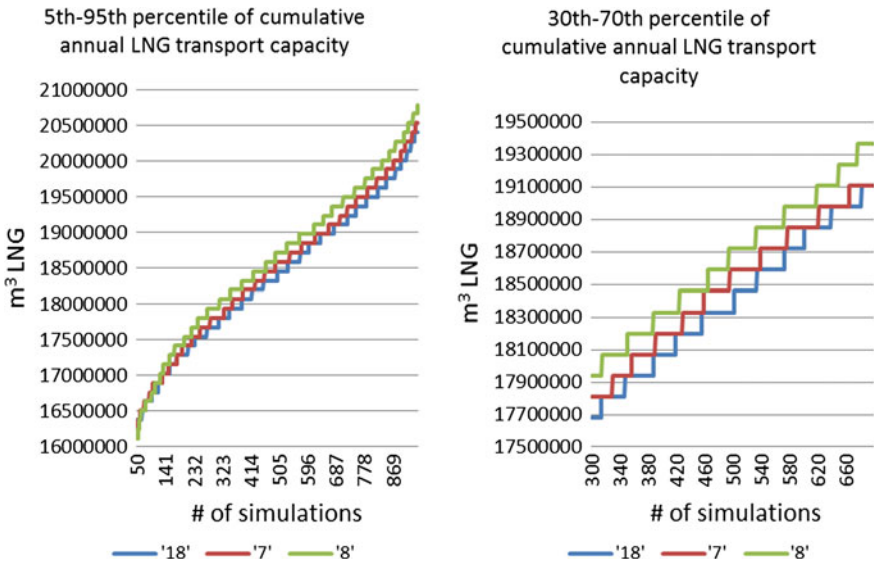

Fig. 12.3 5–95th percentile versus 30–70th percentile of cumulative simulation results

Table 12.9 Best disruption-free volume versus best simulated average and 95th percentile volumes—infrastructure configuration "8" versus "7" and "18"

	Disruption-free volume	Simulated average	Simulated 95th percentile
'000 m^3 per annum	22,230	18,600	16,361
Percentage of disruption free	100 %	84 %	74 %

vessel will only contribute to carry one more shipload of cargo on average, or 130,000 m^3 of LNG. Given the capital and operational expenditures for an LNG vessel, that would result in a low-performing cost-benefit assessment.

The most notable results are the decrease in transported volume that results from the interdependency risk in the transport system. The transport infrastructure configuration with the best simulated average can supply 84 % of the best disruption-free volume, while the best 95th percentile supplies only 74 % of the best disruption-free volume, seen in Table 12.9.

12.9 Cascade Modelling as a Rough Assessment

A question then is how a cascade modelling approach could be used instead of such a detailed simulation analysis, or in addition to detailed analysis. The cascade modelling may (*cf.* Chap. 11) be used for:

- a *rough risk estimation* of linear interdependency risk in the maritime transport system, and
- a *rough vulnerability assessment* of the consequences of supply disruptions.

These are both important contributions that contribute to making the analyst aware of the consequences that interdependency risk may have in a transport system and their vulnerabilities.

The main drawback of the cascade modelling approach in a transport system context is the inability to make detailed assessments of the interdependencies in the network of ports and vessels. An option is to use the experts' knowledge to estimate the additional contribution of network effects when estimating conditional probabilities, extent and duration in the cascade diagram. In the case presented in this chapter the network structure is quite simple. Still, the inventory routing considerations bring in additional information that could be hard to obtain in a cascade diagram. This could for instance be interdependencies between capacities in storages and the effect of queuing of vessels, the effect of storage capacities and load rates and the utilization of vessels. This information would be required if a cost-benefit assessment of investments in infrastructure measures shall be conducted.

12.10 Discussion

The results from the simulation study of the risk-adjusted volumes show the value of performing a risk assessment of the interdependency risks existing in a transport system. Although the conducted risk assessment is based on the use of a rather high-level inventory routing system, it shows that interdependency risks need to be accounted for when assessing the volumes of LNG the system could be contracted to supply.

The added value of the more detailed simulation approach compared with a cascade diagram is improved ability to assess effects of changes in the transport system infrastructure configuration, including the ability to model and assess the interdependencies that exist within the transport system infrastructure itself in detail. In addition, the simulation provides the opportunity to assess the effect of direct mitigation through the inherent flexibility in rerouting the fleet of vessels when a contingency matures.

Cost-benefit assessments have not been considered here, but just by seeing the relatively small contribution to transported volumes of LNG that additional vessels have beyond 10 vessels shows that any change in other elements of the transport system infrastructure should be assessed before adding more vessels to the fleet.

The simulation results could also be used to assess short-term effects when several contingencies mature simultaneously, which is more in parallel with the cascade modelling approach, for instance maximum reduction in supplied volume of LNG as a whole in the system or to specific unloading ports during shorter time

periods, such as a week or a month. Since the specific day a contingency mature is reported in the simulation, "extreme events" can be found, or they can be forced to happen by the simulation model, just to assess the short-term effects.

A weakness in the optimization and simulation model is that there are three unloading ports that have equal demand, and almost equal distance. The fourth unloading port has approximately a doubled demand, but only one-fifth in distance. When the objective function then is to maximize the total throughput for the system, implicitly stating that it is OK to replenish the nearest unloading port in full, then the unloading ports that are located farther away could be supplied much less than the nearest, without any penalty. This contributes to minimizing the difference in throughput volume for the system as a whole as a function of the number of vessels.

12.11 Conclusion

Risk-based design of transport systems is required and interdependency risk in LNG transport systems should be taken into account during configuration design. A rough cascade modelling approach could be used, preferably with transport system experts present that could give a good estimate of additional effects of interdependency risk. A more detailed approach with a model of the transport system configuration and interdependencies presented in this chapter could be used to optimize system infrastructure resources and simulate effects of contingencies on the LNG transport system's ability to supply LNG in the quantities required.

Acknowledgments We would like to express our thanks to the experts that provided input to the LNG transport system contingencies. An article, giving a more comprehensive presentation of this case in relation to a formal vulnerability assessment, is in review process for publication in a scientific journal, with Øyvind Berle as lead author.

References

1. Christiansen, M., Fagerholt, K., & Ronen, D. (2004). Ship routing and scheduling: Status and perspectives. *Transportation Science, 38*(1), 1–18.
2. Christiansen, M., & Fagerholt, K. (2009). Maritime inventory routing problems, In C.A. Floudas & P. Pardalos (Eds.), *Encyclopedia of optimization* (2nd ed., pp. 1947–1955). Heidelberg: Springer.
3. Andersson, H., Christiansen, M., & Fagerholt, K. (2010) Transportation planning and inventory management in the LNG supply chain. In E. Bjørndal & M. Rönnqvist (Eds.), *Energy, natural resources and environmental economics* (pp. 429–441). Berlin: Springer.
4. Rakke, J. G., Stålhane, M., Moe, C. R., Christiansen, M., Andersson, H., Fagerholt, K., et al. (2011). A rolling horizon heuristic for creating a liquefied natural gas annual delivery program. *Transportation Research Part C: Emerging Technologies*, pp. 896–911.

Chapter 13
Risk Management of Interconnected Infrastructures: An Empirical Study of Joint Stress Conditions

Emery Roe and Paul R. Schulman

Abstract This chapter has been written for engineering practitioners, support staff and researchers interested in how to assess and manage risks that arise because critical infrastructures are interconnected, and increasingly so. Infrastructures are large technical systems for water, electricity, transportation, telecommunications and financial services, among others, whose assets and services are considered vital to society. These engineered systems operate under legal, regulatory and mission mandates to be highly reliable, that is, to ensure the safe and continuous provision of the critical service in question, even during (especially during) peak demand or turbulent times. Because they operate under high reliability mandates, their control operators and staff take risk assessment and management seriously. This chapter focuses on what we consider to be neglected but extremely important topics related to the assessment, management and tracking of risks at the interconnected critical infrastructure system (ICIS) level. Special features of infrastructure control rooms are discussed, and an empirical analysis demonstrates conditions under which interconnected infrastructures share risks for joint management purposes.

13.1 Introduction

Many engineers view the interconnections among large engineered systems in a positive light. Normal operations of shipping, rail and road transportation, for example, would not be possible without reliable electricity and telecommunications systems.

E. Roe (✉) · P. R. Schulman
UC Berkeley and Mills College, Oakland, USA
e-mail: emery.roe@berkeley.edu

P. Hokstad et al. (eds.), *Risk and Interdependencies in Critical Infrastructures*, Springer Series in Reliability Engineering, DOI: 10.1007/978-1-4471-4661-2_13,

Engineers also recognize that cross-infrastructure interconnectivity—including interdependencies discussed elsewhere in this volume—has its downside, for example, electrical blackouts can cascade across telecommunications and other systems, including intermodal transportation, that depend on reliable electricity and telecoms. In the negative view, interconnectivity of infrastructures represents accidents and failures waiting to happen or that have happened, while in the positive view interconnectivity is key not only to normal infrastructural operations but also to society's resilience in the face of shocks, surprises or major infrastructure failure.

Because the positives and negatives go together, there are *risks* that engineers must balance and manage when it comes to interinfrastructural connectivity. A good deal of work has been done on analysing the risks. This chapter focuses on under-acknowledged issues with respect to interconnectivity that have, we argue, major practical importance for interconnected critical infrastructure systems (ICIS). These crucial but under-recognized issues include the importance of high reliability management and control rooms for improved risk assessment and management; the special character of infrastructure resilience; and the need to track and measure that resilience.

First we describe high reliability management in infrastructures and thereafter the singular features of infrastructure control rooms in that management. We offer a case study of the conditions under which control variables of different infrastructures overlap, and we describe the importance of infrastructure resilience in these instances as its own form of risk management at the level of the ICIS. The chapter ends with more general considerations about resilience and robustness.

13.2 High Reliability Management of Critical Infrastructures

Why would engineers be interested in how critical infrastructure operations and interconnections are managed? After all, the promise of engineering is to design out the shortcomings of real-time managers and operations. We have even heard one engineer call control room operators Neanderthals. Another said, "I design systems to be not just fool proof but *damned* fool proof—so even a damned fool cannot screw them up". Why then with their emphasis on the better design of future systems should engineers focus on enhancing risk management of present systems?

The answer is straightforward: Operators are responsible for the high reliability management of our critical infrastructures, and high reliability management, because it is mandated by law, regulation and mission statement, must take real-time operational risks of our infrastructures very seriously [1]. Operators and their support staff are an ideal audience for engineers dedicated to better risk analysis. Or to put it the other way around: If engineers cannot improve risk management for operations in real time, why would we believe the same engineers can do so in the longer term? Why should we believe those who are unable to come up with

practical solutions to current infrastructure risks, yet who insist they are more than able to come up with practical solutions for risks in years far ahead?

For the purposes of this chapter, high reliability management is the safe and continuous provision of a critical service, even during—especially during—times of peak-load demand or turbulence. It is typically found in the control rooms of large critical infrastructures, and our ongoing research in California indicates that control operators and their support staffs are preoccupied with reliability-centred ways to reduce the risks of their infrastructures failing. Since infrastructure control rooms are places where reducing risk arising out of interinfrastructural connectivity matters right now in real time, it is important to establish what makes control rooms special.

13.3 Special Features of Control Rooms

Infrastructure control rooms represent a unique organizational niche. They are one of the few institutional frameworks that have evolved to promote high reliability repetitively in the management of complex systems, now and over time. Not all control rooms are the same nor do all infrastructures have control rooms, but they are found throughout many large technical systems, including air traffic control, power plants, electrical grids, large water systems, rail networks, oil exploration and production, ports and telecommunications, to name a few.

Given their evolutionary importance to ensuring high reliability, control rooms are surprisingly under-researched in organizational terms. A great deal has been written in terms of their physical design and technology, and control rooms have been analysed from the standpoint of human factors [2–4]. But organizational analyses are scarce [5–8].

The control rooms of interest in this chapter have six interrelated features of importance for engineering risk assessment and management. Since the reader may be unfamiliar with the features or their importance, we summarize them briefly, giving special attention to the sixth feature and conclude with their overall implication for risk analysis in infrastructures operating under high reliability mandates.

13.3.1 Centrality

Control rooms need not be centralized, but they are central. Participating units are often geographically dispersed (sometimes in separate organizations) and are brought into a functional interrelationship by control room personnel who are situated to monitor and coordinate to produce a mutually desired output. Control room operators are placed to integrate and interpret information, provide instructions and assess risks for reliable real-time operations.

The networked centrality of control rooms among component units is a defining feature of many infrastructures. Even though centrality may give a logical preeminence to control room instructions, participants within the networks must trust this logic and be willing to follow often rapidly shifting instructions (and with them shifting risks). Trust, in other words, carries its own risks.

13.3.2 Control as a Physically Networked Process

Control operators do not "run" their systems in the sense of throwing switches or turning valves. Frequently their instructions are verbal or communicated—given to people who do throw switches, turn valves or steer. That is electronically, they communicate with people located some distance away from the source of the instructions. Even when control operators do push a button manually, it is likely to be the exercise of control at a distance—through electronic instructions or relay switches.

13.3.3 Team Organization

Control rooms are team efforts and teams are their own organizational networks. During peak demand or when the system is in trouble, overlapping attention by team members becomes essential. Control room teams may assemble a wide distribution of analytic and experience-based approaches that promote high reliability management.

The mix of backgrounds allows the team to enhance its coverage and management of risks across several cognitive fronts: from critical analysis to experiential-based practices to rule-following and formal algorithmic orientations. In addition to task overlap and cognitive differentiations of control room teams, this in-group identification and support are essential to overall team situational awareness.

This means that better than others elsewhere, control room operators understand how their infrastructure works, the major risks involved, and what must be done to keep it working to meet the various legal, regulatory and mission mandates for reliability.

13.3.4 Operational Redesign

A unique evolutionary advantage of control operators arises out of the broad analytic and experiential coverage of operators combined with their overlapping specializations and sustained team situational awareness. This advantage is their ability to operationally redesign what are inevitably incomplete or error-vulnerable

designs and technologies. Faulty or inadequate designs often become readily visible only in real-time operations, and it is in real time that high reliability management must reduce the risks arising out of such defects. This means that those designs and technologies have to be redesigned (often through tactical "workarounds") during actual operations or operators face the risks of design-induced infrastructure disruptions or outright failure.

13.3.5 Surprise and Requisite Variety

Because of component complexity in large-networked technical systems and the diversity of external factors that affect them, control room operators are unavoidably confronted with unusual, differentiated and surprising challenges and risks in their operations.

Operational reliability under these conditions lies in maintaining the match between operator skills and tasks by managing the high input variance they confront and transforming it into stable and closely bounded performance output variance [1]. Operators manage so as to keep system operations within *de jure* and *de facto* bandwidths of safe and continuous conditions. Transforming high input into low or stable output variance requires high process variance—flexibility in operator strategies and options—to achieve a "requisite variety" of responses to match the variety of input conditions.

To this end, successful control operators excel in recognizing patterns emerging across their system and in formulating an inventory of contingent scenarios to guide action through a range of specific situations arising in that system. The patterns include experientially tempered judgments of event frequencies used in probability estimates, while the scenarios include those for worst-case risks. Operators do so by developing a domain of competence that lies between seeing the infrastructure primarily from the perspective of formal deductive design principles and seeing it only on the basis of prior experience. The scope of their competence lies between the infrastructure as a system and the specificity of a single case or event failure in that system.

That is why control operators we have studied rely on a set of complementary performance modes within and across which they can operate depending on conditions confronting their infrastructure. These range from anticipatory exploration of options ("just-in-case") when operations are routine and many control strategies and options are available, to a real-time ("just-in-time") invention of options or improvisation of strategies when conditions are unstable (i.e. thereby adding to requisite variety). Operators may operate in a high-risk mode ("just-for-now") when stability is low and options are few and may also be able, in emergencies when options have seriously dwindled, to impose onto network participants a single emergency scenario ("just-this-way") to stabilize the situation.

These alternate but related performance modes are part of a requisite variety of responses needed to match the full range of input variance operators can encounter

in their systems. As we will see, this ability of control room operators to move across performance modes as conditions change is crucial to the resilience of their infrastructure. That said, each performance mode has its own risks, and the challenge in control rooms is to manage the risks as conditions and options change—often in surprising ways; for more, see [1].

13.3.6 Control Variables

Last but in no way least, the way control room operators manage what can often be high input variance to produce low or stable output variance is through their manipulation of specific management factors we call "control variables".

To see how, start with the design logic and the reliability mandates pertinent to managing risks in the large technical system of concern. That design is based on a causal model that identifies essential control variables—a relatively small set of actionable variables changes in which allow control over larger system conditions to realize the safe and continuous provision of the service produced by the infrastructure. Thus, electricity grid controllers focus on directing generation (supply) in relation to changes in load (demand). Controllers can also direct electricity flow along alternate transmission lines and exert control over voltage and frequency. Control operators in California's large-scale water project operate pumps and open floodgates to control the flow rates of water into and out of reservoirs and dams. Infrastructures could not have stable outputs in terms of their services without these factors that they can actually manage as and when needed.

All organizations have control variables, but what the reader should note here is the different role that control variables have in control rooms compared with conventional organizations. While control variables in many organizations (that is, their policies, rules and procedures) impose persisting constraints, operators in infrastructure control rooms must manage their control variables quite rapidly and flexibly—one instruction can quickly supersede another. In conventional settings, policies, rules and procedures are meant to be "sticky"—indeed, their persistence is an important feature for the control of conventional organizational behaviour. Yet air traffic controllers must be able to order a rapid series of adjustments in airspeed, direction and altitude of planes in their sectors. Depending on the changing conditions they face, generation dispatchers for electricity may order increases or decreases in generation among operating plants, they may order reserve generators on or offline, they can make adjustments to change the frequency of current across transmission lines and re-route power to avoid line congestion. Dynamic risks in critical infrastructures could not be managed without this rapid "flexing" of control variables.

How control variables are actually managed by control room operators for the purposes of infrastructure high reliability is also an under-studied area of major importance for engineering risk assessment and management. The questions involved are crucial ones: What are the conditions under which infrastructure

control variables become interconnected across different infrastructures? If operators of the respective infrastructures do not fully apprehend these real-time interconnections, what does this mean for risk management at the ICIS level? Sect. 13.4 presents a short case study illustrating the conditions under which control variables can interconnect for multiple infrastructures and the importance of infrastructure resilience when this happens, even during their normal operations.

13.3.7 Implications

What do these six special features of control rooms mean in a practical sense for the end-user of the critical service in question? In the most fundamental sense, the consumer or customer who turns on the light switch or water tap or wall thermostat or gas oven dial notices none of what has gone on to ensure this always-on, always-reliable service. The service is just there, even during peak demand or turbulent times.

What the consumer does not see is all that effort, behind the scenes in the infrastructures, required to keep the service reliable. In formal terms, low or stable output variance of the critical service is the product of high process variance in a world where input variance is increasing for infrastructures. Unexpected electricity outages, unforeseen cell tower malfunctions, unusual shipping lane congestion, abnormal water pumping problems—all and more have to be managed by control operators in order to ensure the electricity stays on, cell phones don't experience drop calls, cargos are still transported on time and the water is there when needed. For infrastructure control rooms to undertake the kind of management to ensure highly reliable services for the end-consumers is full of risks in need of levels of high management that the end-user does not see or know.

13.4 Conditions for Interconnected Control Variables: An Illustration for Two Infrastructures

Our brief case study examines the interconnectivity between water flows (WFLOW) at the California State Water Project's (SWP) pumps near Tracy (hereafter, Banks Pumps) and electricity flows from the California Independent System Operator (CAISO) to power those pumps.[1] While the Banks Pumps are one element in the SWP, they are extremely important. Their role is basically to

[1] This subsection has been co-authored with Benjamin Baker and is adapted from a 2011 RESIN working paper, "Case Study of Interconnected Critical Infrastructures in the Sacramento-San Joaquin Delta: The interconnectivity of water and power flows at the State Water Project's Harvey O. Banks Pumps, near Tracy California," by Benjamin Baker, Emery Roe and Paul Schulman. Details of the data sources, methods, and acknowledgements are found there.

pump water from northern California (including its rivers, Delta and large storage facilities) to canals, reservoirs and dams for use by Californians south of the Pumps. Water storage is an especially important feature of the SWP (as it is of the federal Central Valley Project), given the prevalence of drought or dry weather years. Whatever the year, however, water still needs to be move from the north to the south, and the Banks Pumps are a key part of the pumping requirement. The Banks Pumps, unlike some other SWP pumps, do not generate electricity but rely on electricity transmitted by CAISO.

We focus on one unidirectional interconnection, namely, how changes in electricity flows into the Banks Pumps affect changes, if any, in WFLOWs through the Pumps. Do unscheduled changes in electricity flows off the transmission grid affect changes in WFLOWs, even during normal operations of both the electricity and water infrastructures? We present evidence for a qualified "Yes" to that question, at least in periods or under conditions of overlapping stress. This conclusion suggests that where conditions of overlapping stress exist for two different but conjoined control variables (electricity flows and WFLOWs), it is more likely that other control variables could be stressed as well during such periods.

13.4.1 Specific Hypotheses

The argument that changes in electricity for pumping affect changes in pumped WFLOWs may look to be an unexceptional statement of fact, but it is not for those who manage the respective systems. As we have just seen, each infrastructure operates under legal, regulatory and mission mandates to be reliable, and this frequently means that there should be fallbacks and alternatives to ensure reliable supply in case of problems arising from elsewhere. There are backup generators at Banks, if regular power supplies are disturbed. For its part, the electricity transmission grid has been designed to a standard of N-2 contingencies, that is, a failure in one of its transmission lines would not necessarily interrupt overall power flows, since alternative routing exists, other things being equal. Changes in electricity for pumping water affects the water being pumped, but those changes must be managed so end-users of each service are not affected in terms of their own consumption. This case study is about managing those changes and the behind-the-scene risks they impose for the control rooms concerned.

As a starting proposition, it seems reasonable to assume that under normal conditions and over a long time horizon, the respective water and power flows in the SWP and CAISO would be of a low and slightly positive correlation: "Low correlation" because, while the infrastructures are connected, each is designed to be reliable even if episodic trouble emerges from another such infrastructure; and "slightly positive" because over the long run, other factors constant, one would expect the demand and supply for water and power to move in the same direction with broad economic and secular trend conditions.

More specifically, since the focus is on the conditions that stress more than one infrastructure, this case study posits: Other things being equal, the more reliability problems in electricity flows to the Banks Pumps, the less water to flow through those pumps, when both infrastructures are stressed during normal operations. That is, we hypothesize a *negative* correlation, not a positive or negligible one, between reliability problems on the electric transmission grid as an infrastructure and the WFLOWs at one of the elements of the water infrastructure during common periods of stress. We expect non-negligible (but not large) correlations in any case because the stressed variables we use for the electricity grid reflect many more seasonal issues and performance conditions than those that connect directly with the Banks Pumps [1].

What does it mean to say that the power and water systems are "stressed"? Start with the case of CAISO, since we are arguing that problems in its transmission grid can affect the WFLOWs through the Banks Pumps under conditions of stress. CAISO's most critical electricity reliability requirement is to balance load and generation across the grid at any point in time and over time. An imbalance of load and generation can cause the grid to collapse, leading to widespread shedding of load ("blackouts"). This balance between load and generation is monitored through the Area Control Error (ACE), which is observed on monitors by CAISO control operators. The ACE must fall within established Western Electricity Coordinating Council limits for set intervals every hour (Control Performance Standard 2; hereafter CPS2).

Our earlier research in [1] found that CAISO control operators are especially sensitive to several factors when it comes to managing CPS2 violations. For the purposes of this chapter, we focus on two. Unscheduled generation outages (OUT) cause CAISO operators difficulties—that is, when generation capacity goes offline unexpectedly and puts at risk balancing load and generation, as does congestion along the transmission lines—that is, when more energy is needed to flow across lines that are already at capacity. These factors, in turn, provide indicators of when CAISO operators are pushed to their performance edge with respect to one of its major reliability standards, the CPS2 standard. The closer to their performance edge, the more stressful that period is for them. Given their importance, the numbers of CPS2 violations, unscheduled OUT and line mitigations (MIT) were recorded for CAISO on an hourly and daily basis.

To put this in the language of control variables, grid reliability is maintained by CAISO operators and support staff by controlling a number of operating factors, including when generator OUT can be scheduled and routine line maintenance undertaken. When conditions make it difficult for CAISO operators to manage control variables successfully, we identify these as conditions associated with a performance edge. The ability of operators in real time to rebound back from these difficult conditions is what we found to be resilience in their high reliability management [1].

SWP control operators also face their own performance edges, associated with periods of stress when it comes to pumped WFLOWs. The SWP is subject to regulatory and legal standards governing WFLOWs through the Banks Pumps, and

these vary over both the short- and longer-term horizons. Their constraints are associated with agricultural water contracts, environmental regulations, court orders, urban water quality standards and other factors. Conditions during certain times of the year make SWP operators especially sensitive to these constraints. What they usually control for becomes more difficult in these circumstances. We shall see in a moment why *lower* WFLOWs would be problematic during these periods, giving SWP operators "less wiggle room", as one SWP support person described it.

To summarize, our core question is this: How, if at all, does the effect of CAISO operators moving to their CPS2 performance edge because of, for example, unscheduled generation OUT and transmission line congestion MIT, reduce WFLOWs at the Banks Pumps, when those WFLOWs and their management are already stressed during normal operations?

13.4.2 Data Sources, Period of Study, and Methods

The California Department of Water Resources (DWR) provided records for how much water the Harvey O. Banks Pumping Station pumped and how much energy banks used to run the pumps. These data span more than 6 years (June 2004–December 2010) of hourly energy records (MWh) and daily pumped WFLOWs (acre-feet). The CAISO power reliability metrics regarding daily CPS2 violations, unscheduled generation OUT and transmission line MIT for 4 years (July 2004–2008) were drawn from [1]. Our study period is, with few exceptions, mid-2004 through mid-2008.

In order to determine whether and the extent to which electricity problems affect WFLOWs during normal operations, we relied on the analysis of variance (ANOVA), which includes correlation and regression analysis for the combined dataset.

13.4.3 Results

Results of the statistical study are presented and discussed below.

13.4.3.1 Banks Water Flow and Electricity Consumption

Start with WFLOWs at the SWP Banks Pumps. Operators, we found, contend with considerable variation over time in the amount of water that is pumped. Water exported from Banks varies substantially throughout the course of a year and between years. The time series in Fig. 13.1 shows how the average amount of water pumped at Banks each month for 2005–2010 varies versus a baseline for all 6 years.

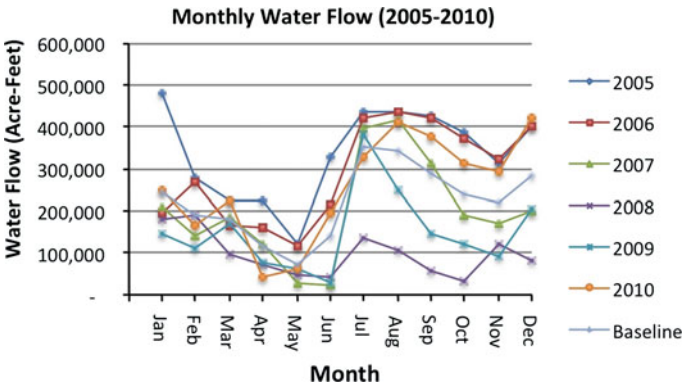

Fig. 13.1 Banks exports of water (2005–2010)

Depending on the year, the amount of water that is pumped is highest during the summer and into early autumn. It is lowest in the spring. Based on our past research, we assume operator stress is measured by the rising difficulty of operators having to match WFLOW rates, their major control variable, with water obligations arising from the agricultural, industrial, urban and environmental sectors. The more difficult the match, the greater the real-time stress, holding other factors constant.

Summer and early autumn can be stressful times for SWP operators, as water is drawn down from reservoirs and dams with diminishing water supplies during times when temperatures are at their highest (summer) or when weather is unpredictable (e.g. temperatures may remain high into the autumn months of September and October).[2] September and October are also when several important environmental standards come into force, which constrain WFLOWs further (e.g. some seek to limit the effect of pumping on fish survival). In other words and recognizing the substantial year-to-year variability, SWP operators come through summer and early autumn having to ensure high WFLOWs and then under more environmental mandates to ensure sufficient water for threatened and endangered species and habitat. To shut the pumps down unexpectedly during this period or deviate with lower flows that planned would be particularly stressful.

The amount of water pumped is proportional to the electricity it takes for Banks to run the pumps (Fig. 13.2). The reason why water pumped and energy usage are not perfectly correlated is because some energy (approximately 20 MWh, based on days without WFLOW) is used for purposes other than pumping water, such as lighting offices at the Banks facility and running heating, cooling and ventilation systems.

[2] A host of other recurring or one-off factors may be involved, such as major fires in October 2007 in southern California, regulatory requirements for smelt and salmon, and gearing up to meet Army Corps of Engineering flood control reserve requirements in major reservoirs.

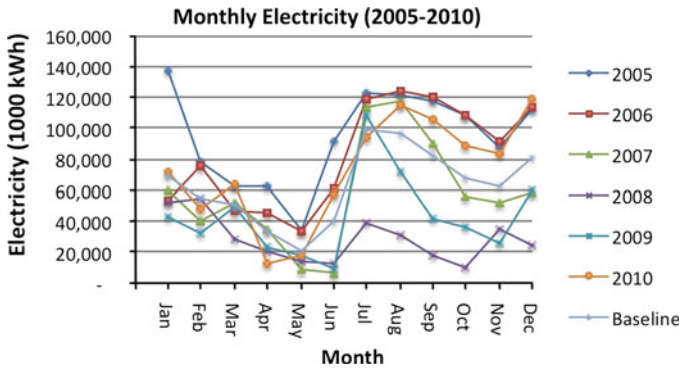

Fig. 13.2 Banks energy usage (2005–2010)

13.4.3.2 CAISO Reliability Indicators

Turn now to the CAISO dataset and reliability indicators. Figure 13.3 shows the number of CPS2 violations on a typical day for any given month averaged over all the years. CPS2 violations appear to be highest in summer. In June and July, average number of violations per day is over eight (8), compared with about six (6) in February through April. The average number of violations is also over eight in October. Based on research [1], the "shoulder months" of April/May and September/October are periods of stress with respect to operator performance. This is because these periods are of seasonal change, which make it more difficult to predict peak loads and their actual occurrence, which in turn have an effect on the repair and maintenance schedules of generators and transmission lines.

A time series of the average daily CPS2 violations by month for each year in the study period (Fig. 13.4) shows again that normal operations during summer months can be stressful, though here as with respect to WFLOWs (Fig. 13.1) each year is different.

When it comes to generation OUT and line MIT, the mean daily unscheduled OUT (Fig. 13.5) are highest from summer into early autumn.

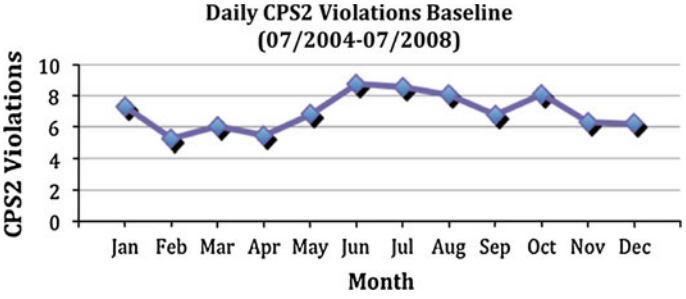

Fig. 13.3 Average daily number of CPS2 violations by month (Averaged over July 2004–2008)

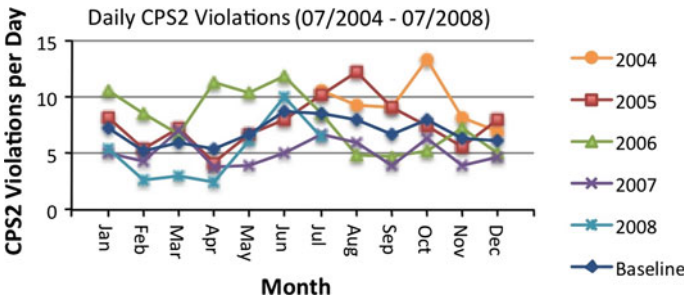

Fig. 13.4 Disaggregated daily CPS2 violations by month and year (July 2004–2008)

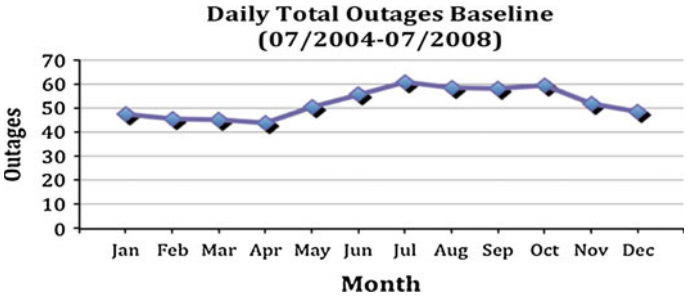

Fig. 13.5 Daily ambient and forced outages by month (Average for period July 2004–2008)

The average daily total transmission line MIT (when electricity must be re-routed because one line is already at capacity) is higher in mid-summer though rising again in autumn (Fig. 13.6).

To summarize, summer months and in some cases the autumn months have the highest number of OUT, MIT and CPS2 violations. It is also, as we saw, the period in which WFLOWs through the pumps are high and necessarily so (i.e. not expected to be declining).

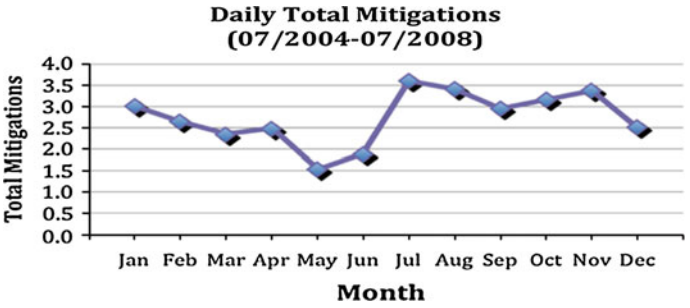

Fig. 13.6 Daily total mitigations by month, (July 2004–2008)

13.4.3.3 Correlation and Regression Statistics

Table 13.1 shows the correlation coefficients of the CAISO daily indicator variables when run against daily WFLOWs at the Banks Pumps. Table 13.1 also disaggregates the July 2004–2008 study period into sub-periods of possible stress, along with their correlation coefficients. In all cases, we tracked the actual unscheduled generation OUT, transmission line MIT and grid CPS2 violations (CPS2) to see how correlated they were with the water flow variable, WFLOW.

As other figures above demonstrate, some years were more difficult than others in terms of the effect of temperature and weather on WFLOWs and power flows. We also saw how the summer months (June through August) and the early autumn months (September and October) could cause more stress for operators. There are also special activities like the Delta Dispatch between May and July, which have caused problems, according to our interviews, since water cooling temperatures of key Delta generators—and thus their availability—are regulated to ensure better spawning habitat for adjacent fish species.

Most Table 13.1 correlation coefficients are positive. That is, WFLOWs and CAISO reliability indicators move in the same direction. This is not surprising, if—and this may be a big "if"—(1) over time water and power flows increase or decrease together with economic and secular conditions and (2) these ups (and downs) in power flows mean more (or fewer) OUT and MIT. (To verify this "if" would have required a much longer time series of data than we were given access to.) That said, the overall correlation coefficients in Table 13.1 for OUT, MIT and CPS2 violations over the entire period (the first row in Table 13.1) are low and positive, as expected for infrastructures that spent most of their time in normal operations rather than in disruption or failure due to the other.

What is of more interest in Table 13.1 are the *negative* correlation coefficients, for these move in the opposite direction, consistent with our specific hypothesis: As line MIT and CPS2 violations increase (indicating increased problems on the

Table 13.1 Correlation coefficients with water flow for all data and various sub-periods

	Outages	Mitigations	CPS2 V	N obs (count)
All data (Jul 2004–2008)	0.097	0.189	0.096	1479
Jul–Dec 2004	−0.079	0.210	−0.147	184
2005	0.141	0.074	0.254	363
2006	0.126	−0.034	−0.081	364
2007	0.285	0.066	0.113	356
Jan–Jul 2008	0.152	−0.077	−0.113	242
Delta Dispatch (May 1–Jul 15)	0.001	0.245	0.192	307
Jun–Aug	0.097	0.242	0.092	430
Shoulder months (Apr. May, Sept and Oct) (Sep'04–May'08)	0.232	0.157	−0.003	486
Oct	0.216	−0.181	−0.341	124
Sep and Oct	0.197	−0.223	−0.277	244

grid), WFLOWs decline or lower, other things constant. Since correlation is not causation, the reverse could as well be argued. For example, the negative sign could indicate is that: As WFLOWs increase, line MIT and CPS2 violations instead decrease in the transmission grid system, albeit by means we have yet to discover.[3]

To see how this works out, the rest of this section focuses on one sub-period of all the days in the months of September and October when (1) both SWP and CAISO are operating under stressors, (2) during which WFLOWs are by and large expected to be high and not declining and (3) where the Table 13.1 correlation coefficients are negative for line MIT and CPS2 violations (but not for OUT) with respect to WFLOWs.

13.4.3.4 September/October Sub-period

Based on the preceding discussion, MIT and CPS2 are not equivalent factors, at least for CAISO operators. CPS2 violations are an "output" variable, while MIT is one of the "input" variables to that CPS2 performance edge. That said, there is nothing in this chapter's discussion of interinfrastructural connectivity that presumes SWP operators could not have CPS2 violations, MIT or whatever as their own *input* variables for determining WFLOWs at the Banks Pumps. Table 13.1 suggests that from the perspective of those WFLOWs as the dependent variable for SWP control operators, MIT and CPS2 violations are each possible independent variables in the September/October sub-period.[4]

Table 13.2 provides the raw statistics of a regression analysis with daily WFLOWs as a function of the independent variables, MIT and CPS2, for the September and October months that fell within the 2004–2008 study period.

Even when rounded off, the numbers and findings in Table 13.2 are very significant for our purposes. The independent variables, MIT and CPS2, are of the right sign (negative), and their respective negative beta-cofficients are statistically significant at the 0.05 level or better.[5] The overall functional relationship between the dependent variable, WFLOW, and the independent variables, MIT and CPS2, is statistically significant (the high F-statistic). The adjusted R^2 suggests that of

[3] For example, we wondered whether hydropower produced by the SWP pumps at high flow periods could have some such effect on the CAISO grid, but those whom we asked did not see how.

[4] Preliminary analysis suggests that unscheduled generation outages (OUT) may have had a statistically significant effect on Banks usage of electricity during on-peak hours during July 2004–December 2005 (the only period for which we had on-and-off peak hourly data). We were told that SWP generation of electricity is done during on-peak hours.

[5] The beta-coefficient is the amount of change induced in the dependent variable by one unit change in the independent variable. If the beta-coefficient were not significantly different from zero, the effect would be to multiply zero times any MIT or CPS2 value, thus rendering the variable as having no effect on the dependent variable, WFLOW.

Table 13.2 Water flows as a function of mitigations and CPS2 violations for the September–October sub-period

Regression statistics						
Multiple R	0.30526198					
R square	0.09318487					
Adjusted R square	0.08565944					
Standard error	3383.01858					
Observations	244					
ANOVA						
	df	*SS*	*MS*	*F*	*Significance F*	
Regression	2	283434345	141717172	12.3826532	7.6034E − 06	
Residual	241	2758200350	11444814.7			
Total	243	3041634694				
	Coefficients	*Standard error*	*t stat*	*P-value*	*Lower* 95 %	*Upper* 95 %
Intercept	12058.5442	369.109925	32.6692494	1.6785E − 90	1131.4507	12786.6377
MIT	−					
176.94576	84.2192091	−				
2.1010143	0.03667868	−				
342.84551	−					
11.046018						
CPS2	−					
126.33433	37.2163863	−				
3.3945888	0.00080356	−				
199.64526	−53.02339					

every 100 movements in WFLOWs at the Banks Pumps during this September–October sub-period, between eight and nine can be explained by the CAISO grid-wide problems in line MIT and OUT.

One way to cross-check the accuracy of the Table 13.2 findings is to determine whether those years where Delta WFLOWs had to be pumped through Banks Pumps irrespective of problems on the transmission grid were less sensitive to CAISO line MIT and CPS2 violations. We were told by DWR key informants that in wet weather years, the SWP is under considerable pressure to pump the now more abundant water out of the Delta into storage as reserves for periods of shortages. The SWP in other words cannot afford *not* to take advantage of a wet year when dry years before and after are likely.

For DWR purposes, a water year runs from October 1 through September 30, inclusive, and one relatively wetter year in the study period was October 2005 through September 2006.[6] When we ran WFLOW as a function of MIT and CPS2

[6] The "2006" in Table 13.1 is based on a calendar year.

for September/October 2005 and for the combined September/October 2005 and 2006, the results were statistically insignificant in terms of their F-statistics and *p* values. That is, during that relatively wet weather year, WFLOWs through Banks appear to have been more insensitive to grid reliability problems when compared with the overall study period in Table 13.2.

It appears our key informants were correct, that is, large amounts of water had to be pumped that year in spite of problems on the grid that would have affected them in other years. This suggests to us a possible resilience on the part of the SWP during normal operations and/or a CAISO resilience during its own normal operations to get through stress periods without having to rely on Banks flows as they did in other years.[7] As noted earlier, such resilience is what we observed in our CAISO research, where control operators were able in real time to absorb perturbations in their own control variables or bounce back from those shocks while planning the next step ahead.

Eight to nine percent of Table 13.2 variance in WFLOWs explained by problems in the wider electricity transmission grid may not seem a great deal to a reader. But it can be very important to dispatchers in the SWP and CAISO control rooms during these stress months. This 8–9 % may represent something they could manage through better coordination compared with all the other unpredictable factors affecting them during the same months.[8] By "better coordination", we mean attempts to reduce line MIT and CPS2 violations in ways that could improve WFLOWs at Banks.[9] This too could become a part of resilience.

The follow-up question then is this: Are respective control operators and their managers coordinating for better performance during their common stress period? To answer that question requires first talking further with DWR control operators, both to confirm their impressions about September and October being mutual stress periods, and if so, what that may have to do with CAISO grid problems.

Based on the work of Kahneman and Klein [9], there is little reason to assume that control operators in respective infrastructures actually know for a fact that problems in one are causing problems in the other. Domain expertise may be so intensively demanding in each infrastructure that problems, when they arise, have to be settled quickly in real time as an infrastructure-specific problem. When we

---

[7] The thrust of this argument is that there may be reciprocal resilience on the part of each infrastructure. In this view, what makes the wet weather year of 2006 special is that the SWP was able to detach its management of the Banks pumps from CAISO requirements, and CAISO was able to function without relying on Banks water flows as part of its load. Before this can be asserted with confidence, however, much more empirical research would have to be done.

[8] An important next step would be to determine how well the daily relationship holds when we drill down to the hourly level for September and October. To do so would require hourly WFLOW data. Access to such information has been restricted for security and competitive market reasons.

[9] It is interesting to note that those 15 days when Banks was shut down for scheduled maintenance and repair were days (with respect to water flows) and hours (with respect to electricity inflows) when CAISO operators managed to have fewer line mitigations and CPS2 violations compared to study period averages.

asked a senior manager of the SWP control room whether he had noticed anything out of the ordinary about September and October with respect to Banks WFLOWs during the study period, he said this was a period of high diversions, in part due to environmental standards coming into play those months. As for CAISO transmission grid issues, he felt CAISO was apt to call with instructions at any time.

13.4.4 Specific Implications with Respect to Infrastructure Resilience

Our findings suggest a useful differentiation of resilience into at least three types, not all seen by the end-using consumer or customer of the critical service. The type we have been talking about in this chapter is *precursor resilience*, which end-users do not see. This is the ability of control operators to correct and adjust operations in real time as needed to keep or bring back conditions within an acceptable bandwidth of limits and thus render outputs and services reliably stable.[10] Precursor resilience allows operators to manage stress and unexpected difficulties while still maintaining a robust service to customers. The other two types of resilience, which end-users do see, involve the ability of the critical service in question to "bounce back" from an actual loss of service, be it through service disruption or system failure.

The ability is bounce back from a disruption, that is a temporary loss of service, involves a set of control operator skills and processes which term *resumption resilience*. Here, operators are able to quickly assess the cause of the disruption and evaluate/improvise options to resume service. Some of the options are built into design or protocols that come into play only in periods of disruption. Should, however, the infrastructure system itself fail, the challenge of recovery now presents itself to operators. Failure means operators have lost the very control variables with which to manage reliably. It is worth emphasizing that, despite infrastructure failure, control operators and their management skills do not disappear. Indeed, operators have important skills and roles that constitute *recovery resilience* for the system after failure. One of the important features of recovery resilience is the intense interorganizational coordination to recover the infrastructures and connections with other systems they depend on and the users who depend upon them.

The distinctions suggest that infrastructure resilience might be better thought of as a continuum of skills and scope that extends across stages of an infrastructure's cycle of operations—including normal operations as well as disrupted, failed and recovered operations—rather than being a factor or capacity that is "on" during disruption or worse, while "off" the rest of the time. We must underscore that such

[10] The process of precursor resilience is described in more detail as bandwidth management under active analysis in Roe and Schulman [1].

resilience should itself be managed and continually reassessed by engineers and practitioners, whether directly as we did in [1] or indirectly as done in this chapter.

To bring the discussion back to our case study, we conclude that precursor resilience in water operations with respect to perturbations in electric transmission grid was evident during at least one time period when both infrastructures are stressed but maintain normal operations. That is, the SWP was able, with precursor resilience to ensure reliable WFLOWs during a period of stress without a temporary loss of service (e.g. an unexpected stoppage in pumping[11]), even when CAISO, its supplier of pumping electricity, was having more difficulty than usual in ensuring its own reliable operations.

13.5 Conclusion: Precursor, Resumption and Recovery Resilience at the ICIS Level

By way of concluding, let us now shift from specific case of CAISO and the Banks Pumps to the more general case of two interconnected critical infrastructures. What does the above imply about infrastructure resilience in its variants at the ICIS level?

Think of the world as occupied by two infrastructures (CIS1 and CIS2), each of which has different stages of operation and both of which are connected through their respective management variables (i.e. the variables could be the same control variable or they could be interconnected as described in the preceding case study via an overlapping stress period). The stages of operations in each infrastructure are again: normal, disrupted, failed, recovered, and, if necessary, a new normal after recovery. In this world, the following three definitions, which we find helpful, are consistent with the above analysis:

Definition 1 Operations in an infrastructure are **robust** with respect to disruptions or failure in another infrastructure when the former continues normal operations in the face of the latter. The normal operations may well depend upon the **precursor resilience** of that infrastructure in managing its reliable operations in the face of surprising or unexpected input conditions from the other infrastructure.

In this view, CIS2 is *robust* with respect to CIS1, when CIS2 can reliably manage its normal operations despite surprises or shocks introduced by CIS1. CIS2 absorbs or bounces back from CIS1-induced perturbations in ways that do not disrupt safe and continuous provision of CIS2 services. In the terminology of high reliability management, an infrastructure's process variance (the ability of its control operators to move across different performance modes as conditions change) is *robust* with respect to its low or stable output variance (control

[11] None of the days of zero water flows through the Banks Pumps during the study period occurred in September or October.

operators are thereby able to maintain stable services in spite of the perturbations of the infrastructure to which it is connected).This leads to a second definition:

Definition 2 Operations in an infrastructure are **resumption resilient** with respect to disruptions or failure in another infrastructure when the first infrastructure returns to normal operations after its own disruption in the face of the initiating perturbations in the other.

CIS2 is *resumption resilient* with respect to CIS1, when CIS2 absorbs or bounces back from CIS1 surprises or shocks that have actually interrupted CIS2 normal operations, for example, that have led to a temporary loss in CIS2 service. In the earlier terminology, an infrastructure's process variance is *resilient* with respect to its output variance, when the ability of its control operators to move across different performance modes is sufficient to return infrastructure operations to their normal levels of low or stable output variance, despite conditions in the other infrastructure.

Both the preceding definitions treat their resilience as a property of an individual infrastructure, in this case CIS2. For recovery resilience, however, we offer the following definition.

Definition 3 Operations in an infrastructure are **recovery resilient** with respect to the interconnected recovery of another infrastructure.

When both are able to coordinate the restoration of their respective control variables and assets. Here, resilience is intensely interorganizational in focus. In the earlier terminology, the infrastructures involved have sufficient process variance to enable the cross-infrastructure and cross-user coordination.

Understanding these types of resilience and their requirements would be a first step in a new approach towards the engineering and design of complex infrastructure systems from a better risk management perspective. Engineers need to recognize that they cannot design systems that are "damned foolproof" and that highly reliable systems are managed to be *reliable beyond design*. We believe that all "designers", be they engineers, policymakers or top-level managers, must trust and facilitate the skills of control operators to add the necessary component of resilience to the engineered foundations of high reliability.

Acknowledgments Over the last 3 years, the authors have been very fortunate to talk to many key informants on Sacramento-San Joaquin Delta infrastructures and to work with other team members in doing so as part of the University of California Berkeley RESIN (Resilient and Sustainable Infrastructure Networks) project supported by the National Science Foundation. Special thanks go to Benjamin Baker for his work on the Sect. 13.4 case study. We also appreciate the editorial assistance of Ingrid Bouwer Utne and Per Hokstad (see especially Utne et al. [10]). None are responsible for any errors of fact, analysis or interpretation that have intruded into this chapter. This material is based on work supported by the National Science Foundation under Grant No. 0836047. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

References

1. Roe, E., & Schulman, P. (2008). *High reliability management*. Stanford: Stanford University Press.
2. Noyes, J., & Barnsby, M. (2002). *People in control*. London: IEE.
3. Stanton, N., Salmon, P., Jenkins, D., & Walker, G. (2009). *Human factors in the design and evaluation of control room operations*. Boca Raton: CRC Press.
4. Ivergard, T., & Hunt, B. (2008). *Handbook of control room design and ergonomics*. Boca Raton: CRC Press.
5. Klein, G. (1998). *Sources of power*. Cambridge: The MIT Press.
6. Perrin, C. (2005). *Shouldering risks*. Princeton: Princeton University Press.
7. Sanne, J. M. (2000). *Creating safety in air traffic control*. Lund: Arkiv Forlag.
8. Woods, D., & Hollnagel, E. (2006). *Joint cognitive systems: patterns in cognitive systems engineering*. Boca Raton: Taylor & Francis.
9. Kahneman, D., & Klein, G. (2009). Conditions for intuitive expertise. *American Psychologist,* 64, 515–526.
10. Utne, I. B., Hokstad, P., & Vatn, J. (2011). A method for risk modelling of interdependencies in critical infrastructures. *Reliability Engineering and System Safety,* 96, 671–678.

Chapter 14
Organizational Challenges Regarding Risk Management in Critical Infrastructures

Petter Almklov, Stian Antonsen and Jørn Fenstad

Abstract Understanding the interconnections between critical infrastructures is a demanding task. This is even more the case when one includes their organizational contexts. In this chapter, we discuss some of the organizational challenges that have to be addressed when analysing and managing risks that involve several infrastructure sectors. The infrastructures of today are often run by networks of private and public entities, rather than single utility companies. Consequently, the number of organizations that need to be involved to map, analyse and manage risks that cross-sectors is increasing. The organizational changes also imply that work is managed and coordinated in ways that imply a stricter focus on efficiency and accountability with regard to core tasks and responsibilities. We argue that cross-sectorial safety management requires other organizational qualities as well. We outline a landscape where technologies become increasingly interconnected at the same time that the organizations managing them become increasingly fragmented. Risk identification and management requires increased transparency between companies that have few incentives to share information or cooperate. We present a set of recommendations and suggestions with relevance for public agencies and for infrastructure owners on how to address the organizational and institutional challenges born out of these processes.

P. Almklov (✉) · S. Antonsen · J. Fenstad
NTNU Social Research—Studio Apertura, Trondheim, Norway
e-mail: petter.almklov@samfunn.ntnu.no

S. Antonsen
Safetec, Trondheim, Norway

P. Hokstad et al. (eds.), *Risk and Interdependencies in Critical Infrastructures*, Springer Series in Reliability Engineering, DOI: 10.1007/978-1-4471-4661-2_14,

14.1 Introduction

While the majority of this book is concerned with methods for analysing interdependencies and the risks they entail, this chapter provides an outline of the organizational challenges that one will encounter when working with risk analysis and management across organizational and sectorial boundaries in the infrastructure sectors. Our key observation is that interdependencies and couplings across sectors pose major coordination and cooperation problems that are not trivial to solve. This affects both the ability to analyse risks and vulnerabilities and the capability to deal with emergencies. We discuss this in the light of the institutional changes in the public sector the last decades. These changes, usually referred to as new public management (NPM), have led to organizational fragmentation in many critical infrastructure sectors. NPM generates a need for new mechanisms for cooperation and coordination within and across sectors. We will discuss some of the research on NPM and organizational fragmentation for two reasons: (a) the organizational fragmentation it entails causes coordination issues with many similarities to those caused by the increased interdependencies between infrastructures and (b) for implementing cross-sectorial risk management, one needs to understand the organizational landscape of critical infrastructures. NPM is a key factor in this, as it influences both how the individual companies operate and the way they *co*operate within and across sectors.

After a brief introductory background, discussing critical infrastructures in the light of societal safety and vulnerability (Sect 14.2), the remaining chapter is structured as follows: in Sect. 14.3, we describe how critical infrastructures are increasingly *interconnected*; in Sect. 14.4, we describe how the organizations operating them are increasingly *fragmented*; and in Sect. 14.5, we discuss the integration paradoxes born out of these developments. We seek to understand the coordinating mechanisms and practices in play, and in Sect. 14.6, we suggest some *organizational requirements* for cross-sectorial risk analysis and management.

14.2 Dependencies, Societal Safety and Critical Infrastructures

Societal safety refers, in the words of [1][1] to "society's ability to maintain critical social functions, to protect the life and health of the citizens and to meet the citizens' basic requirements in a variety of stress situations". Broadly put, it refers to the absence of events that threaten societal functions, *that is*, harmful aggregates of smaller events or the typical catastrophic scenarios. The concept is inextricably linked to that of *vulnerability*. While societal safety is constantly threatened by

[1] They again refer to a Norwegian Parliamentary White Paper [2].

external forces like natural disasters, pandemics and international political crises, the debate on societal safety to a great extent revolves around society's vulnerability to such events. Will the threat harm functions on which we rely? The volcanic ashes over Northern Europe in 2010, for example, were only a threat to societies depending on air transport. 50 or 100 years ago, it would have hardly been noticed. Our vulnerability was thus a consequence of the fact that society is organized around the expectation of a functioning air transport system.

To understand, societal safety is a matter of understanding external threats and the ways these may harm society. Moreover, important vulnerabilities in modern societies do not depend on nature or other external factors to be harmful. A computer software virus can paralyse medical ICT systems, systems which doctors today have just recently come to rely on. Systems like this make society more effective, but as we rely and *depend* on them, we are also increasingly vulnerable to breakdowns.

Critical infrastructures are systems taken for granted. Moreover, they are themselves often built on the expectation of the functioning of *other* infrastructures. This goes both for the technical infrastructure itself, like for water pumps that depend on electricity, but maybe as important is the operational context around it: ICT-based maps, GPS and mobile networks in emergency handling, the dependency on transport to get critical spare components and so on. The tendency to take infrastructures for granted may be a problem when analysing risk, as it may challenge our imagination to really understand how they may be interconnected in different situations. Dependencies do not follow institutional or organizational boundaries, so when analysing and managing risk, several actors have to be involved in this imaginative work.

Since critical infrastructures are systems upon which we build new systems (*e.g.* of production) and that we take for granted in our daily lives, the socio-economic cost of a breakdown is not only the cost of the loss of service itself, but also that of cascades of problems in the systems and societal functions that depend on the failing infrastructure. For example, the cost of a prolonged blackout of the critical infrastructure *par excellence*, electric energy, would be magnitudes higher than the price of delivered electricity in the same period. The price of the *products* delivered by an infrastructure, fresh water, electric power, mobile phone services and access to roads does not at all reflect the value of the production *that depends on* these products. Private or publicly run, critical infrastructures cannot be treated as any business and must be regulated according to society's dependence on them. Moreover, many, but not all of them are what economists call *natural monopolies.* This means that the cost of building a parallel, competing system is so high that it in practice is impossible. This is typically the case for water supply, railroads and power lines. Such monopolies, on which great societal value depend, are always subject to strict regulation or direct public ownership.

14.3 Tight Coupling and Complexity

Today critical infrastructures are growing increasingly connected and interconnected. The failure of the *Galaxy 4* telecommunications satellite in 1998 can serve as an example in this respect [3]. The failure of the satellite immediately knocked out 90 % of all pagers in the US, which seriously affected communications in hospitals and other vital medical institutions. In addition, the satellite failure also disrupted several banking and financial services (*e.g.* credit card transactions). There are numerous other examples of failures in one infrastructure that can lead to disruptions in other infrastructures and in the process, lead to serious human, material and economic consequences. The existence of such cascading effects highlights the tight couplings between various infrastructures and also a degree of complexity that makes these interconnections difficult to identify and manage.

The concepts of coupling and complexity were introduced in safety research by Charles Perrow's seminal work *Normal Accidents* [4]. While Perrow's framework was not initially designed to address infrastructure interdependencies, his key concepts can be instrumental in highlighting some of the challenges related to infrastructure interdependencies. Coupling refers to the degree of interconnectedness in technological systems, *that is*, the extent to which failures are able to escalate rapidly and spread to other parts of the system, or into other technological systems. The concept of complexity refers to the nature of interactions between parts of a system or in our case between infrastructures. If a technological system or an organization is characterized by linear interactions, it will be largely transparent, predictable and follow familiar sequences, much like an assembly line. On the other hand, if it is a system of complex interactions, its processes will be characterized by "unfamiliar sequences, unplanned and unexpected sequences, and either not visible or immediately comprehensible" [4, p. 78]. This is the hallmark of a complex system.

In Perrow's view, tightly coupled (and complex) organizations will eventually produce large accidents. Researchers within the high reliability organization (HRO) approach, however, argue that some organizations that are both tightly coupled and complex have remarkably good safety records. The HRO researchers point towards features like the ability to reconfigure the organization during crises where local expertise is given authority to solve crises. Another such feature in these highly reliable organizations is that they maintain organizational redundancy so that employees have overlapping tasks and competences in order to correct each other's errors. Tight coupling between infrastructures is by no means a new phenomenon. For instance, key components within water and sewerage and transportation are to a large degree dependent on electrical power production. The system's dependence on other infrastructures is also increasing as more components are automated. However, many of these classic dependencies are largely unidirectional. While the water pumps required to pump water to an elevated basin cannot function without electricity, there will not be many ways the loss of water pump pressure can affect the production or transmission of electricity.

The increasing tendency towards *inter*dependencies between infrastructures is a new phenomenon. It may be argued that several critical infrastructures are becoming both more tightly coupled to each other *and, at the same time,* more interactively complex. For instance, computers and software are dependent on electricity, but the very same computers and software may be strongly integrated in the production of electricity. The existence of such "feedback loops" means that the potential for cascading effects will be increasing, at the same time as the intersections between infrastructures are becoming more and more opaque. This combination may lead to surprising interactional effects, and as such require some imagination to be prevented.

Several examples of interdependencies are discussed elsewhere in this book (see Chap. 2). Two classic examples are common cause failures, for example due to geographical co-location of weak points, and cascading failures due to the tight interactions between ICTs and electricity.[2] The former example is related to the spatial proximity between two or more infrastructures. This proximity means that they might be exposed to the same external threats, such as explosions, fires or natural disasters. A well-known example of this is the location of power lines and optical fibre cables in cable culverts underneath the roads. While placing different cables in the same culvert involves some economic advantages, it increases vulnerability since single events can disrupt services related to electricity, ICT and transportation. A fire in a power cable in such a culvert in Oslo demonstrated the potential of such events, as it harmed a several infrastructures and services in unexpected ways (see Chap. 4). Even more, intricate interdependencies are probable outcomes of the computerization and automation of infrastructures which have taken place over the last two decades [6]. In the digital age, society's critical infrastructures rely on the functioning of ICT systems, as ICT software and hardware are integrated in the ability of other sectors to uphold their services. It is thus a vulnerability of increasing importance.[3] For example, a key conclusion in Roe and Schulman's [8] book on the Californian electricity system is that its reliability depends on the performance of skilled control room operators handling disturbances and variations. An implicit consequence of this is an accompanying reliance on the functioning of ICT equipment, such as sensors and remote controls, without which these professionals cannot operate.

The vulnerability introduced by infrastructure interdependencies has previously been discussed in [9]. He makes an important point when stressing that tightly coupled systems with risks crossing organizational boundaries will demand *greater transparency* and knowledge of operations *across organizations*:

> It is one thing for a single organization to figure out how to operate reliably on its own, and then to carry out the required structural and management reforms successfully. It is

[2] According to [5], unidirectional cascades between energy and telecom are by far most commonly documented cross-infrastructure cascades.

[3] See [7] for a discussion of how the increasing complexity of ICT systems introduces new risks that are hard to understand and manage.

> another thing for a *web of interdependent organizations* to do the same thing. In tightly coupled systems, simply identifying vulnerabilities, let alone managing them, is a daunting task. In a sense, risk migrates to the weakest part of the system, but due to overall complexity, the migration occurs without anyone's knowledge, and without a clear understanding of where the weakest links are located. Yet not identifying such vulnerabilities and risks leave systems unprepared to function during extreme events. Resolving this analytic problem will require much greater transparency and knowledge of operations across organizations than has ever existed in the past [9, p. 73].

Importantly, this transparency cannot be created by finding technological solutions alone. In fact, the coupling points between infrastructures must be *recognized* in the first place, in order to create information systems that provide the necessary information flow between sectors. This is the process of *problem framing*, that is, the "selection and interpretation of phenomena as relevant risk topics" [10, p. 48]. As indicated in the above quote from LaPorte, identification of relevant risks is difficult enough within the borders of an organization. When the possible causal chains span across several sectors, concern several institutional levels, and involve both public and private actors, risk identification, analysis and management is even more cumbersome.

14.4 Organizational Fragmentation and its Effects on Infrastructure Risk Management

A few decades ago, most critical infrastructures in the OECD countries were publicly owned and run by integrated utility companies. In the era of the Cold War, controlling infrastructures was a matter of national security. This started to change, however, in the late 80s, with the dawn of a new era of public governance called NPM. Since then, NPM has influenced most public sectors, though to varying degree in different countries. NPM has meant a quite radical reorganization of critical infrastructure sectors in the countries that have embraced its principles most wholeheartedly [11, 15].

Broadly put, NPM can be seen as the introduction of a set of principles and methods for organizing from the private sector into the public sector. Functional splitting (typically between a buyer and supplier in an internal transfer price system), outsourcing of work processes or full-blown privatization are the most typical organizational changes. The most visible trait of NPM is the reorganization and renaming of public bureaucracies. These new organizations are based on an organizational philosophy centred on production, accountability and transparency, in place of the command and control of the old hierarchic bureaucracies. Though often referred to as a de-bureaucratization of the public sector, NPM is arguably a shift to a new form of bureaucracy that is based on principles of accounting [12, 13]. Within the logic of NPM, each organization is to focus on its core production. There has been a shift from being *responsible* for a broadly defined area of responsibility to being *accountable* for the production of a limited set of

specified outcomes. The organizations' performance is typically measured through selected key performance indicators (KPIs), and they are held accountable for their performance according to these indicators. Thus, at least when successfully implemented, NPM provides transparency and control, and the public can place detailed "orders" for products to be delivered by the involved actors in the infrastructure sectors.

NPM gives accountability and transparency by fragmenting organizations into entities that produce countable standardized products and services that are easy to monitor. The fragmentation is as such designed to improve control and transparency, but it is so from the accountant's, not the (necessarily) engineer's perspective. Thus, activities that from an engineering perspective could very well be managed by one organization are divided among different actors to improve accountability from an economic or regulatory standpoint.[4] Based on this logic, NPM has implied a transition in the critical infrastructure industries from integrated companies to "single-purpose organizations", with specialized and non-overlapping roles and functions. This has led to cooperation and coordination issues in several public services [13, 14, p. 1060].

This organizational fragmentation has consequences for reliability of infrastructure sectors, at least in the sense that it changes the practices by which reliability is upheld.[5] There is a distinct development where the involved companies, both in the public and in the private sectors, focus narrowly on delivering according to a few KPIs within their core area of responsibility. In several sectors, this NPM driven focus on accountability and KPIs has led to coordination challenges for more complex tasks *outside* these core responsibilities. This narrowing the focus within individual infrastructure sectors, though it has its advantages, makes it organizationally more challenging to coordinate and perform cross-sectorial risk management.

In empirical studies [16][6] of how public sector reorganization affects critical infrastructure reliability, we have seen examples of the pros and cons of NPM in terms of safety. Day-to-day reliability is often strengthened by the focus on core tasks and strict accountability regimes by which this is followed up. However, NPM-inspired ways of organizing infrastructure production also generate organizational weaknesses that can influence the reliability of critical infrastructures. Some of these weaknesses are also highly relevant for the present discussion of risks across sectors.

Three different sectors were studied: electricity networks, water supply and ICT systems at a hospital. In all sectors, NPM had led to variants of functional splitting

[4] For example, electric power production and grid operations are closely connected activities that are typically separated by law, to avoid undesirable cross subsidizing between the grid operation which is a natural monopoly and the production which is not. A similar split is seen in the European railroad sector, where the railroad systems (monopolies) have been split from the operation of trains to improve competition.

[5] See [15] and (Antonsen et al. 2010). See also [8].

[6] The project report is in Norwegian, but [17] and [15] report some of the findings in English.

along the value chain. Consequently, there were *more organizations involved* in the infrastructure production. One of the electricity network companies we studied can serve as an example of a typical NPM-inspired restructuring. The previously publicly owned integrated utility company had been transformed into a listed private company (though still with substantial public ownership). Throughout the Norwegian energy business, integrated companies have, by law, been separated into network companies (owning and operating the grid) and energy and brokering firms. An important reason for this is that network companies are monopolies. In order to have a functioning market for produced electricity, where the customer is free to choose between different energy providers, the networks have to be "neutral" in terms of whose energy is transported. In addition to this split by law, the network company that was studied, and several other companies, had chosen to outsource its operational work. This meant that the fitters now belonged to other companies competing for operation and emergency preparedness for different sectors of the grid and for specific "packages" of maintenance work. Internally, the company itself was split into a network company (the actual concessionaire) and two internal suppliers. One internal supplier handled the planning functions and did much of the follow-up of the fitting contractors as well. The other ran the control central. Though belonging to the same corporation, these companies were regarded as suppliers to the network company and sold services to the network company and to each other according to formalized contracts. The remainder of the network company, who owns the grid, was basically left with some administrative functions. As such, one integrated utility company was split into a network of cooperating businesses coordinated by contracts and business relationships. Though this reorganization has many advantages, also in terms of reliability, it introduces new organizational complexity.

At first glance, one would suspect that more organizations involved would lead to less transparency, but this is not univocally so. Organizational structures like the one chosen by the electricity company are based on very standardized forms of information and communication management. To be allowed to work for the network company, the suppliers must adhere to strict reporting regimes and standardized ways of operating. This we call *modularization* [17]. A module is interchangeable, because its interface to the system, *that is*, the specifications of the work package, is standardized. The network company can specify what kind of output they need from each of the suppliers, the modules of their system, and demand, under the threat of economic sanction to get it. Thus, though such a system is more complex organizationally, the communication and coordination are in many ways more strictly organized.

An effect of a modularized system is that informal organizational structures are weakened, and communication patterns and cooperation modes are standardized (This is a tendency seen all over the studied sectors.) Operative personnel describe a change from being craftsmen with a fair amount of autonomy to a situation where their work is more strictly governed, where they do the job that is ordered no more or less and where their knowledge and feeling of responsibility for the network as such is weakened. The personal networks across functions are also

weakened, as they belong to different organizations. Good relations and dialogue between planners (with system knowledge) and doers (with practical knowledge) are in particular a potent source of robustness and risk sensitivity. In the old integrated companies, personal networks could facilitate smooth operations and information flow that fostered many of the typical characteristics of a robust organization.[7] These informal organizational traits are more problematic, however, when they span across boundaries between contractual partners. In cases where operational work is outsourced, it is important that competition for contracts is fair and transparent. In this respect, personal networks across functions may be problematic and may even be actively discouraged.

Emergency management depends on good planning and exercises, but improvisation is often a critical element, for example [19–21]. The presence of broad informal networks and the competence they may foster is an invaluable resource in safety and emergency management, for example [18] maybe particularly when improvisation is needed. Trust-based relationships and open communication between people with different responsibilities and tasks are also sources to a creative identification and understanding of complex risks. Eroding networks, and changed career paths due to NPM, may also reduce the number of personnel with knowledge of both practical operational work and a more overall systematic understanding. In general, modularization and related developments increase the organizational distance between personnel with practical knowledge of the system and those with a systematic overview.

A common concern when NPM is introduced in critical infrastructure sectors is that the drive for effectiveness may lead to cheap solutions and reduce technical and organizational redundancy. Our studies of Norwegian infrastructures are inconclusive of whether this is the case [16]. However, NPM introduces some issues of *coordinating* redundancy. The most interesting case, which was also observed by the regulator of the electricity networks in Norway, was that the overall redundancy of fitters to handle emergencies in the industry had been reduced and that several network companies had contracts with the same contractors. Thus, while the emergency response capacity was very good for typical incidents, and more effective than before, there was less slack in the industry as a whole to tackle extraordinary incidents. If several network companies needed assistance, the extra personnel could be contractually obliged to be several places at the same time and as such a false redundancy. One thing this example illustrates is that the regulator needs not only to look at the contracts between buyers and suppliers, but also to check their realism in extreme cases. One example of such cases, challenging the realism of contracts, would be emergencies that influence several sectors.

Transparency is a key goal of NPM and the companies do achieve a better insight into work practices and detailed performance. The infrastructure and the

[7] The role of informal networks is described in some of the literature on *High Reliability Organizations, for example* [18].

work processes are better documented, and responsibilities for core tasks are better defined. This improves the basis for cross-sectorial risk analyses. However, as the operational personnel are attached to organizations external to the infrastructure owner, they basically report what they are paid to report and nothing else. Reports and databases capture a limited amount of standardized items and will not capture the peculiarities and heterogeneity of a complex system. In the Norwegian water supply infrastructure, for example, with components up to 100 years of age and a correspondingly long operational history, it is not easy for an outsider (without operational knowledge) to design a good reporting system covering all potentially relevant details. Moreover, not reporting more than necessary and keeping as much operational knowledge internally can be a rather smart strategy for contractors, as too conscientious reporting would basically make them easier to replace.

Thus, though improved reporting and documentation is often a consequence of NPM, the channels for collective reflection about risk are narrower and less dynamic. To paraphrase Turner and Pidgeon's [22] discussion of culture, the systems are both *a way of seeing and a way of not seeing*. A challenge in a modularized system is to be able to transport a broad enough understanding of operational knowledge across organizational boundaries to be able to make risk assessments both within and across infrastructure sectors.

14.5 Coordination and Cooperation Across Organizational Boundaries: an Integration Paradox

In the two sections above, we have described two parallel developments that must be dealt with in order to manage risks in infrastructure sectors. First, we discussed how the various infrastructures are growing more *tightly coupled*, as they build and depend on each other to function. Particularly important in this respect are the new information and communication technologies, which are weaved into the fabric of the traditional ones (see Chap. 10). Second, we discussed the *organizational restructuring* of NPM, and the mechanisms by which organizations within the networks of organizations maintaining an infrastructure sector coordinate themselves and cooperate. "Coordination is managing dependencies between activities" according to Malone and Crowston [23]. NPM implies an increased division of labour between (an increasing number of) organizations involved in infrastructure production and new ways of coordinating activities between these entities. Technological development on the other hand increases the *dependencies* between infrastructures. Together, these developments create new coordination issues that need to be addressed.

Technically, risks are becoming increasingly *integrated* and interconnected. At the organizational level, however, the organizations that are responsible for dealing with these risks are becoming increasingly *fragmented*. Seen from a safety and reliability perspective, this paradox involves a major challenge when it comes to the identification and mitigation of cross-sectorial risks. Organizational

fragmentation and tighter technical coupling mean that safety is increasingly dependent on the involved actors' ability to cooperate across organizations. In most cases, this cooperation will involve both public and private organizations as both the "seeds of disaster" and the "roots of response" may be found in the private sector [24].

Integrated risk analysis and management implies the enrolment of a diverse conglomerate of actors horizontally and vertically in the public sectors, as well as NGOs and private entities, organizations "with fundamentally different values, cultures and goals" [25, p. 66]. When divided across several organizations, the process of problem framing becomes inherently difficult. Each actor is likely to define their own set of problems related to their core tasks and competencies, and the outcome for which they are accountable. The risks and vulnerabilities that arise in the interfaces between institutions and organizations, and cannot be said to "belong" to any single actor, are far more difficult to assess and to prepare for. Moreover, institutional fragmentation within sectors may make it hard to understand who has the required information or knowledge or the responsibility for different tasks. Consider, for example, the electricity network organization above: it is not trivial for an outsider to understand with whom to cooperate in different stages in a risk management process. While the power network companies are very conscious of the criticality of their product, other sectors like mobile telephone services (and their sub-contractors) may be harder to get hold of and involve. This gets even more complicated with ICT, as the network organization is typically more extreme there. Trying to understand the chain of suppliers and sub-suppliers (of software, hardware and services) and their potential impact on overall system reliability is largely an impossible task.

Systemic risks cross the boundaries between different infrastructure sectors, but also different levels in the sectors. Cooperation between managers and system specialists may improve safety towards cross-sectorial risks, but one would also need to involve practitioners in risk identification and mitigation. Operational practical knowledge is less "mobile" across organizational boundaries. Especially local interdependencies, as the incident at the Oslo railway station, may depend on the local or practical knowledge to be identified and understood. The observed increase in distance between the personnel with operative knowledge and with system knowledge increases the danger that cross-sectorial risk analyses become paper exercises, unless operational knowledge is specifically sought included. We quoted [9, p. 73] calling for "much greater transparency and knowledge of operations across organizations". While transparency, in the form of sharing data and information, may be easier today than before, a challenge for risk analysis across sectors is to include operational competence.

14.6 Recommendations

Based on the above discussed research and a series of workshops with infrastructure owners and authorities in Norway, we suggest some recommendations for the analyses of risks and vulnerabilities that cross infrastructural boundaries and for the preparedness to handle such threats when they materialize.

Knowledge of interdependencies: This book is a good starting point for improving the methodology for risk analyses. It is important to improve the knowledge of typical interdependencies, but maybe as important, to raise awareness of the fact that many interdependencies can be atypical and hard to predict. Recent research by [5] suggests that, contrary to current beliefs, cascades are most often found in a rather limited set of connections between infrastructures and hence that their pathways are not necessarily as unpredictable as often assumed. Risk management thus requires the creativity and technical knowledge to envision the atypical and "weird" incidents, but also the ability to focus along known typical pathways where the dependency is strong enough to result in cascading effects. Methods and best practices on how to identify, map and analyse such risks should be further developed on a national/regional level to support local risk analyses, grounded in local realities and organizations.

Knowledge of the process of analysing interdependencies: An important part of the documentation proposed in the item above must address the organizational, institutional issues involved. For example: How to get information from different private and public actors? Who has responsibilities for providing information and participating in work? What is available in existing databases and documents? The institutional landscape is complicated, and in many cases, it is hard to know whom to contact to get information on vulnerabilities and risks. This is especially true in infrastructure sectors are either wholly or partly privatized. It is also often the case that an organization with responsibility for an infrastructure does not do any operational work, so that if one wants to discuss operational practicalities, one has to address the contractors.

Another issue that should be provided in supporting documentation is guidelines for handling information sensitivity and security issues. Much information about the vulnerabilities of critical infrastructures is sensitive. This can be due to security and due to commercial considerations in the case of private organizations.

Incentives to contribute: Cross-sectorial risk is an arena where responsibilities are seldom clear cut. To analyse and manage risks, involvement is needed from several actors that do not have economic interest in participating and that may not be contractually or legally obliged to participate. Quite naturally, private companies look at the economy when contributing to work like this, but as previously argued also public entities are managed in a way that narrows their focus. Thus, to ensure robust enrolment of public entities, their contribution to cross-sectorial risk management should be specified in the objectives by which they are held accountable. As it is today, many public employees experience that they are transgressing their mandates and not producing according to their performance

indicators when working outside their core areas of responsibility. Without specific incentives, economic or otherwise, cross-sectorial risk management will be an uphill struggle against other more concrete priorities.

Integration of system knowledge and operational knowledge: NPM increases the organizational distance between operational personnel and the ones with responsibility for the system as a whole. Broadly put, the principles of NPM introduce more marked separation between planning and execution. It is a common trait of cascading events crossing over sector boundaries that their causes and solutions involve both factors from the practical operational domain and systemic factors. Thus, risk identification and management depends on cooperation between personnel with competence on both types of factors. We fear that NPM may increase the risk that cross-sectorial risk management may become paper exercises ignoring practical operational issues, due to problems integrating these perspectives across organizational boundaries. To the extent possible, contracts and concessions should seek to address this problem.

Drills: Realistic drills are probably the most effective way to work with the issues discussed above. By specifically selecting cases that challenge the organizational structures and boundaries, coordination challenges, both in emergency handling and in the risk identification phase, are exposed. For example, involving private infrastructure owners and their operational contractors in drills provides good training in handling emergencies and in identifying who should be involved to map and understand uncertainties. In Norway at least, the drills in most infrastructure sectors are of limited scope, and complex organizational challenges are typically avoided, for example by not involving private contractors or other sectors. In our meetings with infrastructure owners and authorities, there was a general consensus that the most useful drills for understanding cross-sectorial risks were the rare examples of regional exercises that involved personnel from a several sectors. Drills should address complex problems technically, but equally so be designed to address complex interorganization cooperation.

While the above discussion and recommendations gives some broad indicators in how to approach the organizational landscape of critical infrastructure protection, more concrete interventions would need to be situated in the specific context. However, *examples* of concrete interventions inspired by our discussion could be (1) Create cross-sectorial forums where personnel from connected infrastructures are given the time and opportunity to identify couplings and vulnerability. (2) Cross-sectorial exercises and emergency drills. (3) When working with scenarios, always try to identify at least one that is "worst case" in terms of how complex it would be organizationally. (4) For authorities, install directed incentives and regulation for cross-infrastructure risk analysis and drills. (5) Partly as a cause of NPM, most infrastructures have more comprehensive documentation than ever. Dedicated projects should be undertaken to establish data-sharing platforms across sectors. This may require public incentives/regulation.

This list of examples is by no means complete and is meant to illustrate how the general discussions of this chapter can be operationalized.

14.7 Conclusion

Two developments, the increased technical interdependency of infrastructures and fragmentation of the organizations that operate them, both create an increased importance of cooperation between organizations in risk management. Risk migrates across infrastructures, and as it does, it forces work with risk analyses and management to cross organizational boundaries. This chapter addresses this issue and discusses it in the light of the nature of organizational and institutional boundaries in the current infrastructure sectors.

We have suggested that a critical issue to overcome in this respect is to be able to access the necessary amount of operational knowledge in the risk identification process. To achieve this, cooperation must be vertical within sectors as well as across sectors. We have outlined some challenges and solutions to such work.

When risk migrates across organizations, it is not always clear with whom responsibility lies. In addition, the post NPM organizations are also designed to focus narrowly on core tasks. Consequently, obtaining the necessary information and cooperation from different companies involved in the infrastructure production is not always straight forward. In many cases, good solutions probably lie on a regulatory level by allocating the necessary resources and incentives to work across sectors. On a lower level, much can be achieved by infrastructure owners actively engaging relevant actors in the private and public sector and not letting the risk analyses, risk management and the scope of exercises stop where it is organizationally convenient.

References

1. Olsen, O., Kruke, B., & Hovden, J. (2007). Societal safety: Concept, borders and dilemmas. *Journal of contingencies and crisis management, 15*, 69–79.
2. MJP. (2001). *Societal safety: The road to a less vulnerable society*. Norwegian parliamentary white paper no. 17 (2001–2002) Ministry of Justice and the Police, Oslo.
3. Rinaldi, S. M., PeerenboomJ. P., et al. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *Control Systems Magazine*, IEEE 21(6):11–25
4. Perrow, C. (1984). *Normal Accidents*. New York: Basic Books.
5. Van Eeten, M., Nieuwenhuijs, A., Luiijf, E., et al. (2011). The state and the threat of cascading failure across critical infrastructures: The implications of empirical evidence from incident reports. *Public Administration, 89*, 381–400.
6. Rinaldi, S. M., Peerenboom, J. P., & Kelly, T. K. (2001). Identifying, understanding, and analyzing critical infrastructure interdependencies. *Control Systems Magazine, IEEE, 21*, 11–25.
7. Hanseth, O., & Ciborra, C. (2007). *Risk, Complexity and ICT*. Northampton, MA: Edward Elgar Publishing.
8. Roe, E., & Schulman, P. (2008). *High Reliability Management. Operating on the Edge*. Stanford: Stanford Business Books.
9. LaPorte, T. M. (2006). Managing for the unexpected: Reliability and organizational resilience. In P. Auerswald, L. Branscomb, T. M. LaPorte, et al. (Eds.), *Seeds of Disaster,*

Roots of Response: How Private Action Can Reduce Public Vulnerability. New York: Cambridge University Press.
10. Renn, O. (2008). *Risk Governance: Coping with Uncertainty in a Complex World*. London: Earthscan.
11. de Bruijne, M., & van Eeten, M. (2007). Systems that should have failed: Critical infrastructure protection in an institutionally fragmented environment. *Journal of contingencies and crisis management, 15*, 18–29.
12. Sheil, C. (2004). An incomplete hypothesis: Deregulation of water and sewerage in Australia. *Utilities Policy, 12*, 153–164.
13. Hood, C., & Jackson, M. (1992). The new public management: A recipe for disaster? In D. Parker & J. Handmer (Eds.), *Hazard Management an Emergency Planning. Perspectives on Britain*. London: James and James Publishers.
14. Christensen, T., & Lægreid, P. (2007). The whole of government approach to public sector reform. *Public Administration Review, 67*, 1059–1066.
15. Antonsen, S., P. G. Almklov, J. Fenstad, A. Nybø (2010) Reliability Consequences of Liberalization in the Electricity Sector: Existing Research and Remaining Questions. *Journal of contingencies and crisis management* 18(4):208–219.
16. Almklov, P., Antonsen, S., & Fenstad, J. (2011). NPM, Critical Infrastructures and Societal Safety (In Norwegian). Report: NTNU Samfunnsforskning AS.
17. Almklov, P., & Antonsen, S. (2010). The commoditization of societal safety. *Journal of contingencies and crisis management, 18*, 132–144.
18. Bourrier, M. (1996). Organizing maintenance work at two American nuclear power plants. *Journal of Contingencies and Crisis Management, 4*, 104–112.
19. Weick, K. E. (1993). The collapse of sensemaking in organizations: The Mann Gulch disaster. *Administrative Science Quarterly, 38*, 628–652.
20. Weick, K. E., & Sutcliffe, K. M. (2007). *Managing the Unexpected: Resilient Performance in an Age of Uncertainty*. San Francisco, California: Jossey-Bass.
21. Andresen, G., Rosness, R., & Sætre, P. O. (2008). Improvisation—taboo and necessity (In Norwegian). In R. Tinmannsvik (Ed.), *Robust arbeidspraksis—hvorfor skjer det ikke flere ulykker på sokkelen?*. Trondheim: Tapir Akademisk forlag.
22. Turner, B. A., & Pidgeon, N. F. (1997). *Man-made disasters* (2nd ed.). Oxford: Butterworth Heinemann.
23. Malone, T. W., & Crowston, K. (1994). The interdisciplinary study of coordination. *ACM Computing Surveys (CSUR), 26*, 87–119.
24. Auerswald, P., Branscomb, L., LaPorte, T., et al. (2006). *Seeds of Disaster, Roots of Response*. New York: Cambridge University Press.
25. McConnell, A., & Drennan, L. (2006). Mission Impossible? Planning and preparing for crisis. *Journal of contingencies and crisis management, 14*, 59–70.

Appendix A
Hierarchy of Hazardous Events

Table A.1 presents a list of potential undesired/hazardous events, according to their cause. This could serve as a check list in a risk analysis of critical infrastructure, cf. Chap. 3. The events are arranged in a hierarchy of three levels.

Observe that the events of this list have to be described further with respect to impact on infrastructures in order to serve as a useful description of events (and identification of "vulnerable locations") within the various disciplines. Such addition event descriptions are indicated below.

Electricity supply

- Failure of transformer to deliver power.
- Failure of supply line(s) (power lines, cables).
- Failure of inlet station.
- Failure of system control centre.
- Failure caused by several simultaneous faults (storm, failure of cable or power line in same trace, etc.).

Water supply

- Event in water source(s).
- Event in water treatment.
- Event in main supply line(s).

Rail traffic (*Railway*, *subway*, *tram*)

- Event on station:
  - Train cannot drive through station area.
  - Event on station area causing several fatalities.
- Event on freight depot.
- Event on line.
- Signal system failure.

P. Hokstad et al. (eds.), *Risk and Interdependencies in Critical Infrastructures*, Springer Series in Reliability Engineering, DOI: 10.1007/978-1-4471-4661-2,

Table A.1 List of main hazardous events (according to cause of the event)

Level 1	Level 2	Level 3
Natural event	Meteorological	Strong wind
		Flooding
		Extreme precipitation
		Extreme temperature
		Lightening
	Geological/geotechnical	Snow slide
		Landslide
		Earthquake
		Tsunami
		Volcanism
	Fire, natural	Forest fire
		Ling grass fire
	Cosmic objects	Meteorite (asteroid)
		Comet
Medical/biological event	Plants and animals	Transferable disease
	Human	Pandemic
		Non pandemic
Technological event	Release of dangerous substances	Chemicals
		Biological
		Nuclear
		Other
	Accident	Industrial fire
		Industrial explosion
		Transportation accident
		Structural collapse
		Other
	Technical/human failure in infrastructure	Water delivery
		Safe food
		Sewage and waste
		Transportation services
		Financial services
		Energy supply
		Communication/ICT system failure
Human behaviour	Malicious acts	Organized crime
		Sabotage
		Espionage
		Terrorism
		War
	Dysfunctional human behaviour	Psychotic (individuals)
		Negligence
		Gangs
		Other

  - Does not work (e.g. 24 h).
  - Gives erroneous information so that more than one train can enter same track.

Road transport

- Event on road.
- Event at traffic junction.
  - Fire.
  - Dangerous goods.
- Event in tunnel.
- Event on bridge.
- Meteorological conditions causing road network not trafficable.

Sea transport

- Event at port (loading/unloading).
- Event at sea.
  - Grounding.
  - Collision.
  - Fire.
  - Capsizing (e.g. icing).

Oil/Gas transport

- Event at gas terminal.
- Event at oil refinery.
- Event at fuel depot.
- Event at onshore pipeline.
- Event at offshore pipeline.
- Event at offshore oil installation.
- Event at chemical plant.

In addition to the above events, initiated in one of the relevant infrastructures, we have more overreaching events (which can "attack" more than one infrastructure). This in particular applies for *natural events/catastrophe* (cf. Table A.1).

Appendix B
Societal Critical Functions (SCF) and the Risk Analysis

Table B.1 lists typical SCF arranged into two levels.

Below, we indicate how use of these SCFs should be an integral part of the risk analysis described in Chap. 3.

Ways the SCF Affects the Scenarios

In this risk analysis, we could specify four types of relations between a SCF and the undesired/hazardous events:

1. "Before the hazardous event occurs". This typically means that the SCF causes the hazardous event, or one of its important functions is to prevent the hazardous event to occur. A typical example is failure in a railway traffic control system, potentially leading to collision between two trains.
2. "After the hazardous event has occurred". This is a situation where the SCF is important to mitigate the consequences of the event. For example, active fire fighting is important in case of fire.
3. "Both before and after the hazardous event has occurred". An example here is the police which is important to prevent crime, but also is important, for example, after various accidents.
4. "Threatened by the hazardous event". Here, we think about situations where hazardous events cause failure in a SCF. A typical example is flooding which can damage, for example, water supply lines, pumping stations.

P. Hokstad et al. (eds.), *Risk and Interdependencies in Critical Infrastructures*, Springer Series in Reliability Engineering, DOI: 10.1007/978-1-4471-4661-2,

Table B.1 List of SCF at level 1 and 2

SCF Level 1	SCF Level 2
Electricity supply power	Production plants
	Transformer and transformer cubicle front
	Distribution net
	Dams, barrages
	Control centres and SCADA-systems
	Mobile backup systems
Electronic communication	Phone and cable systems
	Mobile phones
	Internet
	Closed communication systems for authorities
	Radio communication
	Satellite-based infrastructures, earth-based stations
	Mobile backup systems
Water and sewage systems	Water sources
	Backup systems for water
	Purification plants
	Distribution networks
	Sewage systems
	Control centres and SCADA-systems
Oil and gas supply	Offshore installations
	Pipelines
	Land terminals and refineries
	Depots
	Control centres and SCADA-systems
Transport	Airports
	Railway stations and terminals
	Subways/trams
	Road transport
	Sea transport (terminals/harbours)
Banking and finance	National clearing systems
	Payment systems
	Security systems
Food supply	Logistic systems
	Hygiene and safety
Sanitation	Waste transportation
	Waste depot
Health, social and social security services	Specialist health service hospitals
	Primary health services
	Social services
	Support of medicines
	Laboratories
	Systems for social security services

(continued)

Table B.1 (continued)

SCF Level 1	SCF Level 2
Police, emergency services and rescue services	Police registers
	Police stations
	Emergency and rescue services
	Fire brigade
Public management	Parliament
	Government and administration, crisis management
	The judiciary
	Head of defence
Media and news communication	Radio and television companies
	Press, hard copies
	Internet papers
	Public information services
Important industries (potential for major accidents)	Chemical plants and depots
	Nuclear reactors and nuclear depots
	Defence industry
	Control centres and SCADA-systems
National symbols	Buildings, cultural institutions and monuments
	Mobile objects
	Institutional events
	Institutionalized persons

Vulnerability and Risk Factors

There is a number of vulnerability and risk factors that has relevance for both frequency and consequence of the undesired/hazardous event. Each risk factor and vulnerability element is given a "weight" (say on a scale from 1 to 5). For the vulnerability and risk factors, it is also evaluated whether they are effective "before" and/or "after" the event. These evaluations are relevant for assessing the probability and consequence categories. Headlines for vulnerability and risk factors are as follows:

- Location (e.g. open ground, transportation trace, dense building mass, landslide risk area and terminal for person traffic).
- Geographical scope (e.g. local, city, region, national and international).
- Population density per 1 km^2.
- Outdoor temperature (time of year).
- Time of day.
- Duration.
- Dependencies with other SCF.
- Substitution opportunities (e.g. redundancy of components, bypassing of errors).
- Degree of coupling.
- Culture.

- Mental preparedness.
- Cascade effects.
- Quality of operating procedures and knowledge about operation.
- Level of maintenance and renewal.

Elements of a Cause Analysis

For instance, five frequency categories 1, …, 5 have to be defined (cf. Chap. 3). Next, carry out the following steps:

1. List the SCF being in effect *before* the undesired/hazardous event.
2. For each SCF, assess the strength of the connection to the undesired event on a scale from 0 to 100.
3. List vulnerability and risk factors which affect the frequency of the undesired event, using the above bullet list.
4. Give the status of these vulnerability and risk factors.
5. List additional causes to the event which are not covered by the SCFs, vulnerabilities or risk factors.
6. Assess the frequency of the undesired event based on an evaluation of SCFs, vulnerabilities and risk factors by assessing the appropriate frequency category 1, …, 5 for the event.

Elements of a Consequence Analysis

For instance, five frequency categories 1, …, 5 have to be defined for each consequence dimension considered in the analysis (see examples in Table 3.1). Next, carry out the following steps:

1. List the SCF being in effect *after* the undesired/hazardous event or threatened by this event.
2. For each SCF, assess the strength of the connection to the undesired event, *for example*, on a scale from 0 to 100.
3. List vulnerability and risk factors which affect the outcome of the undesired event, using the above bullet list.
4. Give the status of these vulnerability and risk factors.
5. For each consequence dimension being chosen for the analysis, give the conditional probability for getting a serious consequence, given that the

undesired event has occurred. *Serious* here means that the consequence is more serious than the expected consequence of the event (*for example*, by a factor 10).

6. For each of the consequence dimensions, assess the appropriate consequence category (cf. Table 3.1).

Additional Information to Describe the Undesired/Hazardous Event

The following are some tasks that should be part of the risk analysis outlined in Chap. 3:

1. Give relevant measures to reduce risks.
2. Include free text to describe the risk scenario.
3. Specify whether one of the following applies for the event:

   (i) The event represents a potential for major accidents,
   (ii) There is a strong dependence between two or more infrastructures,
   (iii) The event represents a challenge with respect to risk communication,
   (iv) The event represents a special location (and additional analyses of the location-specific conditions may be required).

These points can serve as a guideline for whether it is needed to carry out more detailed analyses.

Appendix C
Risk Analysis Methods

Table C.1 gives an overview of some risk analysis methods, with a few references.

Table C.2 suggests typical applications of these methods. The first column indicates the decision situation that motivates the study, then examples of relevant analysis methods are given, also roughly indicating the complexity of the methods (mainly regarding required competence in statistics and modelling): L = low, M = medium, H = high. The last column suggests possible scope/objective of the analysis.

P. Hokstad et al. (eds.), *Risk and Interdependencies in Critical Infrastructures*, Springer Series in Reliability Engineering, DOI: 10.1007/978-1-4471-4661-2,

Table C.1 Short description of main methods in risk analyses of infrastructures

Abbreviation	Full name	Short description	References
BN	Bayesian network	Probabilistic network to model cause–effect relations. Direction of dependency defines the hierarchy between nodes	[1, 2]
D-R	Dose–response	Derives the probability of critical situations, defined as the probability of dose (e.g. amount of precipitation) becoming greater than response (e.g. capacity of drainage system)	[3]
CCA	Cause–consequence analysis	Integrates FTA with an event sequence analysis. Similar to ETA, but has a different graphical layout	[4]
CEDA	Cause and effect diagram analysis	Method to identify and classify the causes of an undesired event. Should also structure the relevant knowledge and experience of the study team	[4]
CA	Change analysis	Determines the potential effects of proposed modifications to a system (or a process)	[4]
ETA	Event tree analysis	Analyses the progression of a hazardous event from being initiated to the final consequences.	[5]
FTA	Fault tree analysis	Is particularly suited to identify and analyse systematically the various failure causes of a (sub)system. Will identify combination of failures that lead to a hazardous event	[5]
FMECA	Failure modes, effects and criticality analysis	Modules/sub-systems are reviewed to identify all failure modes and the causes and effects of these failures (both on sub-systems and overall system)	[5, 6]
FNA	Flow line network analysis	Describes the flow in a distribution network. The flow depends on physical capacity of the infrastructure and other physical parameters and may be compromised due to failures in the system	[7, 8]
GIS/GARA	Geographical information system/GIS-assisted risk analysis	GIS provides visualization of infrastructure assets and the tracking of their associated risk factors and offers the capabilities to spatially analyse data. Can be used for optimizing total cost of owning and operating infrastructure assets	[9, 10]

(continued)

Table C.1 (continued)

Abbreviation	Full name	Short description	References
HACCP	Hazard analysis and critical control points	Systematic system to identify specific hazards and measures for their control to ensure safety. Used by the food industry and drinking water supply to ensure safe production/supply	[11]
Hazid	Hazard identification	An approach for identifying the hazardous events, threatening a system	[4]
HAZOP	Hazard and operability analysis	Detailed and systematic technique for identifying hazards and operability problems throughout an entire system (plant, infrastructure)	[4, 12]
HRA	Human reliability analysis	A collective term for various methods with the following steps: (1) task analysis, (2) human error identification, and (3) human reliability quantification	[4, 13, 14]
LOPA	Layer of protection analysis	Semi-quantitative method for identifying protection layers and deciding whether existing safety barriers are adequate	[4]
–	Markov model	Models the various states (e.g. failed, deteriorated, being repaired) of a component/system	[5]
PHA	Preliminary hazard analysis	Initial analysis to identify the hazardous events, and assess frequency and consequence categories (e.g. H, M, L, cf. Chap. 3)	[4]
QCRA/QMRA	Quantitative chemical (microbiological) risk assessment	Tool for chemical/microbiological risk assessment (e.g. drinking water): identifies hazards, assesses number exposed and effects (dose–response curves)	[15, 16]
RBD	Reliability block diagram	Similar capabilities as the FTA. Illustrates (combination of) causes to failure by a reliability block diagram rather than by using a fault tree	[5]
SBD	Safety barrier diagram	A graphical presentation of the evolution of undesired events through different system states, depending on the functioning of the safety barriers intended to abort this evolution	[4]
SA	Sensitivity analysis	Analysis to examine how results of an analysis vary as individual assumptions are changed	[4]

(continued)

Table C.1 (continued)

Abbreviation	Full name	Short description	References
SWIFT	Structured what-if technique	Structured brainstorming session where a group of experts raise what-if questions to identify possible hazardous events and their causes, consequences and existing barriers and then suggest risk-reducing measures	[4]

References of Table C.1

[1] Caine, J. (2001). *Planning improvements in natural resources management, guidelines for using Bayesian networks to support the planning and management of development programmes in the water sector and beyond*. Wallingford: Center for Ecology & Hydrology. ISBN 0903741009

[2] Kjaerulff, U. B., & Madsen, A. L. (2006). *Probabilistic networks for practitioners—A guide to construction and analysis of Bayesian networks and influence diagrams*. Denmark: Aalborg University.

[3] http://www.epa.gov/raf/publications/guidelines-for-exposure-assessment.htm

[4] Rausand, M. (2011). *Risk assessment: Theory methods and applications*. New Jersey: Wiley.

[5] Rausand, M., & Høyland, A. (2004). *System reliability theory* (Second Edition ed.). New Jersey: Wiley.

[6] IEC 60812. (2006) Analysis techniques for system reliability—Procedures for failure mode and effect analysis (FMEA).

[7] EPA. (2008). Epanet 3. Users Manual. http://www.epa.gov.

[8] Billinton, R. (1989). *Composite system adequacy assessment—The contingency enumeration approach*. IEEE Tutorial Course Reliability Assessment of Composite Generation and Transmission Systems, course text 90EH0311-1-PWR, 1989, paper no 5.

[9] Lindley, T., & Buchberger, S. (2002). Assessing intrusion susceptibility in distribution systems. *Journal AWWA,94*(6), 66–79.

[10] MacGillivray, B., Hamilton, P., Strutt, J., & Pollard, S. (2006). Risk analysis strategies in the water utility sector: an inventory of applications for better and more credible decision making. *Critical Reviews, Environmental Science and Technology,36*, 85–139.

[11] http://www.who.int/foodsafety/publications/fs_management/haccpteachers/en/index.html

[12] IEC 61882. (2001). *Hazard and operability studies (HAZOP studies)—Application guide*. Geneva: International Electrotechnical Commission.

[13] Kirwan, B. (1994). *A guide to practical human reliability assessment*. London: Taylor & Francis.

[14] Gertman, D., Blackman, H., Marble, J., Byers, J., & Smith, C. (2005). *The Spar-H Human Reliability Analysis Methodm NUREG/CR-6883*. Idaho: Idaho National Laboratory.

[15] http://www.epa.gov/risk/guidance.htm

[16] http://www.epa.gov/risk/guidance.htm

Table C.2 Uses of the risk analysis methods for critical infrastructures

Decision situation	Methods	Analysis complexity	Possible scope/objective of analysis
Select/design system (size)	Network models, FNA	H	Identify required capacities and redundancies
	D-R	H	Decide capacity of draining system
Hazard identification	Hazid	L	Identify need for risk-reducing measures
	SWIFT/HAZOP	M	Identify need for risk-reducing measures
	FMECA	L	Identify effects of technical failures
	FTA	H	e.g. to investigate need for redundant systems
	RBD	M	e.g. to investigate need for redundant systems
Plan for risk reduction/avoidance	CEDA	L	Identify causes of the undesired events?
	LOPA/SBD	L	Are existing barriers adequate?
	HRA	M/H	Identify potential for human errors causing maloperation
	CCA	H	Detailed analysis of specific undesired events
	HACCP	M	Control supply of safe water
	QMRA/QCRA	H	Identify (effects of) microbial/chemical contaminations
Develop emergency plans	PHA & others	L/M	Plans for warning, crisis handling, obtaining substitutes and recovery
Protect against undesired events	PHA	L	Prioritize risk-reducing measures
	HRA	M/H	Improve procedures
Extend risk analyses to cope with specific problems and plan for preparedness	FTA	H	Identify causes of failure events
	ETA	M	Identify consequences of undesired events
	BN	H	Identify effect of risk-influencing factors, thereby assess effects of risk-reducing measures
	GIS/GARA	H	Give more complete (geographical) picture of hazards/vulnerabilities
Changes in network capacity or reliability	Network models (FNA, Epanet)	H	Optimize water availability for consumers
	FTA	H	Causes of network failures

(continued)

Table C.2 (continued)

Decision situation	Methods	Analysis complexity	Possible scope/objective of analysis
New (type of) users to be connected	SWIFT/Hazid	M/L	For example, food industry, hospitals.
Unreliable equipment observed	Markov	H	Maintenance optimization
Security problems; new threats	SWIFT/HAZOP	M	Identify threats and vulnerable points
Changes in environment	Hazid/SWIFT	L/M	New buildings, roads; new hazards appeared
Modifications/life extension	PHA	L	Identify "new" hazardous events and required measures
	FTA/RBD	H/M	Analyse "new" failure causes
	CA	L	Assess effects of modifications
Condition assessment	Markov	H	Predict service life of physical assets; maintenance planning

Author Biography

Editors and Authors of Chaps. 1–4:

Per Hokstad is a senior research scientist at SINTEF, Department of Safety Research. He was cand. real at the University of Oslo in 1968 in mathematical statistics (mathematics and physics). Until 1985, he was Assistant/Associate Professor at the Norwegian Institute of Technology, University of Trondheim (now NTNU). In 1985, Hokstad started at SINTEF and has a broad experience in modelling and application of risk analysis, safety and reliability engineering. Main areas of application are in the offshore and transport industry, and Hokstad has been project manager for various studies within safety and reliability. During the period 1990–2000, he was also Adjunct (part time) Professor in safety at the Institute of Mathematical Sciences, NTNU. Hokstad is a member of the editorial board of Reliability Engineering & System Safety.

Ingrid Bouwer Utne is a Professor of Marine Operation and Maintenance Engineering at Department of Marine Technology, Norwegian University of Science and Technology (NTNU). Utne has an MSc in Product Design Engineering and a PhD in Safety, Reliability and Maintenance from NTNU. She has worked as a researcher in SINTEF, Statoil, and Grieg Shipping. In 2010, she was a Visiting Scholar at UC Berkeley, where she worked with the Macondo blowout. Utne has published scientific articles on risk analysis, safety indicators, system safety engineering, maintenance, and environmental analyses related to the offshore oil and gas industry, fisheries and aquaculture and offshore wind energy.

Jørn Vatn holds a PhD in Maintenance Optimization from NTNU and is currently Professor in maintenance optimization, at the Department of Production and Quality Engineering, NTNU. In his research, he covers the entire RAMS field (Reliability, Availability, Maintainability and Safety). Main focus within maintenance is mathematical and probabilistic modelling relevant for condition

P. Hokstad et al. (eds.), *Risk and Interdependencies in Critical Infrastructures*, Springer Series in Reliability Engineering, DOI: 10.1007/978-1-4471-4661-2,

monitoring, optimization of maintenance, opportunity-based maintenance and grouping of maintenance activities. Main application areas are offshore oil and gas production, offshore wind energy and the railway industry.

Authors of Chaps. 1, 5 **and** 6:

Henrik Hassel is an Associate Professor of Risk and Vulnerability Assessment at Department of Fire Safety Engineering and Systems Safety, Lund University, Sweden. Hassel has a BSc in Fire Protection Engineering, an MSc in Engineering, Risk Management and Safety Engineering and a PhD in Risk Management from Lund University. Since 2010, Hassel has worked as a researcher and lecturer in the area of risk analysis with a special focus on critical infrastructure systems. He is also the Director of the Master's Programme in Risk Management and Safety Engineering given at Lund University.

Jonas Johansson is an Assistant Professor in Risk and Vulnerability Management of Technical Infrastructures at the Department of Measurement Technology and Industrial Electrical Engineering, Lund University, Sweden. He holds a PhD in Automation and a MSc in Electrical Engineering, both from Lund University, Sweden. His main research interest is vulnerability and risk management of complex systems, particularly large-scale critical infrastructures and the impact of interdependencies. He currently also holds a position as a part-time technical risk consultant at Grontmij AB, Sweden. In 2012, he was a visiting scholar at Johns Hopkins University, USA. He is also a member of Lund University Center for Risk Management.

Authors of Chaps. 7 **and** 8:

Gerd Hovin Kjølle is a Senior Research Scientist at Department of Electric Power Systems, SINTEF Energy Research and an Adjunct Professor at Department of Electric Power Engineering, Norwegian University of Science and Technology (NTNU). Kjølle holds an MSc and PhD in Electric Power Engineering from NTNU. Her research has mainly been within energy systems planning, power system risk and vulnerability analyses, reliability of electricity supply, fault and interruption statistics and electricity supply interruption cost assessment.

Oddbjørn Gjerde is a Research Scientist at Department of Electric Power Systems, SINTEF Energy Research. Gjerde has an MSc and PhD in Electric Power Engineering, from the Norwegian University of Science and Technology (NTNU). He is mainly working with tasks related to power system risk and vulnerability analyses, and reliability of electricity supply.

Authors of Chap. 9:

Rita Maria Ugarelli is a Senior Scientist at SINTEF Building and infrastructure at Department of Water and Environment and Adjunct Professor at Department of Water and Environment, Norwegian University of Science and Technology (NTNU). Rita is teaching in the courses of urban water, at bachelor level, and in

advanced urban water systems hydraulics and infrastructure asset management at master and PhD level. She holds an MSc from Bologna University in water supply systems reliability and a PhD in prediction of optimal time of rehabilitation planning in wastewater networks with the Oslo system as case study. She has been Assistant Professor for 10 years in Bologna University in Italy for the course of hydraulics. Ugarelli has participated in several EU projects on water and wastewater representing Bologna University or SINTEF (e.g. CARE-W, CARE-S, AWARE-P, PREPARED, TRUST), and she is now leader of the projects related to deterioration process of urban network infrastructure. Rita is a member of the International Water Association.

Jon Røstum is a senior researcher at SINTEF Building and infrastructure at Department of Water and Environment. Røstum has an MSc in water and wastewater engineering and a PhD in statistical modelling of pipe failures in water networks from NTNU. He has previously worked in a consultant company, and he has also held a position as an Assistant Professor at NTNU in the course urban water systems. He has worked on several EU projects on water and wastewater infrastructure (e.g. CARE-W, CARE-S, Techneau, Prepared and Trust). The focus has been on asset management, information system, risk analysis, rehabilitation planning and benchmarking. Røstum was MC member of COST action C18 "Performance assessment of urban infrastructure services: The case of water supply, wastewater and solid waste" (2004–2008) and was the chairman of COST C19: "Proactive crisis management of urban infrastructure" (2004–2008). Røstum is today MC member of COST IC0806.

Authors of Chap. 10:

Maria B. Line holds an MSc from the NTNU, Institute for Telematics, 2002. Since then Line has been a Research Scientist at SINTEF in Trondheim. Line is currently a PhD candidate at the NTNU, Institute for Telematics. She is looking into Smart Grids as a critical infrastructure and studying management of ICT security incidents. Her scientific interests include privacy, intrusion detection, security awareness and risk assessments.

Inger A. Tøndel received her MSc degree from NTNU in 2004 and has since then been a Research Scientist at SINTEF ICT. Mrs. Tøndel's research interests include electronic privacy, access control, threat modelling and security requirements engineering.

Authors of Chaps. 11 **and** 12:

Bjørn Egil Asbjørnslett is a Professor of Marine System Design at Department of Marine Technology, NTNU. Asbjørnslett has an MSc in Industrial Economics and Technology Management, and a PhD. in Project Planning and Control from NTNU. He has an industrial background in project management and supply chain management from the offshore oil and gas industry and the fast-moving consumer goods industry. He has been a lead researcher in maritime transport system design in projects for industrial companies within shipping, offshore oil and gas and the

process industry. Asbjørnslett has published scientific articles within risk and vulnerability analysis, accident analysis, transport system design, energy efficiency and emission mitigation, and human factors related to the shipping industry and the offshore oil and gas industry.

Inge Norstad is a Research Scientist at the Norwegian Marine Technology Research Institute (MARINTEK), and a PhD student at Department of Industrial Economics and Technology Management, NTNU. Norstad has an MSc in Industrial Economics and Technology Management and is a former officer in the Norwegian Army. His research focuses on the use of optimization-based methods for solving routing and scheduling problems within maritime transportation. Norstad has published scientific articles on routing and scheduling for the shipping industry.

Øyvind Berle is a PhD student at Department of Marine Technology, NTNU. His research focus is vulnerability of maritime transportation systems, in particular on how to increase the ability of systems to withstand low-frequency high-impact scenarios. Elements of this research include how to approach these problems in a structured manner, how to prepare to recover systems and how to quantify the effect of mitigating measures. As a part of his doctoral studies, he spent a year as a Fulbright fellow at Massachusetts Institute of Technology (MIT). Øyvind Berle currently works as a shipping analyst at DNB Markets.

Authors of Chap. 13:

Emery Roe is an Associate of the Center for Catastrophic Risk Management (CCRM) at the University of California, Berkeley. A long-time-practicing policy analyst, he is also a senior researcher on CCRM's Resilient and Sustainable Infrastructure Networks (RESIN) project. In RESIN, he and Paul Schulman are focusing on new approaches to conceptualizing and managing interconnected critical infrastructures. Roe is author or co-author of many articles and books, including Ecology, Engineering and Environment (2002) and High Reliability Management (2008). His most recent book, *Making the Most of Mess*: *Reliability and Policy in Today's Management Challenges*, is forthcoming from Duke University Press. His academic credentials come from the University of Michigan, Cornell University and the University of California, Berkeley.

Paul Schulman is James Irvine Professor of Government at Mills College, Oakland, California. He has done extensive research on the organizational challenges of maintaining high reliability in managing hazardous, complex systems such as nuclear power plants, air traffic control centres and the California high-voltage electrical grid. Most recently, he has been a member of the Reliable and Sustainable Infrastructure Networks (RESIN) project at the University of California, Berkeley, an NSF-funded project to develop a methodology for risk assessment of interconnected infrastructures in the California Delta region. His books include (with Emery Roe) *High Reliability Management* (Stanford University Press, 2008) and *Large-Scale Policy-Making* (Elsevier, 1980) and

numerous articles in journals such as the American Political Science Review, Journal of Politics, Administration and Society, the Journal of Policy Analysis and Management, The Comparative Journal of Public Administration and the Journal of Contingencies and Crisis Management. He has a PhD in political science from The Johns Hopkins University and has been a Visiting Professor at the University of California at Berkeley, and Brown University.

Authors of Chap. 14:

Petter G. Almklov is Senior Research Scientist at NTNU Social Research. He has a PhD in Social Anthropology and an MSc in Engineering Geology (both from the Norwegian University of Science and Technology). His main research interests are work processes and uncertainty management related to modelling and simulations, epistemology in high-technological settings, ICT in organizations as well as societal and occupational safety. The main research settings are the petroleum industry, critical infrastructures and space research control rooms. His wide-ranging interests are reflected in his publication record, which spans journals in the fields of safety, anthropology, science studies and information systems.

Stian Antonsen is an Organizational Sociologist from NTNU. He holds a PhD on safety management and safety culture. He works as discipline lead at Safetec Nordic and a senior research scientist at NTNU Social Research. Antonsen's scientific publications are related to safety culture, safety management, societal safety and research methodology.

Jørn Fenstad is researcher at Studio Apertura, NTNU Social Research and has a Master degree in geography. He has participated in a number of qualitative and quantitative research projects in which topics such as organization and safety have been the main focus. The research has been conducted in collaboration with companies in the petroleum industry, the maritime sector and the aquaculture industry.

Index

P. Hokstad et al. (eds.), *Risk and Interdependencies in Critical Infrastructures*, Springer Series in Reliability Engineering, DOI: 10.1007/978-1-4471-4661-2,