Risk and Vulnerability Analysis of Interdependent Technical Infrastructures

Addressing Socio-Technical Systems

Jonas Johansson

LUND UNIVERSITY

Doctoral Thesis in Industrial Automation
Department of Measurement Technology and Industrial Electrical Engineering

2010

Keywords: Critical Infrastructures; Technical Infrastructures; Socio-Technical Systems; Risk analysis; Vulnerability Analysis; Resilience; Network Analysis; Response Systems; Crisis Management

Illustration and figures: © Jonas Johansson

Number of Pages: 189

Department of Measurement Technology and Industrial Electrical Engineering
Faculty of Engineering, LTH
Lund University
Box 118
221 00 LUND
SWEDEN

http://www.iea.lth.se

ISBN: 978-91-88934-53-6
CODEN: LUTEDX/(TEIE-1061)/1-189/(2010).

Printed in Sweden by Media-Tryck, Lund University, Lund 2010

Aut viam inveniam aut faciam

[I will either find a way or make one]

Abstract

The society of today is highly dependent on technical infrastructures. Several incidents around the world the last decades have clearly highlighted the major effects technical infrastructure breakdowns have on life, health and economy of society. The vulnerabilities inherent in our technical infrastructures must be addressed in a proactive manner; it is not feasible to wait for major incidents to highlight them. What further exaggerates the complexities of technical infrastructures is that they are highly interconnected and mutually dependent of each other. Disturbances in one infrastructure can thus easily spread and influence the function of several other infrastructures, leading to widespread consequences for society. In order to proactively and properly manage technical infrastructures, different types of risk and vulnerability analyses give valuable input. The aim of thesis is to develop a modelling approach and methods for such analyses, with focus on identifying technical infrastructure vulnerabilities.

The presented modelling approach is based on dividing the model of the technical infrastructure into one structural and one functional part, enabling the analysis of interdependent technical infrastructures for both structural and functional strains. The methods for vulnerability analysis have three perspectives, in order to comprehensively address the complexities of vulnerabilities from different viewpoints: global vulnerability analysis, critical component analysis and geographical vulnerability analysis. As the resilience of technical infrastructures depends critically on the restoration capacities of supporting actors, a method addressing this is also presented. The focus of the presented methods is on vulnerability analysis of technical infrastructures, but their use in wider context of risk and vulnerability management is also addressed.

Empirical studies of electrical distribution systems and a railway system, consisting of seven interdependent subsystems, have been carried out to demonstrate the proposed modelling approach and the applicability and validity of the methods to address the complexities associated with identifying vulnerabilities of interdependent socio-technical infrastructures.

It is concluded that the proposed research gives a valuable foundation for input to proactive policy- and decision-making of technical infrastructure risks and vulnerabilities.

Acknowledgements

As spring is finally starting to take a firm grip over this year's prolonged Swedish winter, I'm writing these final words of the thesis on a Sunday two days before printing. It is with much warmth and happiness I can look back on these five and a half years as a PhD-student. There are so many people who have stood by me in the ups and downs and so many inspiring people that I've met during these years, that the simple "thanks" below just doesn't feel enough.

First, I want to express my gratitude towards my supervisors. All of you have been a source of inspiration and given me valuable advices and support throughout my PhD-years. Olof Samuelsson in the world of electric power engineering, Henrik Tehler in the world of risk and vulnerability, and Christian Rosén in the world of what it means to be a PhD-student. Gustaf Olsson, my first supervisor, for taking me in as a PhD-student

All the people at IEA deserves thanks for providing an inspiring work environment, an administratively uncomplicated time (special thanks to Ulf), the coffee discussions, the Trivselkommitté activities, and all niceties with belonging to a work place. Especially Jonas, Dan, and Tomas, deserve thanks for all the fun stuff we've done outside the scope of work.

During my years, I have also tightly belonged to a research group called FRIVA (under LUCRAM). The people constituting FRIVA have contributed with a highly inspiring research environment, for which I'm most grateful. This group of people have substantially influenced my view of what research is all about. Special thanks goes to Kurt for keeping us all in control and steering the project towards success.

Thank you Henrik for all the fun time we spent together debating over our articles, screaming at the matlab code, discussing risk and vulnerability, being a friend, and…… beer. Thank you Alex for letting me drag you along in the path of technical infrastructure risks and vulnerabilities, I hope you have benefited as much as I did from our time together.

I thank all the companies and organization that most willingly have shared details about your technical infrastructures and the opportunities for discussions along the way, making the conducted research possible. These include, not exclusively: Banverket, Järnvägsskolan, E.ON, and Lunds Energikoncernen. I also give thanks to my other part time employer during the second half of my PhD-time, Grontmij. All the people at Grontmij and the people I met with my second hat on have given me valuable insights to the practical aspects of technical infrastructures and also a fun time.

Special recognition and thanks go to the Swedish Civil Contingencies Agency, MSB, for funding the research project. Your support is greatly acknowledged.

Finally, thanks and love to my big family and all my friends who have stood by me and enriched my life immensely during these years. Without your support and love, I wouldn't be sitting here writing these final words. Gina, thank you for your love, understanding, and encouragement during the thesis writing process and in making my life much happier. You deserve many big big hugs!

Lund, 28 March 2010
Jonas Johansson

Contents

Chapter 1

Introduction

The present chapter introduces the motivation behind the research, objectives and delimitations, main research contributions, and lists the research papers forming the compilation thesis. The chapter together with the appended papers forms the foundation of the thesis. However, to form a more easily accessible whole for the reader and to put the appended papers in a research context and motivate the conducted research, subsequent chapters deal more thoroughly with concepts and definitions, modelling approaches, vulnerability analysis methods, and introduces the appended papers. A brief discussion and the main conclusions of the research are presented in the last two chapters. The reader is directed to the respective appended paper for detailed information about the studied systems, modelling approaches, analysis methods, results, and conclusions regarding the results.

1.1 Motivation

The society is becoming increasingly dependent upon the service of reliable technical infrastructures. These services are largely taken for granted and are assumed to never cease, until some major crisis highlights the inherent vulnerabilities of these critical infrastructures. The storm Gudrun that hit southern Sweden in 2005 (2 weeks after the tsunami struck the South East Asia) rendered some 650 000 customers without electrical power supply and severely damaging the function of telecommunication systems, roads, and Railway operations (Johansson et al., 2006). In 2003, there was a major power outage, affecting the entire southern Sweden and eastern Denmark. The outage lasted for about 6 hours, affecting some 4 million people (e.g. Larsson and Ek, 2004). There exist many more incidents like these, where technical infrastructures fail and lead to major disruptions in the society. To address a few, there are the power outages in Auckland in 1998 (Newlove et al., 2000), the ice-storm in Canada in 1998 (Fischer and Molin, 2001; Chang et al., 2007) and the power outage that affected half of Europe in 2006 due to the luxury line Norwegian Pearl (UCTE, 2006). The hurricane Katrina in

2007 wiped out most of the critical infrastructure in the New Orleans area for a considerable amount of time, severely crippling recovery operations (Boin and McConnell, 2007). All these incidents have one common denominator, they were very unlikely to happen and lead to extensive consequences for the society.

Technical systems are usually designed to cope with incidents that happen somewhat frequently, leading to small consequences when they occur. Large-scale disruptions, however, happen more seldom and the systems are usually not effectively designed to cope with these types of disruptions, such as the examples above. If the frequency of incidents, both natural and man-made, is plotted against the consequences they tend to follow a power law distribution (e.g. Amin, 2004; Nedic, 2006). The author's main interest is the tail in this power law distribution, where the consequences are high and the probability of occurrence is low. In this area historical data and experience are very limited, sometimes lacking. In Haimes (2009b) a recap of Talbebs[1] three attributes of an extreme event is given: (a) it is an outlier, as it lies outside the realm of regular expectations; nothing in the past can convincingly point to its possibility, (b) it carries an extreme impact, and (c) in spite of its outlier status, human nature makes us concoct explanations for its occurrence *after the fact*, making it explainable and predictable. The main question thus becomes: How do we find these extreme incidents *before* they occur?

The technical infrastructures around us are becoming both more complex, in terms of number of components, the narrower limits they are designed to operate within, and more interconnected, interdependent, with each other (e.g. Zimmerman, 2001; Little, 2004). The main reason behind this development over the last decades, the author believe, is efficiency. Do more, quicker, faster and better. Addressing the complexity of single infrastructure systems, not to mention the interdependencies between technical infrastructures is a major challenge. Not only must the system limits within one system be clearly identified, but also how malfunctions in one infrastructure can spread to other infrastructures must be addressed. As Zio (2007) and Kröger (2008) point out, in order to address the complexities of such systems new methods for their analysis are needed, since "… the current quantitative methods of risk analysis seem not to be fully equipped to deal with the level of complexity inherent in such systems" (Zio, 2007, p. 505). The question thus become, how do we handle this complexity?

[1] The original source is: Talbeb, N.N., (2007). The Black Swan: The Impact of the Highly Improbable. New York, Random House.

There are several other questions that's deserves reflecting upon. What will happen if strains, different from what is expected, affect the system? How will the system react and how large can the consequences become? How close to the limits are they operating? What are the limits? How do we identify what can go wrong? To what type of strains are these systems vulnerable? Are there any critical components within these systems that if they falter cause large consequences? Are there any critical geographical locations so that if a natural hazard strikes this area, the function of one or several infrastructures is severely hampered? In short, how vulnerable are these system and these interconnected "systems-of-systems"?

The motivation behind the research is to address the type of questions stated above. The point of departure for the presented research, coming from an engineering perspective, is Complexity Science, more specifically the research field of Network Theory and influences from the field of Systems Thinking. There, of course, exist several methods and approaches for addressing the questions stated earlier, all with different aims and from different points of view. The aim has been to develop models and methods for proactive vulnerability assessment of both single and interdependent technical infrastructures from a slightly different perspective than traditional network analytical approaches, addressing the fidelity of the modelling approach, the socio-technical aspects of technical infrastructures, and the applicability and feasibility of the proposed modelling approaches and vulnerability methods in a practical context. In Grubesic et al. (2008) an overview and a discussion of the applicability of network analytical approaches for vulnerability analysis of networks are given. One of the conclusions in the article is that existing studies of attack tolerance for complex networks fall somewhat short in incorporating network use/flow, which is addressed in the present research. In Pederson et al. (2006) an overview of modelling approaches for analysis of technical infrastructure interdependencies is given, in which it is pointed out that method development in this area is highly relevant. In Peerenbom and Fisher (2007) it is stated that the "science" of infrastructure dependencies is still relatively new and much research efforts are still required in order to address the complex and pervasive nature of interdependencies. The author, of the present thesis, argues that several perspectives, both regarding models as well as methods, are needed in order to understand and analyse the complexities associated interdependent technical infrastructures. It is thus not believed that there exists a single all encompassing solution, a view shared by, for example, Peerenbom and Fisher (2007), Murray et al. (2008), and Eusgeld et al. (2009).

My personal motivation is my never-ending desire to understand the form and function of complex technical infrastructures and the context in which they operate. Environmental, economical, legislative, and political factors together with en ever increasing demand from the society of the services that these systems provide, make this a highly interesting and challenging research field. I believe that risk and vulnerability analysis hold several beneficial aspects in the quest to understand and improve our technical infrastructures in a proactive manner. I also believe that risk and vulnerability analysis can serve as a bridging platform to discuss and assess technical system aspects in an understandable way for people with differing backgrounds, such as engineers, economics, politicians, lawyers, and the public.

1.2 Objectives and Delimitations

As presented in the previous section, an open mind of what can happen to technical infrastructures is needed. The aim of the thesis is to present a way of how to close the gap between "normal" analysis, where usually only small deviations around a rather stable operating state is taken into account, and the analysis of unexpected large-scale disruptions. The theoretical field within which the research is conducted is risk and vulnerability management, and the path which was followed for most of the research is that of vulnerability analysis – simply because it is the author's belief that these types of analysis enables the assessment of technical infrastructures for high consequence and low probability incidents.

To narrow the scope of the research further, the aim of the presented research is to develop methods for vulnerability analysis of the fundamental part of technical infrastructures, i.e. the network that supports the transport of the desired services. These services could be electricity, communication, water, oil, gas, cars, trains etc. However, since the organization supporting the technical infrastructure to a large extent influences the infrastructures vulnerability, the aim has been to develop methods addressing this issue – taking a socio-technical view of the technical infrastructures under study. Lastly, no matter how good methods one develops, they are useless if not being put into practice. Thus, how vulnerability analysis, as presented in the present thesis, can be used in a risk and vulnerability management scheme for electricity distribution systems is also addressed.

The major objectives of the research are thus in short:

- To develop methods for structural vulnerability analysis of single technical infrastructures, identifying scenarios that can lead to large consequences. The focus is to enable the analysis of a large part of the possible scenario space and at the same time attain results with higher fidelity than existing methods.

- To develop methods for structural vulnerability analysis of inter-dependent infrastructures, identifying scenarios that can lead to large consequences. The focus is to enable the analysis of a large part of the possible scenario space and at the same time attain results with higher fidelity than existing methods.

- To demonstrate the applicability and feasibility of the proposed modelling approach and vulnerability methods by empirical studies.

- To develop a method for addressing the issue of assessing organizational response system capabilities with respect to restoring an infrastructure under strain.

- To demonstrate how vulnerability analysis can be utilized as a part of a risk and vulnerability management scheme of technical infra-structures.

As always when it comes to research projects, delimitations have to be made in order to find a feasible way to address the objectives. With respect to the above objectives the major delimitations are in short:

- Vulnerabilities due to the impact of market, legislative, and financial factors are not included in the presented vulnerability analysis methods since these mainly have impact on the infrastructure in longer time frames than the aim of the methods.

- Vulnerabilities due to changing operational constraints, such as changing generation capacities or changing load demands within the network system have not been explicitly analysed, although they can be addressed with the proposed modelling approach.

1.3 The Research Process

The research behind the thesis has been far from a straight path, although for the reader it might appear so. This section addresses what has influenced the research, which paths I chose to follow and which I chose to discard. As such, this is a brief overview, as seen in Figure 1.1, over the five and a half years as a PhD-student, starting in the autumn of 2004 and up to today, the spring of 2010.

Throughout the PhD-studies I have gratefully belonged to an inspirational and creative research framework program, namely FRIVA (Framework Program for Risk and Vulnerability Analysis) within LUCRAM (Lund University Centre of Risk Analysis and Management). The researchers within this program come from both natural and social sciences, giving me the benefit of learning different viewpoints of what research is all about, on methods, and on the way of how to conduct research. During the studies I have also belonged to a research group consisting of electrical engineers at the department of Measurement Technology and Industrial Electrical Engineering, giving me a centre of gravity in the engineering field of electrical power systems and automation. After my Licentiate Thesis in Automation in 2007, the need for a better understanding of the context in which these systems operate lead me to start working part time at a consultant company. This has given me the opportunity to further develop parts of the presented methods for a more practical environment, working with risk and vulnerability management of electrical distribution companies. All these environments have undoubtedly formed the presented research.

In the beginning of the research process, my interest was focused on technical infrastructures and their operational limits when it comes to delivering the services the society so highly depend upon. Given the framework program, the field of risk and vulnerability management seemed to be a fruitful path to follow; more specifically vulnerability analysis seemed to be the least researched field and the path forward in addressing high consequence scenarios. In order to proactively analyse the vulnerability of systems, models are of necessity. I came across Network Theory, which had started to be used for the modelling and analysis of several large-scale technical infrastructures. The simplicity of the modelling approach appealed to me, since already early in the research the goal was to analyse the vulnerability of interdependent technical infrastructures. However, many of the approaches in the research field solely focused on topological network properties. The development of simplified functional models, to complement the topological properties was thus addressed in order to achieve a higher feasibility and applicability of the

analysis. In the process of the development of methods for vulnerability analysis of interdependent technical infrastructures, it was a natural and straightforward step to start with method development and vulnerability analysis of a single technical infrastructure, namely electrical distribution systems (appended paper I and II). The interest in using the proposed vulnerability methods in a risk and vulnerability management scheme for electricity distribution systems took me on a slight detour from the method development process (appended paper III). I then steered research back to the original path, working with development of a modelling approach for vulnerability analysis of interdependent systems. The proposed modelling approach was illustrated in Johansson and Jönsson (2008) and was applied to the analysis of a fictional railway system. During this time, the notion of technical infrastructures as being socio-technical systems and the impact it had on the vulnerability of infrastructures became stronger. In an effort to, at least to a small extent, address the social side of socio-technical systems, development of methods for the analysis of response system capabilities took me on the second slight detour from the main path (appended paper IV). In order to test the feasibility of the proposed interdependent modelling approach in the context of vulnerability analysis of interdependent systems, the railway system in the southern part of Sweden was modelled and analysed (appended paper V) – a part of the research process that made me fully aware of the complexity of interdependent socio-technical infrastructures. Now at the time for my thesis, I've ended up with extensively more knowledge about the form and function of technical infrastructures as socio-technical systems and how to analyse them, only to realize how little I really know in relation to what I want to know.

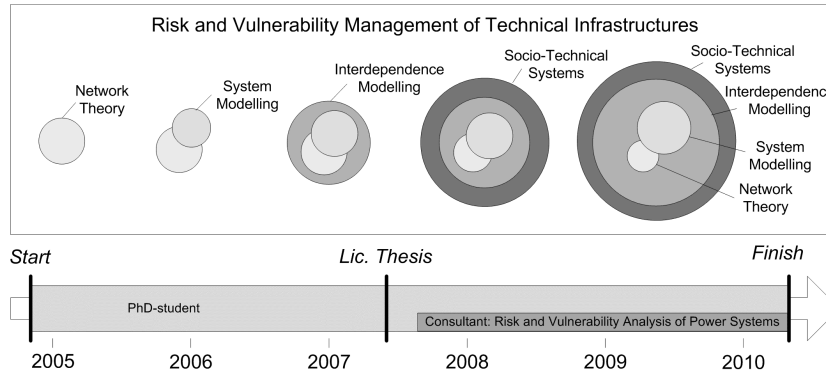


Figure 1.1. Overview of the research process.

1.4 Appended Papers

The following list of publications form the basis of the present doctoral thesis, which will be referred to in the text with their roman numerals. Journal papers [I] and [II] are properly peer-reviewed, conference paper [IV] went through a limited peer-review process, and conference paper [III] was accepted by abstract. Journal paper [V] is subject to a proper peer-review process. In Chapter 6 a short introduction of the papers together with the author's contributions for each of the papers are given. The papers are appended in the end of the thesis and have been selected from the reason of giving the best picture of the conducted research. The journal paper (Johansson and Jönssson, 2010), treating the modelling approach of interdependent technical infrastructures, was not included since it didn't extensively widen this picture in comparison with appended paper V.

[I] Johansson, J., Jönsson, H., Johansson, H., (2007). Analysing the Vulnerability of Electric Distribution Systems: A Step Towards Incorporating the Societal Consequences of Disruptions, *International Journal of Emergency Management*, Vol. 4, No. 1, pp.4–17.

[II] Jönsson, H., Johansson, J., Johansson, H., (2008). Identifying Critical Components in Technical Infrastructure Networks, *Journal of Risk and Reliability*, Vol. 222, Part O, pp. 235-243.

[III] Johansson, J., Svensson, S., (2008). Risk and Vulnerability Management of Electrical Distribution Grids, *Nordic Distribution and Asset Management Conference* (NORDAC 2008), Bergen, Norway, September 8-9.

[IV] Wilhelmsson, A., Johansson, J., (2009). Assessing Response System Capabilities of Socio-Technical Systems, *The International Emergency Management Society* (TIEMS2009), Istanbul, Turkey, June 9-11.

[V] Johansson, J., Hassel, H., Cedergren, A., (2010). Vulnerability Analysis of Interdependent Critical Infrastructure: Case study of the Swedish Railway System, Submitted to *International Journal of Critical Infrastructures*.

1.5 Related Publications

In addition to the appended papers, several publications have been published within the research. Appended paper [I] and [II] are updated versions of conference articles [1] and [2], respectively. Appended paper [I] and [2,3] were partly covered in the author's licentiate thesis [5].

[1] Johansson, J., Jönsson, H., Johansson, H., (2006). Analysing Societal Vulnerability to Perturbations in Electrical Distribution Systems. *Proceedings of International Workshop on Complex Network and Infrastructure Protection* (CNIP), Rome, Italy.

[2] Johansson, J., Lindahl, S., Samuelsson, O., Ottosson, H., (2006). The Storm Gudrun a Seven-Weeks Power Outage in Sweden, Presented at: *Third International Conference on Critical Infrastructures* (CRIS2006), Alexandria, VA, USA.

[3] Jönsson, H., Johansson, J., Johansson, H., (2007). Identifying Critical Components in Electric Power Systems: A Network Analytic Approach, *Proceedings of European Safety and Reliability Conference 2007* (ESREL2007), Stavanger, Norway.

[4] Johansson, H., Jönsson, H., Johansson, J., (2007). *Analys av sårbarhet med hjälp av nätverksmodeller* (Analysis of vulnerability with network models), LUCRAM report 1011, Lund University, Lund. (In Swedish)

[5] Johansson, J., (2007). *Risk and Vulnerability Analysis of Large-Scale Technical Infrastructures: Electrical Distribution Systems*, Licentiate Thesis, Department of Industrial Electrical Engineering and Automation, Lund Institute of Technology, Lund University, Media-Tryck Lund University, Lund, Sweden.

[6] Johansson, J., Hassel (former Jönsson), H., (2008). A Model for Vulnerability Analysis of Interdependent Infrastructure Networks, *Proceedings from the joint Annual Conference of European Safety and Reliability Association and Society for Risk Analysis* (ESREL2008 & 17th SRA-Europe Conference), Valencia, Spain.

[7] Johansson, J., Wilhelmsson, A., (2008). Vulnerability Analysis of Socio-Technical Systems: Addressing Railway System Vulnerabilities, *Proceedings from the first Young Researchers' Seminar*, Malmö, Sweden.

[8] Johansson, J., Hassel, H., (2010). An Approach for Modelling Interdependent Infrastructures in the Context of Vulnerability Analysis, Submitted to *Reliability Engineering and System Safety* after special invitation to the Special issue of selected papers from ESREL2008.

[9] Johansson, J., Samuelsson, O., Hassel, H., (2010). *Tekniska infrastrukturers sårbarhet (Technical infrastructures vulnerability)*. Chapter in FRIVA – Risk, Sårbarhet, och Förmåga - Samverkan inom krishantering, Final report for research project FRIVA2, to be published 2010.

1.6 Research Contributions

The main research contributions of the doctoral thesis are given below. Discussions and conclusions regarding the presented research are given in Chapter 7 and Chapter 8, respectively.

- Definition of vulnerability and how the concept, as used in the presented research, relates to other concepts such as risk and resilience.

- Modelling technical infrastructures by an approach of dividing the infrastructure into two parts, a topological model and a functional model, enabling the modelling of interdependent technical infrastructures and the vulnerability analysis of both structural and functional strains.

- A method for assessment of global vulnerability of technical infrastructures. Global vulnerability analysis is a way to assess the performance of a system when it is subjected to strains of varying type and magnitude.

- A method for identifying, screening and ranking critical components in technical infrastructures. Certain components or sets of components lead to severe consequences when they malfunction. These components or sets of components are termed critical and are regarded to be the vulnerability of the system to failures in these components.

- A method for analysing geographical vulnerabilities. The approach has been to identify critical geographical locations, which are geographically constrained cells where the simultaneous malfunctions of components in the cells gives rise to large consequences.

- Empirical vulnerability analysis of single and interdependent technical infrastructures, by the methods of global vulnerability analysis, critical component analysis and geographical vulnerability. Exemplifying the modelling approach and the method's validity and applicability by assessing the vulnerability of electrical distribution systems and an interdependent railway system.

- An approach for assessing response system capabilities regarding restoring technical infrastructures after strains. The method was evaluated in a preliminary study with the Swedish Railway Administration.

- Development of several tools in Matlab® in order to map infrastructures, to visualize analysis results and foremost to simulate behaviour of infrastructures under various types of strain.

The research, as presented, can also be regarded from the view of being a conceptual framework for the facilitation of vulnerability assessment of technical infrastructures. Further, it is argued that the research is both applicable and valid for vulnerability analysis of socio-technical interdependent technical infrastructures, as so demonstrated by the empirical studies.

1.7 Empirical Studies

The research, as presented in the thesis, involves several empirical analyses. Three different electrical distribution systems have been modelled and their vulnerability analysed. Two were mixed rural/urban 20/10kV distribution systems (appended paper I) and one was an urban 10kV distribution system (appended paper II). A preliminary study regarding response system capabilities and restoration times of the railway system for large strains was performed together with The Swedish Railway Administration (appended paper IV). The southern part of the Swedish railway system, consisting of seven interdependent systems, has been modelled and its vulnerability analysed with three different methods (appended paper V).

1.8 Outline of the Thesis

In Chapter 2 the main concepts and definitions regarding risk and vulnerability analysis of technical infrastructures are given. Concepts and definitions such as crisis management, resilience and robustness, and critical infrastructure, are also discussed. The chapter as such introduces the conceptual points of departure for the conducted research.

Chapter 3 introduces the approach chosen for the modelling of technical infrastructures. It is argued for an approach where the structural properties and the functional properties are separated in order to facilitate a modelling approach for both individual systems as well as interdependent systems with the aim to enable vulnerability analyses.

Methods for vulnerability analysis of technical infrastructures are the focal point in Chapter 4. Three different perspectives are introduced: global vulnerability analysis, critical component analysis, and geographical vulnerability analysis. These three perspectives are argued to give complementing and valuable insights in the quest of finding technical infrastructure vulnerabilities.

Chapter 5 puts the presented methods in slightly larger perspective. How the proposed vulnerability analysis can be used in a risk and vulnerability management scheme is briefly discussed. In the effort towards analysing technical infrastructures as socio-technical systems, a method for the assessment of response system capabilities for restoring technical systems after strains is also discussed in the chapter.

Chapter 6 briefly introduces the appended papers and states the author's contributions for each of the paper.

The thesis ends with an overall discussion regarding the presented research in Chapter 7 and in Chapter 8 a brief summary and some thoughts on future research is given.

Chapter 2

Main Concepts and Definitions

In the area of risk and vulnerability research, many different definitions, concepts, and terms exist. This chapter begins with the author's viewpoints of some of the most important of these and how they are used in the present thesis. A brief reference to research conducted in this area is given, to either support or discuss the choice of viewpoint. The chapter starts with a summary of crisis management, as it is serving as the foundation for the present research. The following section holds a discussion around the concepts of risk, uncertainty, and vulnerability, followed by a section regarding technical infrastructures. The closely related subject of critical infrastructures is introduced and the chapter ends with a discussion regarding infrastructure interdependencies.

2.1 Crisis Management

Crisis management is normally divided into four main phases: mitigation (also referred to as prevention), preparedness, response and recovery. This model goes under the abbreviation PPRR. Mitigation and preparedness are actions and activities taken before a crisis occurs to mitigate the likelihood and/or consequences of an undesired event. In the response phase, actions are taken during a crisis to meet the emergency needs that arise. After the crisis, there is a recovery period in order to return to a normal or desired state. In Figure 2.1 the different phases of crisis management are illustrated. The figure is based on the merging of two frameworks, the framework from FEMA (Federal Emergency Management Association) (FEMA, 1997) and the framework from CCMD (Canadian Centre for Management Development) (CCMD, 2003).

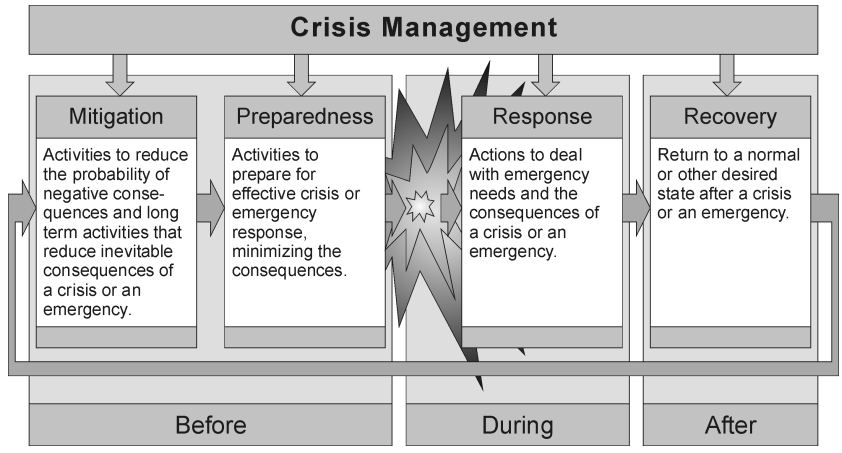


Figure 2.1. The different phases of crisis management in accordance with FEMA and CCMD.

PPRR has been criticized for not being the best model for risk management, since it may inhibit the risk management process. For example Kelly (1999) criticizes the framework for being linear and that it oversimplifies the complexity of a crisis. Crondstedt (2002) claims that the model creates artificial barriers between the four elements, implying a sequential consideration and implementation of the elements and that all the elements appear to be equally important. Although criticized, it is a well-known and applied model within the area of crisis management, and it gives an overview over the normal phases considered.

The focus for the research in the present thesis is mainly on proactive crisis management, i.e. concerning the phases of mitigation and preparedness. The proposed methods mainly concern the vulnerability analysis of technical infrastructures in a proactive manner, i.e. identifying system weakness in order to derive appropriate mitigation strategies before any hazard or threat exploits the vulnerabilities. Parts of the research can however also be utilized, with appropriate further research, in the response and recovery phase (appended paper IV).

2.2 Risk, Uncertainty and Vulnerability

The word risk is commonly used in everyday life. Humans think daily in risk terms in order to cope with the reality we live in. Sometimes risk is used as a term to describe the likelihood of an event, for example the phrase "there is a risk of rain today".[2] Sometimes it is used, as in this thesis, as a combination of what can happen, how likely it is and what the consequences might be if it happens (Kaplan et al., 1981). This can be exemplified with the phrase like "the risk involved in buying that apartment is too great". The buyer has some notion of what can happen (the property market can drop) how likely that is (the market interest is most likely to go up in the near future and stay high) – and the consequences (I will lose money if I'm forced to sell within three years). The buyer has thus made a decision not to buy the apartment using a risk-based approach. All risk-based decisions are made under some form of uncertainty, if we had perfect notion of the likelihood and the consequence – it would not be a risk it would rather be a fact. The concept of vulnerability is not as commonly used as risk. Most often vulnerability refers to how a system, organization, or human performance is degraded if some hazard or threat exploits the vulnerability (e.g. Haimes, 2006). Consider the phrase "I can't afford loosing money on the apartment". Here the buyer has identified a vulnerability, he/she can't afford losing money. Sometimes vulnerability refers to a state in a system, such as a door left open, making it easy for a burglar to access a house. Vulnerabilities can be identified without quantifying the likelihood of something exploiting them; the open door can for example be identified as a vulnerability regarding burglary without quantifying the likelihood of a burglar breaking in. The author's definitions of the terms risk, uncertainty and vulnerability and their relationship are treated in the following subsections.

Risk

Traditional quantitative risk analysis (QRA) is based on three questions – "the set of triplets" – to quantitatively assess the risk for a system (Kaplan et al., 1981):

[2] Here it can be noted that what constitutes a risk may differ from the viewpoint of the assessor. The tourist looking forward for a sunny day on the beach may have a different view regarding the risk of rain compared to the farmer who after several weeks of drought are looking forward to the "risk" (or rather chance) of rain (Hansson, 2005). The author will not further dwell on the different perspectives and perception of risk in the thesis, other than noting that it may differ depending on the viewpoint of the assessor.

1. "What can happen?"
2. "How likely is it that that will happen?"
3. "If it does happen, what are the consequences?"

If all of these three questions can be answered, the risk of a system can be appropriately defined. This leads to the definition of risk as a function of the probability of an unwanted event and the severity of consequences of that event (Kaplan et al. 1981):

$$R = \{< S_i, L_i, X_i >\} \tag{2.1}$$

Where S_i denotes the *i*:th risk scenario, L_i denotes the likelihood of that scenario, and X_i denotes the resulting consequences. The notion of *scenario* is central to the risk definition. A scenario is seen as the possible way a system can go from one point to a future other point. In two Kaplan articles in 1991 and 1993 the index *c* for completeness was added (Kaplan et al., 2001):

$$R = \{< S_i, L_i, X_i >\}_c \tag{2.2}$$

The completeness indicates that the set of scenarios {*Si*} should be "complete" and denumerable, i.e. all possible scenarios should be included and this set of scenarios should be finite. In reality, it is hard, if not impossible, to cover the whole scenario space, i.e. an infinite number of scenarios have to be analysed in order to cover the entire scenario space. Furthermore, all the scenarios must be disjoint in order to correctly depict the risk, which in reality might not be so easily achieved. These two practical problems, completeness and disjointness, have lead to a refinement of Kaplans definition of risk (Kaplan et al. 2001):

$$R = \{< S_\alpha, L_\alpha, X_\alpha >\}, \alpha \varepsilon A \tag{2.3}$$

where α ranges over a set *A*, which, in general, is nondenumerable. *A* can be thought of as the set of points in the total scenario space. Each point, α, in the interior of the total scenario space also represents a scenario, S_α, and the set of interior points, representing the set of all risk scenarios, can be designated by S_A. Connecting equations (2.2) and (2.3) by using the principle that every scenario, S_i, is itself a set of scenarios yields that each S_i can be visualized as a subset of S_A. The set of scenarios in the risk analysis, $\{S_i\}$,

should be; complete ($\cup S_i = S_A$), finite, and disjoint ($S_i \cap S_j \; \forall \; i \neq j$) for practical purposes. Such a set of subsets of S_A Kaplan and colleagues define as a "partitioning", P, of S_A. A risk analysis thus means to identify a partitioning of the underlying risk spaces of S_A, namely S_i. Equation (2.3) can thus be written as:

$$R_p = \{< S_i, L_i, X_i >\}_p, \text{ where } R_p \approx R \tag{2.4}$$

R_p is thus an approximation of R based on the partition P.

The refined definition of risk is more conceptually attractive for practical risk analysis, since the risk of a system can be approximately estimated by a finite number of risk scenarios by partitioning the scenario space. Furthermore, the condition of scenario disjointness can be relaxed if one does not seek to quantify and add up the likelihoods of the scenarios.

Performing a risk analysis of any given system is then basically a task of answering the three questions: 'What can happen?', 'How likely is it that that will happen?', and 'If it does happen what are the consequences?'. To answer these questions, subjective "expert" opinions often lie as the foundation of the risk analysis. Answering the first question requires an open mind from the risk analyst to identify possible scenarios, which is not easy since the perception of possible scenarios is often based on scenarios that have happened before, i.e. historical events. This would lead to an incomplete risk assessment of the system, since future events seldom is a mirror of historical events. Estimating the probability of a scenario occurring is fundamental for the quantitative risk analysis. While seemingly straightforward to assess the probability, it is not always possible or the estimate may have questionable quality. The probability might not be known and methods and knowledge for deriving it might be lacking, leading the analyst to discard the scenario, thus compromising the completeness criteria. If the system under study is complex and the number of possible scenarios seems insurmountable, the quality of the probability and consequence estimations might suffer.

Uncertainty

Risks and vulnerabilities are always associated with some form of uncertainty, e.g. uncertainty of the likelihood of occurrence or uncertainty regarding the possible consequences that may arise. As Hansson puts it: "Risks are always connected to lack of knowledge. If we know for certain that there will be an explosion in a factory, then there is no reason for us to talk about that explosion as a risk. Similarly, if we know that no explosion will take place,

then there is no reason either to talk about risk." (Hansson, 2005, p. 1). Aven even defines risk as "the combination of possible consequences (outcomes) and associated uncertainties." (Aven, 2007, p. 746).

Uncertainty can be either due to natural randomness, aleatory uncertainty, or due to lack of data or knowledge, epistemic uncertainty. Aleatory uncertainty is related to knowing the possible outcomes, just not which outcome it will be due to unpredictable variation in the performance of the system under study. This type of uncertainty cannot be reduced. Epestemic uncertainty is due to a lack of knowledge about the system under study and can be reduced, in principle even eliminated, with enough study and data sampling of the system. In risk and vulnerability analysis, these uncertainties are addressed by the use of probability, frequency, or likelihood estimations in a quantitative or qualitative manner. The issue of uncertainty is not specifically addressed in the present thesis other than noting that: "At a fundamental level, uncertainty is uncertainty, yet the distinctions [of different types of uncertainty] are related to very important practical aspects of modelling and obtaining information." (Winkler, 1996, p. 127).

Vulnerability

There have been arguments against the traditional risk analysis approach since it tends to focus on the hazard or threat, and not the ability of the system to withstand hazards or threats, i.e. focus is on mitigating the hazard or threat (initiating event) instead of making the system less vulnerable (e.g. Dilley and Boudreau, 2001; McEntire, 2003). Another approach to assess the risk for a system is to quantify its vulnerability and its exposure to hazards or threats that could exploit this vulnerability (e.g. Buckle et al., 2000). Some define vulnerability analysis as taking a wider scope than traditional risk analysis (e.g. Einarsson and Rausand, 1998; Holmgren, 2004). The author argues that the definition of risk, as put forward by Kaplan and colleagues, does not exclude this wider scope of the traditional risk analysis. It is further argued that vulnerability analysis is about taking a different point of view, rather than widening the scope of a traditional risk analysis.

Vulnerability is a concept that is used in many research areas, but its definition is often ambiguous and sometimes misleading (Buckle et al., 2000; Dilley and Boudreau, 2001; Weichselgartner, 2001; Haimes, 2006). Many definitions explicate vulnerability as the system's overall susceptibility to loss due to a negative event, i.e. the magnitude of the damage given a specific strain. In order for the vulnerability to be meaningful, it must be related to specific hazard exposures (e.g. Dilley and Boudreau, 2001). A system might

thus be vulnerable to certain hazard exposures but robust and resilient to others (Hansson and Helgesson 2003). In addition, two identical systems are viewed as always equally vulnerable to all possible hazard exposures, independent of the environment in which they operate.

The vulnerability for a system can be viewed from two perspectives. The first perspective is to assess a system's overall vulnerability to threats and hazards, a global perspective. The second perspective is to find critical parts or components that the system is vulnerable to the loss of (e.g. Apostolakis and Lemon, 2005; Latora and Marchiori, 2005). Further, vulnerability is regarded as a property that arises from the states of the system (e.g. Haimes, 2006).

The term *hazard* is normally used for strains on a system stemming from non-man-made sources such as earthquakes, severe weather conditions or tsunamis. Einarsson and Rausand (1998) define *hazards* to be related to accidental events and *threats* to be related to deliberate events. In the field of electric power system analysis the term *disturbances* is normally used to describe hazards, both from within and from outside of the system. In appended papers [I, II] the term *perturbation* was used to describe the combination of both hazards and threats. In appended paper [IV] and [V] the term *strain* was used. In the present thesis, the terms *perturbations* and *strains* are used synonymously to describe both hazards and threats that can be either endogenous or exogenous.

In short, *vulnerability is defined* as the consequences that arise when a system is exposed to a strain of a given type and magnitude. A strain that affects a system normally moves it from its planned or desired system state into an unplanned or undesired state. Vulnerability analysis is thus the exploration and identification of these unplanned or undesired states of a system and estimating the associated consequences.

The N-1 criterion, often used in the design of electrical power systems, can be said to be a vulnerability criterion. The N-1 criterion states that the system should tolerate the failure of any single component, regardless of the initiating event, and still maintain its function. Normally the system is only evaluated for the single failure of components and not for several simultaneous failures. Given the definitions above, the strain is that one component fails to function. The vulnerability is then described by the possible scenarios and the probability and consequences of these. If there is no consequence for any of the scenarios, the system is not vulnerable to the strain, i.e. one component failure.

Defining Risk and Vulnerability

The concepts of risk and vulnerability are rather tightly related to each other. The following section discusses and tries to visualize the author's definition and the relationship of these two terms. For the discussion of risk, the author draw upon concepts put forward by Kaplan and colleagues (c.f. Kaplan and Garrick, 1981; Kaplan et. al., 2001). For the discussion of vulnerability, resilience, and risk, the author draw upon concepts put forward by Haimes (c.f. Haimes, 2006, 2009a, 2009b). Nevertheless, the proposed definitions below are put forward by the author alone.

In Figure 2.2 the *normal state*, S_0, of a system is shown in a phase plane. The normal state can be viewed as an "as planned" or "desired" state of the system. Hazards or threats, called here initiating events (*IE*), can push this system into an *end state, ES*. The end state represents the state where the consequences are evaluated, thus:

A *risk scenario* is defined as the full trajectory, from S_0 to ES.

Different initial events might lead to the same end states. Traditional risk analysis is based on defining and assessing the probability of an initiating event and then finding the corresponding consequences, as described by the end state. In the phase plane of a system there will be certain points (e.g. the loss of a critical component) that can be reached by different initial events (e.g. rough weather, technical malfunction, or a malicious attack) and that can lead to different end states. These points are referred to as middle states. In traditional risk analysis, such a middle state, *MS,* is of limited interest – i.e. focus is on the initiating event and the corresponding consequences. For any given system, there will be a numeral of possible ways from the initial state to a numeral of possible end states. There might even be several initiating events that lead to the same end state. Sets of these traditional risk scenarios, from S_0 to ES, will go through a well-defined middle state, MS.

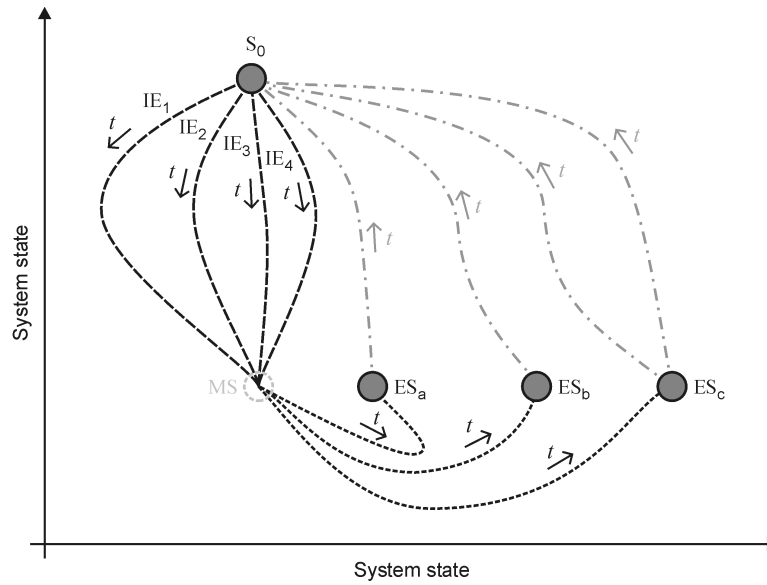


Figure 2.2. The concept of risk. S_0 = system as planned, IE = Initiating Event, MS = Middle State, ES = End State.

For the definition of vulnerability, these middle states are the focal point. In Figure 2.3 the phase plane is redrawn to illustrate the changed point of view, going from risk to vulnerability. By identifying which states a system can be in (e.g. for an technical infrastructure network these could be one component out of function, two components out of function, and/or changes of production and demand) it is possible to evaluate the end states, i.e. the possibility of estimating the consequences that arise. A major point here is that there might be several initiating events that lead to the same middle state, and by focusing on finding these middle states and the associated end states the focus has shifted from finding hazards and threats to the system and instead finding system vulnerabilities that may or may not be exploited, thus:

A *vulnerability scenario* is defined as the full trajectory from a middle state (MS) to an end state (ES).

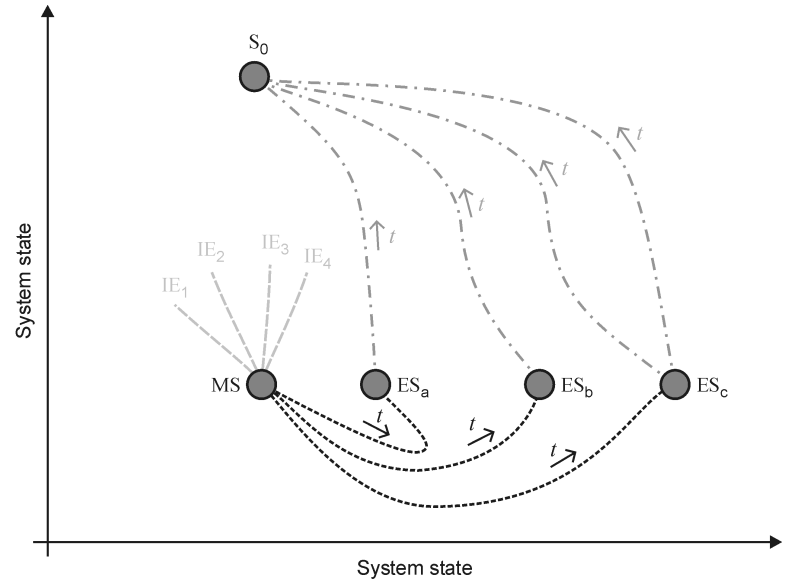


Figure 2.3. The concept of vulnerability. S_0 = system as planned, IE = Initiating Event, MS = Middle State, ES = End State.

Normally only the initial consequences are evaluated, and the path from ES back to the normal state, S_0, is not included in the end state. The trajectory from a middle state to an end state, and the consequences the end state represents, is seen as the *robustness* of the system. For most systems, there will be a desire to return to the initial or a desired state after the system has been exposed to a strain. It should be noted that it is not always possible, or even desired, to bring back the system to the initial state. In those cases, the system will return to a *new desired state* (not illustrated in the figure). The trajectory from a middle state to the end state and the efforts necessary to return the system to the initial or a desired state are viewed as the *resilience* of the system (resilience and robustness is further discussed in section 2.3), see Figure 2.4.

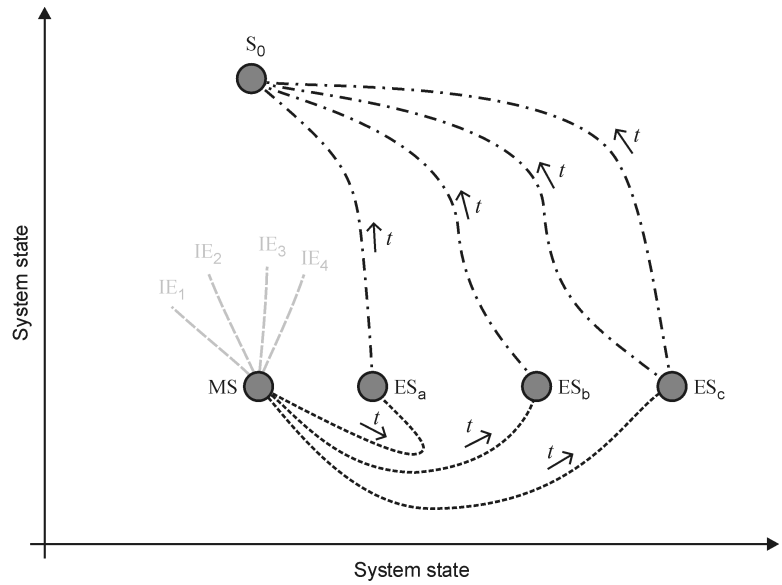


Figure 2.4. The concept of resilience. S_0 = system as planned, IE = Initiating Event, MS = Middle State, ES = End State.

For the system to go from the S_0 to MS, it has to be exposed to a strain. For electric power systems, at transmission and sub transmission level, the N-1 situation can be regarded as a point corresponding to MS. The system should withstand the loss of any single component without loss of the service it provides regardless of the type of initiating event. Identifying a system's vulnerability thus gives the answer to what consequences that arise given a specific strain, without identifying the specific initial event that led to MS.

In Figure 2.5 the concepts of risk, vulnerability and resilience are brought together. The identification of all the middle states and the end states of the system is defined as a *vulnerability analysis*. The vulnerability analysis methods presented in the thesis focus on identifying middle states and estimating the consequences associated with the end states. Depending on the aim of the analysis, the ES can either correspond to a point where the initial consequences are evaluated (appended paper I and II) or it can be the same as S_0, i.e. including the path of the recovery (appended paper V).

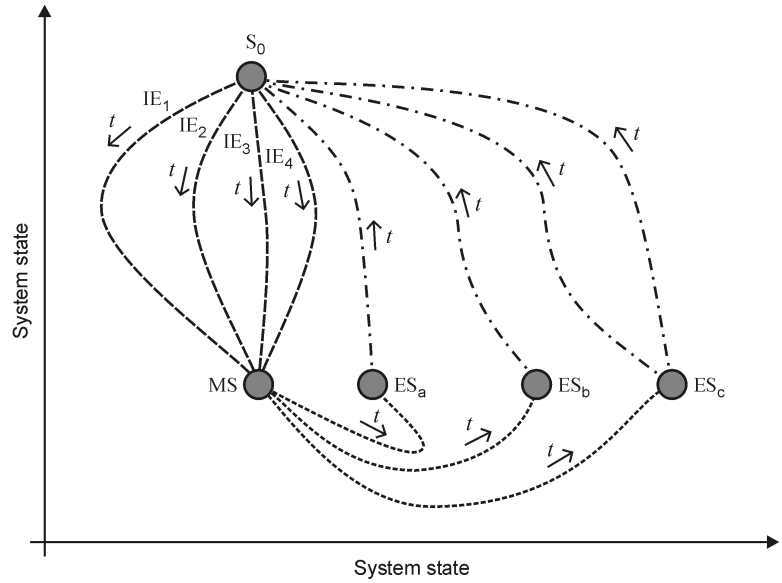


Figure 2.5. Bringing risk, vulnerability, and resilience together. S_0 = system as planned, IE = Initiating Event, MS = Middle State, ES = End State.

A vulnerability analysis can be complemented by identifying and quantifying the probability of initial events, which can put the system into the middle states. This then corresponds to a *risk analysis*, but the starting point of the analysis vastly differs compared to a traditional risk analysis. Instead of finding system vulnerabilities, the focus in traditional risk analysis is towards identifying threats and hazards that affects the system. This in turn will affect the choice of mitigation strategies to consider, either constructing barriers to protect the system from threats or hazards (risk analysis approach) or constructing a less vulnerable system that copes with strains regardless of the type of threat or hazard that affects the system (vulnerability analysis approach).

The times, *t* (together with an arrow), as indicated in Figure 2.2 to Figure 2.5, are an important part of the phase plane representation of the system. Each movement from one state to another state requires time. This time could be anywhere from more or less instantaneously to years or even decades, depending on both the type of system and the type of risks and vulnerabilities the analysis tries to capture. For technical system networks the times, in general, from an initiating event to an end state, as depicted in

Figure 2.5, are usually in the order of milliseconds to hours. From the end state back to the planned or desired state, these times, in general, range from seconds to hours or even weeks.

The concluding remark is that the major difference between the concept of vulnerability and the concept of risk is the aspect of not estimating (qualitatively or quantitatively) the type and the likelihood of an initiating event. As such, vulnerability is seen to be part of risk; a view shared by Aven (2007) and Wisner (2001). The omission of the search for initiating events lead to the prospect of a more thorough and more open-minded search for possible vulnerable states of the system, in contrast to a traditional risk perspective where focus is on finding initiating events and quantifying the likelihood of these.

If desired, and possible, the vulnerability analysis can be complemented with an assessment of the likelihood of perturbations exploiting the vulnerability, i.e. yielding a risk analysis. This can for example be necessary in a management perspective, i.e. in order to select between different alternative investments or activities for risk and vulnerability mitigation in a rational manner. It should be noted however that this is not always possible, or at least very difficult, to estimate the likelihood of a strain due to lack of knowledge and experience, i.e. uncertainties. These types initiating events could for example be terrorist threats, malicious acts, rare weather phenomena, or unlucky combinations of component failures. As such, vulnerability analysis gives valuable information of the system performance when exposed to various strains, i.e. how it copes and recovers. It thus gives important information to what types of strains the system is vulnerable, and for which it is not. In this perspective, a vulnerability analysis holds a way to assess the operational limits of a system. Operational limits are here defined as the limits for which the system performance is regarded as acceptable for a given type and magnitude or strain.

With respect to the phase plane description of the possible system states, a major simplification has been made in order to more clearly define the relationship between risk and vulnerability. The simplification concerns the omission of the longer time perspective in the representation of the system states. Viewed over longer time perspectives, systems evolve and change, giving rise to new states (initial, middle and end states) that have to be tracked, evaluated and mitigated for an effective risk and vulnerability management scheme. In the present thesis, the methods presented are for the vulnerability analysis of a specific system configuration, i.e. a snapshot of the systems vulnerability given that specific configuration. However, using the

proposed methods with respect to changing system configuration would open up for possibility to analyse the vulnerability of a system for longer time perspectives, i.e. following the vulnerability trajectory. The proposed methods can also be used to evaluate different optional system configurations for either existing or new systems, in the efforts to reduce its vulnerability. This lies outside the scope of the present thesis, but should be regarded as highly notable for future research.

2.3 Resilience and Robustness

Risk and vulnerability is tightly coupled to the concepts of *resilience* and *robustness*, as pointed out in the earlier section. The term resilience has no single clear definition (e.g. Haimes, 2009a). In general, it can be said to be the ability of a system or an organisation to react and recover from unanticipated disturbances and events (e.g. Hollnagel et al., 2006). Zio (2009, p. 131) puts the view of resilience versus reliability by stating "… systems should not only be made reliable, i.e. with acceptably low failure probability, but also resilient, i.e. with the ability to recover from disruptions of the nominal operating conditions". Hansson and Helgesson (2003) define resilience as "the tendency of a system to recover or return to (or close to) its original state after a perturbation". A more operationalized definition of resilience is given by McDaniels et al. (2007). This definition points 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 (2003) defines 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 is here seen to be the antonym of the two terms robustness and resilience. Robustness is viewed as the ability for a system to withstand a strain, and resilience viewed as a systems ability to recover from a disturbance. Risk analysis, vulnerability analysis and resilience engineering all share a common denominator: to better understand and improve system performance in a proactive manner. However, it is argued that they take different perspectives, giving complementing valuable information of the system under study.

2.4 Critical Infrastructures

Technical infrastructures are often grouped in the category of *critical* or *lifeline* infrastructures, since they provide modern society with services that are essential to its physical and economic survival. In McCarthy et al. (2005), critical infrastructures are defined as those that provides life-essential services, such as: shelter, food, water, sanitation, evacuation and transportation, power and fuels, medical care, public safety, communications and access to financial resources. In the report, several critical sectors are identified: energy, water and wastewater, transportation/postal and shipping, health service, emergency service, telecommunication, and banking and finance.

From a Swedish perspective, there is no clear definition of what constitutes a critical infrastructure. The Swedish Civil Contingencies Agency[3] has given examples of what constitutes critical infrastructures (KBM, 2005):

- Telecommunication
- Data communication
- Electrical power supply
- Provision of fuels
- Water supply, wastewater, and district heating
- Transport and distribution
- Police, emergency management, health care and alarm systems
- Financial services
- Critical governmental services

The above examples of critical infrastructures are more or less coherent with the list in the Critical Infrastructure Working Group (CIWG) behind the Executive Order 13010 (Executive Order, 1996) creating the President's Commission on Critical Infrastructure Protection (PCCIP) in the USA. Electrical power supply stands out as an especially critical infrastructure since many other infrastructures depend heavily on a reliable power supply.

From a European Union perspective, a programme on Prevention, Preparedness and Consequence Management of Terrorism and Other Security Related Risks (EPCIP) was adopted on 12 February 2007. In the act (COM, 2006, p. 15) critical infrastructures are defined as "…those assets or

[3] The Swedish Civil Contingencies Agency (MSB) was created in 2009, taking over the former responsibilities of the Swedish Emergency Management Agency (KBM).

parts thereof which are essential for the maintenance of critical societal functions, including the supply chain, health, safety, security, economic or social well-being of people".

With respect to the research in the present thesis, the proposed methods are regarded as most applicable to the technical systems of critical infrastructures, e.g. telecommunication, data communication, electrical power supply, water supply, wastewater, and district heating, and transport and distribution.

2.5 Technical Infrastructures

Technical infrastructures are systems that are serving a large spatial area, such as a country, municipality, or city, and consist of a vast number of components that interact in a way that usually requires specialized knowledge in the field of applied and industrial sciences to be understood. These types of systems are often referred to as *complex* in the research literature. The border for where a system is to be regarded as being only *complicated* and when it becomes *complex* is not clearly defined. There exist several research papers, discussing the difference between complicated and complex, and which system can be regarded as one or the other (e.g. Axelrod et al., 2000; Ottino, 2004; Amaral and Ottino., 2004a and 2004b). Complicated can loosely be defined as a system with many "moving" parts or as a system where parts have to work in unison to accomplish a function. Complex can loosely be defined as a system that consists of parts that interact in ways that heavily influence the probabilities of later events. The term complex is normally also used to indicate that a system has properties such as non-linearity, adaptability, and emergence. Technical infrastructures are here also argued to belong to the category of *socio-technical* systems. The function of technical infrastructures highly depends upon the interaction of both physical and actor networks, since they "collectively form an interconnected complex network where the actors determine the development of the physical network, and the physical network structure affects the behaviour of the actors" (Verwater-Lukszo and Bouwmans, 2005, p.2379).

The author's viewpoint is that the technical part of the system that constitutes the foundation for the supply of required services can be regarded as a complicated system, e.g. railroads, electrical networks, roads, and water distribution pipes. The larger view of a technical system, including societal, economical, legal, organizational, and other contextual factors, most certainly force the analyst to regard it as a complex system.

2.6 Technical Infrastructure Interdependencies

The technical infrastructures that support and form the basis of the society we live in are so complicated, and even complex, that modelling and simulating any one of them in the context of risk and vulnerability analysis is not a straightforward task. In the hallmark of efficiency and cost reduction, they are also often tightly interconnected. This means that a disturbance in one infrastructure can easily affect the performance of other infrastructures. Severe disturbances in the electric power system for example lead to disturbances in the telecommunication networks and transportation infrastructures. These affected systems are also necessary for an appropriate recovery of the power system. Mutually dependent infrastructures are termed *interdependent* infrastructures. In order to correctly assess the vulnerability of an infrastructure, its dependence and interdependence on other infrastructures must be integral to the analysis. Several incidents around the world have highlighted this increased vulnerability of technical infrastructures due to dependencies and interdependencies. Three real-life examples are given below to briefly illustrate the impact of interdependencies.

The power system blackout in southern Sweden and eastern Denmark on 23 September 2003 (e.g. Larsson and Ek, 2004) showed the impact on the society when the demand for electricity is not met. This incident was the largest blackout in Sweden in 20 years. About 5 million people were affected and the cost for society was estimated to 500 million SEK. The system went down because one nuclear reactor was disconnected from the grid (due to internal problems) and one bus bar malfunctioned, i.e. an N-2 contingency (can be seen as an N-3 contingency depending on the view of the fault of the bus bar). The incident lasted for roughly 6 hours and led to about 18 GWh of energy not served. The incident had a major impact on business and industries in the area. The communication system used by the police did not function properly and in some areas the cell-phone system went down. Severe traffic problems arose, e.g. the bridge between Sweden and Denmark had to be shut down due to problems with the traffic monitoring system. The railway in the southern parts of Sweden and the underground railway in Copenhagen went out of operation. Copenhagen airport had to shut down for incoming flights, leading to severe air traffic problems. The blackout clearly showed the society's dependency on electricity.

The Auckland blackout in 1998 was an incident that could not happen, but did (e.g. Newlove et al., 2000). The improbability of the blackout meant that the owner of the grid, Mercury Energy, had not made a contingency plan for the event. The four 110 kV cables feeding the central business district (CBD)

in Auckland worked intermittent for a period of a couple of weeks before finally caving in. Intermittent outages in CBD lasted from January to March, affecting some 10 000 companies and roughly 4000 residents. Fire stations and hospitals in the area had to shut down. Restaurants could not store the food properly, leading to a demanding work situation for the health authorities that had to control and confiscate unserviceable food. Computers and databases needed by local authorities for the mitigation of the crisis ceased to function. Pumps needed for the water supply in buildings stopped working. The local police and the social services had problems with helping people trapped in buildings and tunnels. In order to mitigate the effects of the power outage, a large amount of reserve power generators had to be brought in from other countries. The prioritization of the reserve power was to some extent problematic since the local power company responsible for the grid and the local authorities had different opinions. In order to repair the faulty cables, specialized repair crews had to be flown in from Australia. The economical consequences of the crisis were significant. The power outage highlights how the failure in one technical infrastructure spreads and impacts both other technical infrastructures as well as emergency management agencies and strengthens the view of technical infrastructures as socio-technical systems. The incident also highlights something that should be inherent to any vulnerability analysis: Expect the unexpected. While seeming obvious, this proves extremely difficult in practice.

The two incidents described above were both due to a limited amount of technical failures in the system. There are also incidents where large amounts of the components in a system are destroyed and must be replaced, leading to a different type of strain. In January 2005 the storm Gudrun hit the southern parts of Sweden. It had wind speeds of up to 46 m/s and destroyed large parts of the rural electricity distribution systems in southern Sweden (e.g. Johansson et al., 2006). During the night of the 8th and 9th of January some 650 000 customers were without power supply. The full restoration of the power supply took seven weeks. The telecommunication system, used for operation and control, was unable to reach half of the substations in the area during the event. The train service between Malmö and Stockholm was interrupted for about two weeks. The incident has lead to a massive investment programs in order to replace overhead conductors with underground cables for the major distribution companies in Sweden. For one major distribution company this means replacing roughly 17 000 kilometres of bare conductors with cables. The storm also rendered the road network unusable due to the sheer amount of trees scattered over the roads. This severely hampered the speed of restoration of the networks. The severe

consequences of the incident led to an acceleration of the introduction of amendments to the Swedish Electricity Act (SFS 1997:857) regarding compensation for customers and the requirement that electricity distribution companies have to, on a yearly basis, perform risk and vulnerability analysis and derive mitigation strategies of the identified risks and vulnerabilities.

The above examples briefly illustrate the importance of a proper understanding of how infrastructures are coupled, the consequences that the malfunction of one infrastructure can have on other infrastructures, and the impact on the society as a whole. Interdependencies between technical infrastructures are not only a technical issue but also affect social and environmental systems that depend upon their services. Rinaldi and colleagues (Rinaldi et al., 2001) have put forward a useful framework for the understanding and analysis of interdependent infrastructures. The framework is based on six dimensions, which ideally are orthogonal; Coupling and response behaviour, Type of failure, Infrastructure characteristics, State of Operation, Types of interdependencies, and Environment. It is pointed out that the development of a comprehensive architecture or framework for interdependency analysis is a major challenge. In Rinaldi (2004) several candidate techniques for modelling and simulating interdependent infrastructures are described and discussed. The paper points out the lack of analytical modelling and simulation tools for the study of interdependencies and the need of more comprehensive research in this area. Zimmerman (2001) gives several good examples of infrastructure interdependencies.

There are several papers either giving an overview (e.g. Peerenboom et al., 2007; Brown et al. 2004) or describing certain modelling and simulation methods for analyzing infrastructure interdependencies (e.g. Gursesli and Desrochers, 2003; Robert, 2004; Tolone et al., 2004; Balducelli et al., 2005; Xiao et al., 2008). The proposed modelling and simulation tools all capture aspects of critical infrastructure interdependencies. Nevertheless, it is apparent that there is still a massive need for research and development in this area regarding risk and vulnerability analysis of critical infrastructures and the effect of interdependencies. In appended paper V a method for vulnerability analysis of interdependent technical infrastructures is presented.

Chapter 3

Modelling Technical Infrastructures

This chapter gives an overview of the main theoretical foundations that have influenced the research approach regarding modelling technical systems, both single and interdependent systems. The modelling of any real-life system, or system-of-systems, requires well-defined system boundaries and usually simplifications of the system representation. Where to draw the borders and what simplifications that are valid, are set by the context in which the model will be used. The author's overarching belief is that a model is useful if it helps in extending the knowledge of the system under study. Jay Forrester, the founder of System Dynamics, made a statement in Forrester (1971), which captures the essences regarding the usefulness of models:

> *"There is nothing in either the physical or social sciences about which we have perfect information. We can never prove that any model is an exact representation of "reality". Conversely, among those things of which we are aware, there is nothing of which we know absolutely nothing. So we always deal with information which is of intermediate quality – it is better than nothing and short of perfection. Models are then judged, not on an absolute scale that condemns them for failure to be perfect, but on a relative scale that approves them if they succeed in clarifying our knowledge and our insights into systems."*

A similar but more succinct statement is alleged to have been made by Box in the book Empirical Model-Building and Response Surfaces[4], in Box (1976) there are however statements with the same essence:

> *"Essentially, all models are wrong but some are useful."*

[4] Box, George E. P.; Norman R. Draper (1987). *Empirical Model-Building and Response Surfaces*. Wiley. pp. 424. ISBN 0471810339. The author could unfortunately not get hold of a copy of this book.

The appropriateness of a model should thus be judged in the context it is used and what real life behaviour it is set out to capture. The aim of the chapter is to introduce previous inspiring research as well as the author's proposed modelling approach. The first section introduces the field of network theory and gives a brief overview of research conducted within this area. The subsequent sections present the author's approach to modelling technical infrastructures.

3.1 Network Theory

The ideas behind the research described in the present thesis stems partly from the field of network theory. The predecessor of Network Theory is the mathematical field of Graph Theory, initiated by Leonhard Euler and "the seven bridges of Königsberg"-problem in 1736. There are numerous examples of the application of graph theory and network theory. The brief introduction to network theory given here is based on Watts (2004), Grubesic et al. (2008), Holme (2004), Newman (2003), and Strogatz (2001). The first reference takes a popular science approach to the subject, while the latter four references give a good overview of the subject and have extensive references to related literature. The theory described in the present section stems from these references, if not explicitly stated otherwise. The aim is to give the reader a basic understanding of Network Theory, as it is a part of the modelling approach

The basic concept of Network Theory is to build a model of real-world networks and describe the form and, in various degrees, the function of the network by different measures. Network theory has been used to study a wide range of systems (e.g. Albert and Barabási, 2002), such as: social networks (e.g. celebrity networks), technical networks (e.g. the Internet and electrical power systems), cellular networks, and the studies of the written human language.

For network theoretical studies of technical infrastructures, only the most fundamental part of the infrastructure is usually modelled, i.e. structural properties of the system that facilitates the physical transportation of the services they provide and in general no or limited functional aspects of the network is modelled.

Fundamentals of Network Theory

A fundamental element of Network Theory is the graph. A graph consists of *vertices* (sometimes referred to as nodes), *V*, and *edges* (sometimes referred to as arcs or links), *E*, which together build a *graph*, G(V,E), see Figure 3.1. The number of vertices and edges are normally denoted *N* and *M*, respectively. Let *v* and *w* describe two vertices. An adjacency matrix, *A*, describes the network, where $A_{vw} = 1$ if there is an edge between these two vertices, i.e. $(v,w) \in E$, and $A_{vw} = 0$ if there is no edge between two vertices, i.e. $(v,w) \notin E$. The size of A thus corresponds to N. Normally a vertex cannot have an edge to itself, i.e. $A_{vv} = 0$, and only one edge can exists between any two vertices. If these restrictions are not fulfilled the graph is termed a *multigraph*. A graph can be directed or undirected. A directed edge is normally termed *arc*. It is possible to assign values to the vertices and the edges; such graphs are referred to as a *weighted* or a *valued* graph. It is also possible to differentiate between types of vertices or types of edges (as done in appended paper I, II and V). Throughout the thesis, vertices/nodes and arcs/edges will be referred to as *components*.

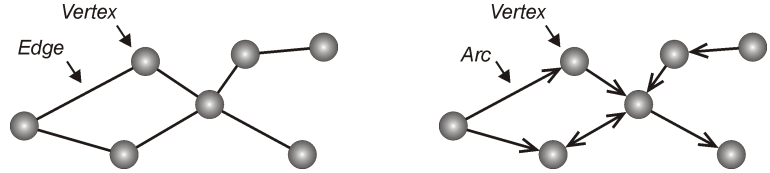


Figure 3.1 Example of a) an undirected graph with an edge and vertex indicated, and b) a directed graph with an arc and a vertex indicated.

Describing the Network Structure

The idea behind network theory is the notion that it is possible to draw relevant conclusion about the modelled system (e.g. electric power systems, railroads, internet, nervous systems, the relationship of dating on the internet, friendship among children in a school, or the organizational structure of company), by the knowledge of its topology, as represented by a graph. By measuring the structure of the network or by quantifying properties of the network when it is changed or, by some means, degraded, interesting properties of the system can be found. The modelling approach also facilitates the comparison of different types of real-life systems

There exist several terms and numerous metrics with the aim to describe and measure the *static structure of a network*, in Table 3.1 only a few of the most

commonly used are described briefly in order to give guidance to the reader, not familiar with network theory, in the understanding of appended Paper I.

Table 3.1. Brief overview over terms and metrics used in Network Theory (e.g. Johansson, 2007)

Term	**Description**	
Path	Defined as a sequence of vertices $\{v_1, v_2, \ldots, v_n\}$ such that $A(v_i, v_{i+1})=1$, i.e. there is an edge (v_i, v_{i+1}) for every i. A path where no vertex appears twice is called an *elementary path*.	
Circuit	A path that ends in the same vertex as it starts, i.e. $v_1 = v_n$. A circuit that consists of three edges is called a *triangle*. A circuit where only the first and the last vertex are the same is called an *elementary circuit*. A graph without any circuits is called a *tree* if it is connected and a *forest* if it is not.	
Length	Describes the number of edges in a path, which is equal to the number of vertices in the path minus one.	
Shortest path (geodesic)	A path starting in vertex, v, and ending in vertex, w, with the smallest possible length is called a *geodesic* between v and w.	
Distance	*Distance* is simply the length of a geodesic between v and w. The average distance of graph is referred to as the *characteristic path length*.	
Degree of v	The number of edges connected to the vertex v. If the graph is directed, one discriminates between *in-degree*, number of arcs coming in to the vertex, and *out-degree*, number of arcs coming out from the vertex. The *Average Degree of v* is simply the arithmetic mean of the degree for all vertices, v, belonging to G.	
Metric	**Description**	**Equation**
Betweenness, C_B,	A measure that tries to capture the importance of a vertex, v, or edge, e, in a network. It is a measure that describes how many shortest paths, geodesics (σ), that goes through a specific vertex or edge.	$C_B(v) = \sum_{u \in V} \sum_{w \in V \setminus \{u\}} \frac{\sigma_{uw}(v)}{\sigma_{uw}}$ $C_B(e) = \sum_{u \in V} \sum_{w \in V \setminus \{u\}} \frac{\sigma_{uw}(e)}{\sigma_{uw}}$
Clustering coefficient, C	Describes how clustered the network is in form of the density of triangles in the network (Watts and Strogatz, 1998). C_i is the *local clustering coefficient*, M_i is the number of edges that exist between the neighbours of vertex i, and k_i is the number of neighbours for vertex i	$C = \frac{1}{n}\sum_{i \in V} C_i = \frac{1}{n}\sum_{i \in V} \frac{M_i}{k_i(k_i-1)/2}$
Average Inverse Geodesic length, l^{-1}	Describes how tightly coupled the network is, (Latora et. al. 2001). N is the number of vertices and $d(v,w)$ is the distance, length of the shortest path, between v and w.	$l^{-1} = \frac{1}{N(N-1)}\sum_{w \neq v} \frac{1}{d(v,w)}$

Dynamics of Network Models

The *dynamic of the network* is the measuring of some chosen property of the network when removing or adding vertices and edges. The removal of nodes and edges are normally described as *attacking* the network. There are different *attack strategies* that usually are based on a random process or by using some measurement of the importance of nodes or edges and then removing these in a certain order. The importance is usually based on a *centrality measure* for the network. A centrality measure is some global property of the network, e.g. average inverse geodesic length (see Table 3.1), measured while the network is being attacked in succinct steps. In Figure 3.2, an example is given. The global property that is measured has the aim to reflect the performance of the network for the given attack strategy. Measuring the performance for different attack strategies yields valuable information of robustness of the network.

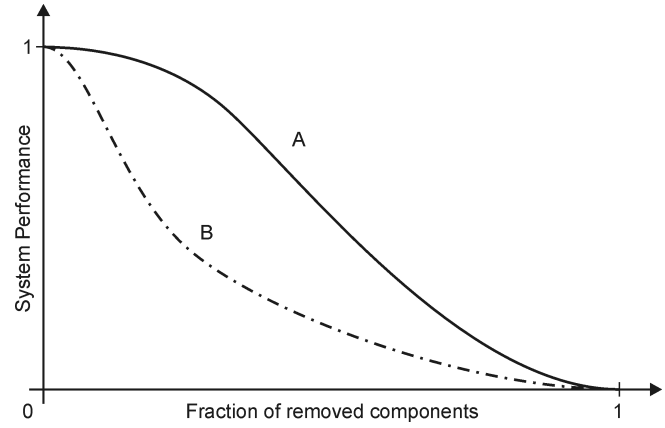


Figure 3.2. Measuring the system performance. On the vertical axis is the normalized performance of the network and on the horizontal axis is the fraction of removed components (nodes and/or edges). Let the two curves, A and B, represent the system performance for two different attack strategies. Since the system performance drops faster for attack strategy B than for A, it can be stated that the system is more robust to attack strategy A than to attack strategy B.

3.2 Network Modelling of Technical Infrastructures

There has been a wide interest in the application of network theory with the aim to analyze and understand complex systems. The following section gives an overview of some of the most relevant research in this area with respect to the present thesis. The term Network Modelling, instead of Network Theory, is deliberately used in order to capture that some of the exemplified research literature also tries to capture the physical behaviour of the system. The section should be viewed as an introduction to the application of network theory for the analysis of various technical infrastructures. Network theory applied to electrical power system is more extensively described, since this is the main perspective in the appended papers. However, in order to demonstrate the applicability of network theory to other technical systems, brief examples from transportation infrastructures and telecommunications networks are also given.

Electric Power Systems

Studies of electrical power systems with use of network theory have mostly aimed at the transmission level, in contrast to appended paper I and II where the distribution level is studied. This is because during the last decades large scale power outages have occurred in many countries around the world: Canada (1998), New Zealand (1998 and 2006), USA (1999), Sweden (2003), USA and Canada (2003), Great Britain (2003), and Italy (2003), just to name a few. These power outages have led to a need for new methods and tools for power system analysis.

Crucitti and Latora with co-authors have made several contributions in the field of network theory with respect to analysis of technical systems. Their overall approach is the study of cascading failures in complex networks based on a simple dynamical redistribution of load in the network (Crucitti et al. 2003b, 2004a). The average efficiency (Crucitti et al. 2003a) of the network is used as a measure of the performance of the network. The proposed method is used to analyze the Internet and the electrical power grid of the Western United States and in Kinney et al. (2005) the North American power grid is analyzed. In Crucitti (2004b) the structural properties of the Italian electrical power grid is analyzed and in Crucitti et al. (2005a) a network analytical approach is used to locate critical lines in high voltage electrical power grids. Although the proposed method for cascading failures has several interesting properties, it appears to be too generalized to straightforwardly be applicable to vulnerability analysis of electrical power systems.

Chassin and Posse (2005) conduct a topological reliability analysis of the Eastern and Western North American electrical power system. A Barabasi-Albert scale-free network model is used together with a simple failure propagation method. A commonly used power system reliability index is calculated (LOLP – loss of load probability) and compared with reliability indices calculated by standard power engineering methods, with closely matching results.

Albert et al. (2004) studies the North American power grid from a network perspective (14,099 nodes and 19,657 edges). In their work, they distinguish between three different node types: generators, transmission nodes, and distribution substations (i.e. not a homogenous network). The performance of the network is measured by a proposed measure called connectivity loss. Connectivity loss, CL, measures the fraction of lost connections between generation nodes and distribution substation, averaged for all distribution substations.

Holmgren (2004 and 2006) has written a licentiate and a doctoral thesis on the subject of vulnerability analysis of electrical power delivery systems based on network theory. In the licentiate thesis, the focus is mainly on assessing vulnerability of electrical transmission systems using network theory. For the doctoral thesis, the focus was shifted towards game theory.

Sun (2005) conducts a structural analysis of two power grids in China (above 110kV) and the West American power grid (above 115kV), using network theory. The paper also discusses the possibilities to utilize network theory in order to study and understand cascading failures in power networks. It is concluded in the paper that application of network theory in power systems is still on a theoretical level but highlights that network theory can play an important role to provide, reliable, effective, and crucial suggestions in order to improve the performance of large-scale power systems.

Transportation systems

In later publications of Crucitti and colleagues, the focus shifted from electrical power systems towards spatial centrality measures of urban streets (Crucitti et al. 2005b, Porta et al. 2005, Porta et al. 2006), using the same modelling approach as for the analysis of electrical power systems.

Jenelius and colleagues have made several contributions in the area of vulnerability analysis of road networks (e.g. Jenelius, 2007; Jenelius and Mattson, 2008). Vulnerability studies of both the impact of single road

failures (N-1) and area covering disruptions have been carried out. Jenelius (2007) use of the term consequence models is similar to the present thesis use of functional models.

In Demšar et al. (2008), critical locations for the street network of the Helsinki Metropolitan Area in Finland are identified by the use of Network Theory. They examine the vulnerability of the network by the use of line graphs and network theoretical metrics; cut vertices of the line graph (vertices that if removed separates the line graph into two or more subcomponents), vertices that have high betweenness, and vertices that have low clustering coefficient. As such, it is a static network approach where the metrics are calculated in order to identify critical locations.

In Zio et al. (2008), a network theoretical approach is used to evaluate the safety and the vulnerability of a section of the road network of the Provence of Piacenza in Italy. They use static measures, characteristic path length and average clustering coefficient, as well as efficiency measures, global and local, to assess the safety of the existing road network and contrasting them against road development plans. In their safety measure they also include a measure for the probability of an accident for a given link, thus extending the strictly network analytical approach towards safety and reliability. In Zio and Sansavani (2007) a similar approach is used to study the tramway network of Milano.

Telecommunication systems

Crucitti et al. (2003a) studies the average efficiency of the Internet using the same network theoretically approach as for the analysis of the electrical power grid of the Western United States and urban streets, thus illustrating the applicability of network theory for the study of differing technical infrastructures.

In Latora and Marchiori (2005) a method, based on network theory, for the identification of critical components of the network (defined as the nodes/edges crucial for the functioning) of Internet backbones is presented. They demonstrate the applicability of the method on two networks, the Ca*net3-network and the Infonet-network.

In Houck et al. (2004) a simulation approach for a telecommunication network (telephony) in a metropolitan area is given. They use this simulation approach to assess the performance of the network due to network failures (component failures) or traffic overload. This study does not strictly fall

under the category of a network modelling approach since it is a scenario based simulation approach, but it has interesting discussion of vulnerabilities for voice based telecommunication systems worth mentioning.

In Murray et al. (2007), the vulnerability of the Abilene fiber-optic telecommunication network is addressed by removing routers and assessing the performance with respect to the flow between origins and destinations and connectivity. They conclude that strict network analytic properties are not always appropriate measures for system performance when studying networks with flows.

Booker and colleagues (Booker et al., 2008) uses a network analytical approach to develop efficient computational methods, both analytical and Monte Carlo based, for assessing expected traffic loss in fiber optic backbone networks. It should be noted however, that they employ a reliability based approach and not a vulnerability based approach.

In Gao and Guo (2009) the vulnerability analysis of electric power communication networks is carried out. Two communication networks in China are evaluated by using a network theoretical approach.

3.3 Functional Modelling of Technical Infrastructures

To what extent functional models, models to capture the physical behaviour, was incorporated varied greatly in the exemplified network modelling approaches given in the previous section. For many network theoretical studies, the nodes and edges are homogenous and only structural properties of the network are considered (e.g. Holmgren, 2004). Some studies take the system representation one step further and use heterogeneous nodes, i.e. differentiates between generators, transmission and substations, (e.g. Albert et al., 2004). The most advanced network theoretical studies also include constraints on nodes and edges in order to simulate cascading effects (e.g. Crucitti et al., 2003b; Kinney et al., 2005, Sansavini, 2009).

The relation between network theoretical measures and vulnerability is not straightforward, important characteristics of the systems are lost when using a traditional network analytical approach, thus not capturing the dynamical behaviour of the system and some actions taken to enhance the resilience of a system. Traditional engineering models for capturing the physical behaviour of technical infrastructures have been around as long as the infrastructures themselves (e.g. Glover and Sarma, 1994). However, as Chassin and Pose (2005) points out for bulk power systems, the analyses of technical

infrastructures are computationally very burdensome when using standard engineering methods. This will lead to the fact that only a very small subset of all possible scenarios are examined It is argued that by using a network theoretical approach and simplified functional models, it is possible to study much larger parts of all possible scenarios in the quest of finding system vulnerabilities.

In Holmgren (2004) the closing remark is that it is an open question whether graph modelling should be extended or if it is better to adapt existing power engineering simulation methods for vulnerability analysis. The author, like (Holmgren, 2006), believes that the answer of what models and methods to use probably lies in between. In Eusgeld et al. (2009) a framework for the use of network analytical approaches for screening analysis and detailed modelling of the operational dynamics for the screened out vulnerabilities is suggested, thus combining the two approaches in two successive stages. The modelling approach in the presented research (appended paper I, II and V) can be viewed as a middle ground of the two approaches above, using a network analytical approach together with simplified functional models in order to achieve reasonable computational times. In Murray (2008) an overview of different approaches (scenario-specific, strategy-specific, simulation, and mathematical modelling) for the vulnerability analysis of networks is given, where it is concluded that multi-methodological approach, taking advantage of the different methods benefits, would facilitate greater understanding of infrastructure vulnerabilities.

It is the author's belief that risk and vulnerability studies of technical infrastructures would benefit from cross-fertilization between traditional engineering disciplines, mathematical modelling of complex systems, resilience engineering, and risk and vulnerability management. The present thesis is believed to be a step in that direction.

3.4 System Modelling Approach

The author argues for an approach of separating the structural model and the functional model of a system, see Figure 3.3. There are several advantages with this approach of modelling systems. The tools and methods as presented in the thesis can be applied to other single technical infrastructures than electrical power systems and applied to interdependent systems other than the railway systems. What changes from different systems is the functional model, i.e. how the system reacts to perturbations and the estimation of the consequences, while the methods for vulnerability analysis remains the same. The modelling approach enables the vulnerability analysis of both structural

strains (removal of system components) and functional strains (changes of supply and demand). Lastly, the separation gives a common platform, i.e. the structural model, for all types of technical systems that has proven to be a fruitful approach in order to combine different technical infrastructures into one "system-of-systems" model in the pursuit of understanding and analyzing the effects of interdependencies (appended paper V).

The physical properties describing the system behaviour are generally well researched for most technical infrastructures and should be used, where applicable, as input for the derivation of functional models. The choice of appropriate functional models depends on the aim of the analysis; they could be full-scale physical models or simplified models depending on choice of trade-off between computational times and fidelity of the result.

In the structural model, all the components are modelled in accordance with their geographical co-ordinates. This has the benefit of enabling the use of GIS-applications, more easily mediate results, and, most importantly, enables vulnerability analysis with respect to geographically confined strains. In order to limit the size of the structural model, components that have the same basic structural influence can be merged into one (e.g. representing the breaker and the cable in an electrical distribution system with an edge). The same trade-off issues regarding abstraction versus fidelity are also valid here.

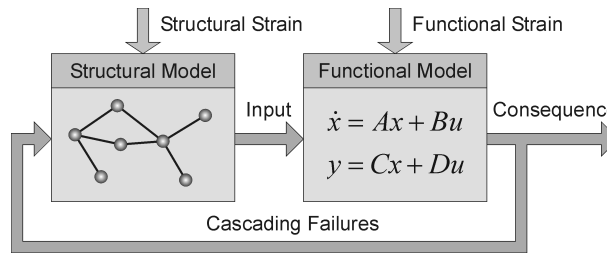


Figure 3.3. Schematic representation of the proposed division of the structural model and the functional model for any given system representation.

3.5 Interdependency Modelling Approach

There is currently much effort devoted in the research community towards developing models and methods for the analysis of interdependent infrastructure systems. An overview of methods and models are given in (Pedersen et al., 2006; Eusgeld et al., 2008; Xiao et al., 2008). The research literature regarding infrastructure interdependencies can roughly be divided into two categories: *empirical approaches* and *predictive approaches*. Empirical approaches aims at analyzing past events in order to increase the knowledge and understanding of interdependencies (e.g. McDaniels et al., 2007; Chang et al., 2007; Zimmerman and Restrepo, 2006; Rahman et al., 2009). This type of studies helps the understanding of the cascading mechanism, clarifies to what extent the society is affected by cascading infrastructures failures, and gives general guidance towards policy and decision-making. Predictive approaches, on the other hand, aim at modelling and simulating interdependent infrastructure systems in order to improve the understanding of how disturbances cascade through interconnected infrastructures and anticipate the effects of interdependencies. There exist a wide range of different models and methods, depending on the purpose and perspective of the analysis. These include, for example: economic-mathematical models (e.g. Haimes and Jiang, 2001), economic system dynamics models (e.g. Min et al., 2007), agent based models (e.g. Brown et. al, 2004), Petri-net based models (e.g. Laprie et al., 2007), and network models (e.g. Apostolakis and Lemon, 2005). The two approaches are complimentary, and necessary in the effort of using them as input to risk and vulnerability analysis and as a basis for strategic planning of prevention and mitigation strategies. The research, as presented in the thesis, falls in the second category of these two approaches.

The existing methods and models all address the issue of interdependencies, but from different viewpoints. The challenges regarding understanding, characterizing, analysing and modelling these types of interdependent systems are immense and the research in the area is still in an early stage (Little, 2002; Pedersen et al., 2006). The author argues that models and methods that have different viewpoints are necessary in order to appropriately and comprehensively address the issue of critical infrastructure interdependencies, i.e. it is not believed that it is possible to find a universal, all-encompassing, model (Murray et al., 2008; Eusgeld et al., 2009).

The proposed modelling approach (Johansson and Hassel, 2010; appended paper V) for vulnerability analysis of interdependent infrastructures takes as starting point the single system modelling approach, as presented in the previous section. Each system is modelled with a structural and a functional

model together with the geographical location of the components, in accordance with section 3.4, and dependencies between infrastructures components are modelled as *dependency edges* between the structural layers of the infrastructures, see Figure 3.4.

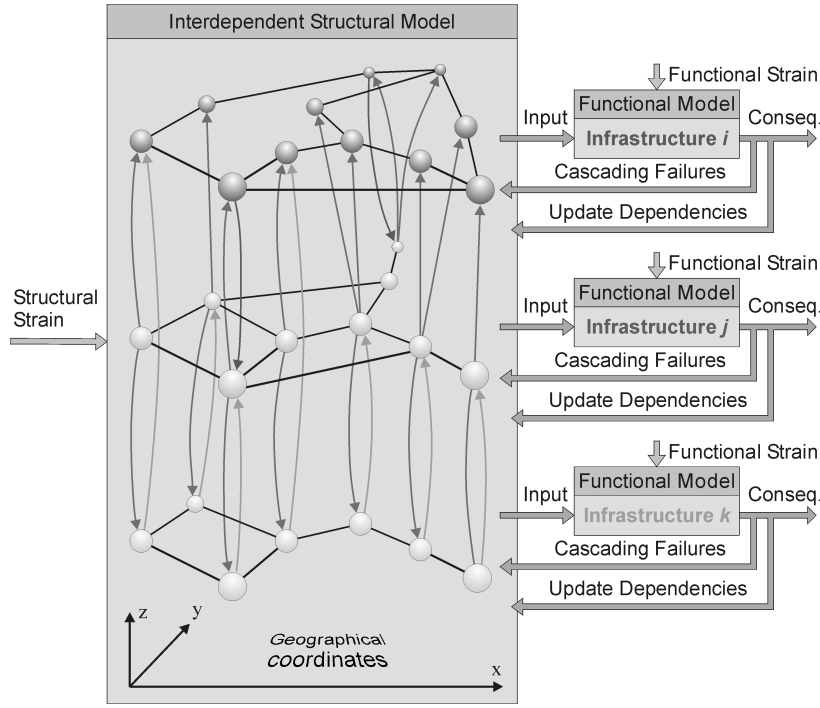


Figure 3.4. Schematic representation of the proposed interdependency modelling approach.

As stated earlier, there exist several frameworks and definitions regarding dependencies and interdependencies. The more commonly cited framework for characterisation is the one proposed by Rinaldi et al. (2001). Here interdependencies are characterised as either *physica*l (an output from a system is required as an input to another system and vice versa), *cyber* (the state of a system is dependent on information transmitted through an information infrastructure), *geographic* (two or more systems can be affected by the same local event, i.e. they are spatially proximate), and *logical* (includes all other types of interdependencies, for example related to human behaviour). In Zimmerman and Restrepo (2006), a coarser characterisation is

given: *functional* and *spatial* (where spatial is identical to geographic interdependency as referred to above). In the proposed modelling approach, inter-/dependencies are characterised as either *functional* (arguing that physical, cyber, and logical inter-/dependencies can be treated in the same basic modelling way) or *geographical* (identical to the definition by Rinaldi et al. and Zimmerman's spatial).

It is argued that interdependency is a macro-property of "system-of-systems" and on the component level of technical infrastructures, only dependencies between components exist. *Dependency* is defined as a unidirectional relationship, the state of infrastructure *i* is dependent on the state of infrastructure *j*. *Interdependency* is defined as a bidirectional relationship, the state of infrastructure *i* is dependent on the state of infrastructure *j*, *and* vice versa. These definitions are in accordance with Rinaldi et al. (2001). In the proposed modelling approach, each system is separately mapped and modelled in accordance with their system model (structural and functional) and their dependencies of other systems. In the simulation the same strategy applies, each system only acts upon local information regarding the state of their dependencies to other systems. The main benefit is that models for each of the system can be developed together with domain specific experts. Each of the systems is brought together in a "system-of-systems" model, revealing how the dependencies add up and enables the analysis of interdependencies in a macro-perspective. Important to note in this context is that dependencies can be of *first order* (direct dependencies), which are usually quite easily spotted and their existence rather well known, and *higher order* dependencies, which is more difficult to understand the effects of without explicit modelling and simulation. For example, if infrastructure *i* is dependent on infrastructure *j* and infrastructure *j* is dependent on infrastructure *k*, then a second order dependency exists between infrastructure *i* and *k*. These types of higher order dependencies and interdependencies are captured with the proposed modelling approach.

Technical infrastructures are usually very tightly coupled with each other, in the sense that failures in an infrastructure directly have an impact on dependent systems. In order to loosen the tight coupling between infrastructures, buffers are usually incorporated between the infrastructures. For example the use of UPS (Uninterruptible Power Supply) in telecommunication systems and the use of water storage in water supply systems. The common denominator for these types of buffers is that they have limited capacity and thus time of operation. This type of time-dependency is also incorporated in the proposed modelling approach as a

time delay between the loss of a dependency and the impact of it, where the length of the time delay represents the buffer capacity. In this perspective, it becomes important to address the issue of restoration times for failures, since it will determine whether disturbances are spread between infrastructures that are separated by buffers. In appended paper IV, an approach for the assessment of restoration times with respect to response system capabilities is presented.

Chapter 4

Vulnerability Analysis

Now it is time to bring together concepts and theory along with the modelling approach, described in the previous two chapters, in order to discuss the approach for vulnerability analysis of technical infrastructures. Here the emphasis is on the structural vulnerability analysis of technical infrastructures. The proposed methods (appended papers I, II, and V) all address the vulnerability analysis of technical systems when exposed to strains that affect the structural part of the infrastructure (i.e. component failures). It should be noted however that the presented modelling approach also opens up for the possibility to address vulnerabilities due to functional strains, also in combination with structural strains.

The chapter starts with a section discussing the challenges with vulnerability analysis of technical infrastructures, followed by a section regarding the modelling of strains. The four following sections introduce three different types of vulnerability analysis of technical infrastructures (as used in appended papers I, II and V).

4.1 Challenges for Vulnerability Analysis

Technical infrastructures are rather complex systems in respect of the sheer number of components they consist of, the societal context they operate in, and the knowledge it requires to understand and analyse their behaviour. It is thus important to employ a systematic approach for the vulnerability analysis of such systems, in order to ensure appropriate and valid results that can be used as input to policy and planning processes.

There are several challenges regarding structural vulnerability analysis of technical infrastructures. One of the challenges is the large number of components they consist of, which leads to a "combinatorial explosion" when it comes to analysing component failures. For structural vulnerability analysis

of technical infrastructures, the number of possible system states to cover will grow rapidly with the number of components the system consists of and the order of simultaneously removed components of the system. In fact, the number of possible system states to analyse will be:

$$\frac{n!}{(n-k)!\cdot k!} \tag{4.1}$$

where n is the number of components in the system and k is the number of simultaneously component failures. For a network consisting of 800 components (i.e. roughly corresponding to the normal size of an urban electrical distribution system on the 10kV level) the number of scenarios to analyse will be: 800 for one component failure, about 314 000 for two simultaneous component failures, and roughly 85 000 000 for three simultaneous component failures.

The sheer amount of scenarios that has to be analysed for a comprehensive vulnerability analysis leads into the trade-off problem regarding fidelity versus abstraction of the models (e.g. Eusgeld et al., 2009). Although engineering models have a high level of fidelity, i.e. a good correspondence between analysis result from the model and reality, they are computationally burdensome. Mili et al. (2004, p. 40) points out that, coming from an engineering perspective, in bulk power transmission systems planning and operation a "… N-k security analysis for k > 1 is perceived as being impossible to achieve due to the huge number of cases that need to be investigated". On the other hand, using very abstract models will usually lead to a lower fidelity of the result and it might be hard to go from the analysis result to concrete suggestions of improvement. The models and the methods for vulnerability analysis, as presented in the thesis, were all implemented into computer simulation programs. The level of fidelity for the models in conjunction with the types of analysis that were performed was thus ultimately constrained by memory availability and feasible simulation times.[5]

[5] As a note of interest: The simulation times for the analysis in appended paper I was about 8-12 hours for the global vulnerability analysis for each type of strain. The critical component analysis in appended paper II took about 36 hour for three simultaneous component failures. For appended paper V the simulation time was about 3,5 days for the global vulnerability analysis and roughly 9 hours for the critical component analysis for two simultaneous failures (estimated time for three simultaneous failures was 150 days). The code was implemented in Visual Basic®

The general approach of the functional models used in the research was to use breadth first search algorithms combined with capacity constraints.

It is also a practical challenge to map the systems into models due to the large amount of components, availability of data, fragmented ownership, and the reluctance of the stakeholders to share classified information about infrastructures. This especially becomes a challenge when addressing the issue of interdependency analysis of technical infrastructures, a view shared by (de Bruijne and van Eaten, 2007) and (Kröger, 2008).

4.2 Modelling Strains

The outcome of the vulnerability analysis critically depends on how the strain is organized (e.g. Murray et al., 2008). In structural vulnerability analysis, strains are achieved by removing components, either randomly or in a targeted fashion. These are called *attack strategies* in network theoretical approaches. Random attacks are the removal of components in a random fashion, where each component has equal probability of being removed. Targeted attacks are the removal of specific components or removing components in decreasing order of their criticality. The criticality of a component is usually described by different types of topological measures (e.g. node degree or beetweenness). It is also possible to use non-topological criticality measures, i.e. functional measures, for targeted attacks. In electrical power systems it would, for example, be possible to target overhead lines (edges) in order of their relative length or substations (nodes) in order of their rate of loading. The attack strategies are a way of finding the middle states of the system, in accordance with section 2.2. By assessing the corresponding consequences for these middle states, the vulnerability of the system can be assessed. The attack strategies used in the present thesis for global vulnerability analysis are random removal and targeted attacks based on centrality measures (appended paper I, II, and V).

The applied strain, removal of components, corresponds to components entering *failure states*. The failure state for a component is for the presented research binary, i.e. either working or not. There can be a number of reasons for a component entering a failure state: natural hazards, terrorism, antagonistic threats, technical failures, accidents, human failures, or maintenance reasons.

[I] and Matlab® [II and V] and run on a computer with a single core AMD Athlon XP 2500+ processor.

The *type* of a strain corresponds to what type of attack strategy is used. The *magnitude* of strain corresponds to the amount of components that have been removed.

4.3 Three Perspectives

All the challenges as described in 4.1 put constraints on the type of vulnerability analysis that can be performed. As Haimes and Longstaff (2002) and Murray et al. (2008) also point out, vulnerability is a multifaceted concept and relying on a single measure or approach to describe systemic weaknesses might be hazardous. In the presented research, three different perspectives are used in the efforts to attain a picture of technical infrastructure vulnerability. It is argued that the three perspectives give complementing, and to some degree overlapping, crucial information about a systems vulnerability.

The first perspective is *Global Vulnerability* (appended papers I and V), which gives a good overview of what type and magnitude of strains the system (also including system-of-systems) is vulnerable to. This corresponds to the perspective that most network analytical approaches take. The major shortcoming is that due to the immense amount of scenarios that has to be analysed for large magnitudes of strain, only a sample of scenarios can be analysed in concurrence with the challenges stated above.

The second perspective is C*ritical Components* (appended papers II and V). Here the emphasis is to exhaustively analyse all possible scenarios up to a certain type and magnitude of strain. This gives a certainty about the inherent vulnerabilities of the system (also including system-of-systems). The shortcoming is that only a significantly small portion of the possible magnitude of strain can be analysed.

The third perspective is *Geographical Vulnerability* (appended paper V), which concerns finding vulnerabilities due to spatially close co-location of system (also including system-of-systems) components. Here the type of strain is geographically related and the magnitude of strain corresponds to the size of the geographical area or volume. The benefit of this type of analysis is that it is easier to go from identified vulnerabilities to geographically constrained hazards and threats (such as fires, bombs, storms, floods, tsunamis, and hurricanes).

4.4 Global Vulnerability

The aim of global vulnerability analysis is to describe the vulnerability of a system for different types and magnitudes of strain. The method for assessing global vulnerability of a system is based on measuring the performance of a system model, may it be a single system or interdependent system-of-systems, for different strains. The result of an analysis is usually presented in a plot with the performance of the network plotted against the magnitude of the strain. The performance drop is usually described by some consequence measure, e.g. amount of unsupplied energy for a power system or the number of travellers who cannot reach their destination for a transportation system. By studying this type of plots, conclusions regarding the systems vulnerability can be drawn. A network is considered as vulnerable if the performance is highly degraded, i.e. there is a high degree of loss of function, for small magnitudes of strain. Since the vulnerability of the system is studied, the measure of performance drop is initially zero and normally rises for higher magnitudes of strains. Figure 4.1 illustrates the basic concept of global vulnerability plots, in analogy with section 3.1. The figure illustrates the system performance drop for three different types of strain, labelled A, B, and C. Since the performance drops more rapidly for strain A than for strain B and C, strain A is considered more harmful to the system than strain B and C. The system is thus more vulnerable for that type of strain. Figure 4.1 could also illustrate the performance drop for three different systems given the same type of strain. Thus, it is possible to benchmark systems against each other, under the assumption that the performance drop can be equally measured for the different systems.

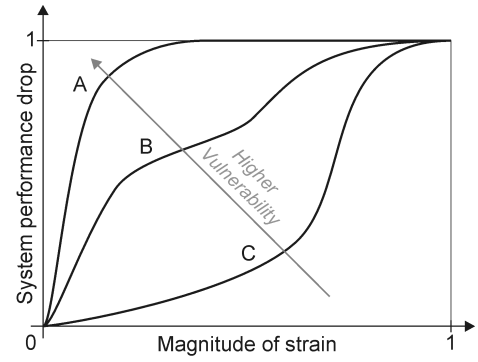


Figure 4.1. System performance drop for three different types of strain, or the performance drop for three different systems given the same type of strain.

Figure 4.2 shows the result from a global vulnerability analysis for a 10 kV electrical distribution system for a city, consisting of 352 nodes and 352 edges with the strain type random removal of nodes and the magnitude of strain from one up to all nodes removed. The number of customers without power supply is used as the measure for the system performance drop. The black line shows the mean consequences for 50 000 simulations. The light grey area contains 90% of the calculated consequences. The dotted grey lines illustrate maximum and minimum consequences found for a given magnitude of strain. The figure clearly shows the variability of consequences that exists for a given magnitude of strain. Even if 17.6 million scenarios were analysed[6], only an extremely small portion of all possible scenarios was covered, potentially overlooking important scenarios. The global vulnerability analysis however gives an idea of how the system reacts to different magnitudes of strain and the possible variability of consequences depending on the order of which components are removed. The result can also be used to describe the probability of the consequences becoming higher than a certain threshold for a given magnitude of strain, see Johansson and Hassel (2010).

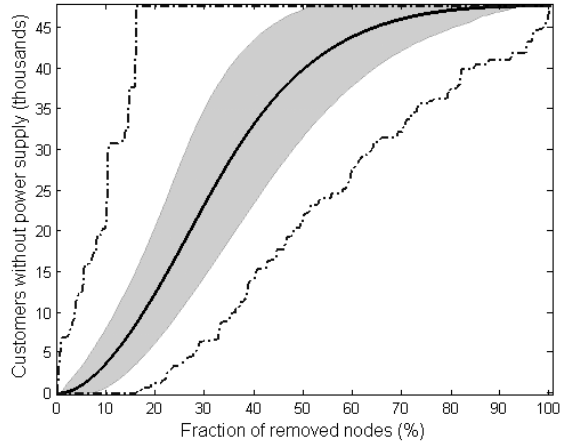


Figure 4.2. Results from a global vulnerability analysis, with 50 000 iterations, were the strain is random removal of nodes for an electrical distribution system. The thick black line is the average value, the grey area contains 90% of the consequences for a given fraction of removed nodes, and the dotted grey lines are the minimum and maximum consequences found for a given magnitude of strain.

[6] 50 000 runs with the consecutive removal of zero up to all nodes and consequence evaluation for each consecutive step, i.e. 50 000·352 ≈ 17.6 million.

4.5 Critical Components

The global vulnerability analysis gives important information about the overall vulnerability of the studied system when exposed to large variability of the magnitude of strain. Another important aspect is to identify components that are highly critical for the system performance. These critical components point out where mitigating efforts should be focused in order to reduce the vulnerability of the system with respect to small magnitudes of strain. The criticality of a component is described by the consequences that arise when it fails to perform its intended function. Critical components can also be viewed as local vulnerability of the system, where the failure of a component or a set of components is regarded as the strain to the system.

A *failure set* is a set of components that fail simultaneously. The size of the failure set is defined by the number of components that are included in the failure set. The order of a failure set, k, is equal to the failure set size, i.e. a third order failure set consists of three components that are out of function simultaneously. This is in analogy with the N-1 design criterion, where k is equal to one. A component that is critical for certain set sizes is defined as a k:th order critical component.

Exhaustive scenario analysis for all possible combinations of component failures will yield the full range of consequences for different orders of simultaneous component failures. The critical component analysis is thus a way of identifying, for the given strain, all possible middle states of the system (in analogy with section 2.2), thus addressing the issue of completeness of the vulnerability analysis. This completeness has a major shortcoming, it is only possible to analyse up to a small order of critical components due to computational constraints. For the exemplified electrical distribution system in the previous section analysing only critical nodes, the number of scenarios would be: for N-1 352 scenarios, for N-2 roughly 62 000 scenarios, for N-3 roughly 7.2 million scenarios, and for N-4 roughly 628 million scenarios.

Another issue when evaluating critical components is the large amount of scenarios and associated consequences that the analysis give rise to. To be able to more easily rank and identify critical components and for what order they are critical, the concept of *Synergistic consequences* has been developed (appended paper II). Synergistic consequences are the consequences a failure set give rise to that can not be traced back to any subset of the failure set, i.e. the consequence that in some sense is due to the composition of the involved components in the set. The notion of synergistic consequences is therefore very useful in the screening of highly critical components. In addition to the

use of synergistic consequences, it is also necessary to have a way of ranking the criticality of single components and combination of components. In appended paper II an approach for this is suggested. The identified critical components give valuable input regarding which components that should be studied in further detail, either for vulnerability mitigation activities or for analyses regarding the probability of a threat or hazard exploiting the vulnerability.

4.6 Geographical Vulnerability

Geographical vulnerability analysis is the third perspective of structural vulnerability analysis. Here it is important that the components of the system are modelled in accordance with their geographical location. A strain is then applied to a geographically confined cell space (i.e. an area or volume), and components situated within this cell space are removed. The magnitude of strain corresponds to the size of the cell space. Normally the cell space is defined to be an area (square, hexagon, circle, triangle etc.). The results of geographical vulnerability analysis are highly dependent on the cell size, the shape of the cell and displacement of the cell grid. The benefit of performing geographical vulnerability analysis is that critical geographical locations can be found (e.g. redundant power cables that are co-located) due to geographical dependencies. Another benefit is the generally good correspondence between the strain and hazards/threats that could exploit the vulnerabilities. Such an analysis also reveals what geographical areas are most vulnerable and their level of vulnerability compared to other areas.

There are relatively few research articles addressing the issue of analysing geographical vulnerabilities, none have been found where both functional and geographical interdependencies between infrastructure systems are taken into account at the same time and only a few articles either address single infrastructures or multiple infrastructures.

Jenelius and Mattson (2008) use square cells (with three different sizes; 12.5, 25 and 50 km) and examine the impact of cell size and grid displacement on the result when assessing the vulnerability of road networks under area-covering disruptions. Patterson and Apostolakis (2007) use a hexagonal grid approach (with cell size with the radius of 7 m, simulating a bomb) to study geographical interdependencies (omitting any functional interdependencies) between technical systems in a university campus area. Robert and Morabito (2010) present a methodology for identifying and evaluating geographical interdependencies among critical infrastructures based on a manual top down analysis of geographically interdependent infrastructures. In Restrepo et al.,

(2006) geographical interdependencies in electric power infrastructures is analysed.

In appended paper V, a method for geographical vulnerability analysis is presented, taking into account both functional and geographical interdependencies at the same time.

Chapter 5

Managing Socio-Technical Systems

The first section of this chapter briefly discusses the use of vulnerability analysis as a supplementary part of traditional risk analysis, and puts vulnerability analysis in a risk and vulnerability management perspective (appended paper III). In the second section, a method for the assessment of socio-technical system's recovery times is discussed. This is addressed by taking a socio-technical view of technical infrastructure and assessing response system capabilities, an important aspect when analysing vulnerabilities (appended paper IV). It is recognized by the author that the discussion in this chapter is rather rudimentary, but it fulfils its purpose in the effort of putting the presented vulnerability analysis methods in a wider perspective.

5.1 Risk and Vulnerability Management

The identification of a system's vulnerability to different types and magnitudes of strains is extremely important. The research as presented in appended paper I, II and V gives valuable insight into how to address the structural vulnerability of technical infrastructures, but in order to address the management of risks and vulnerabilities of technical infrastructures a wider scope is needed. In appended paper III such a wider scope is discussed regarding electrical distribution systems. Some of the reflections made in the paper are however argued to be valid for the risk and vulnerability management of other technical infrastructures as well.

The arguments for performing a vulnerability analysis are: (1) the inherent problems of finding the events that could lead to large consequences when initiating the analysis by identifying threats and hazards that could affect the system, i.e. severe deficiencies might be overlooked (2) the inherent problems regarding accurate estimations of the probability for unlikely events and finding the "true" probability for each and every component in a technical system.

As stated earlier, see section 2.2, vulnerability analysis is regarded to give a complementing view in respect to a risk analysis. For a *risk analysis*, the initial focus is primarily to identify threats and hazards that could affect the system. Here the initial concern is to identify threats and hazards and the likelihood of these, i.e. the *screening of scenarios* to consider is based on the *likelihood* of occurrence. In order to identify risk scenarios that could lead to large consequences, usually requiring the occurrence of several simultaneous events, a very open and imaginary mind of the analyst is required. For risk scenarios regarded as unacceptable, the *mitigation strategy* is normally to insert some form of *barriers* between the threat or hazard and the system. For a *vulnerability analysis*, the initial focus is to find vulnerable states of the system, i.e. system states associated with large consequences. Here the consequences that could arise are the main concern, i.e. the *screening of scenarios* to consider is based on the *consequence*. For vulnerability scenarios regarded as unacceptable, the *mitigation strategy* is normally to build a more robust and resilient system by *changing the system*. As such, it is argued that risk analysis and vulnerability analysis give complementing views of the system and leads to different types of mitigation strategies.

For example, the criticality component analysis can be used for exhaustive system vulnerabilities identification for small magnitudes of strain. With the proposed criticality measure (appended paper II) a priority ranking of which components that need to be especially robust and reliable can be established. This type of analysis also clearly states the maximum consequences that could arise given the type and magnitude of strain. For example, consider an electrical distribution system. The analysis gives that for two simultaneous failures, a maximum of 30% of the customers will be unsupplied. For three simultaneous failures, the corresponding consequence is determined to be 50%. This could be regarded as an acceptable vulnerability of the system. However, if one case of two simultaneous failures gives rise to 100% percent of the customers being unsupplied, and for the rest of the scenarios, with two simultaneous failures, a maximum of 30% of the customers are unsupplied. This could be determined to be an unacceptable vulnerability, and mitigation strategies should hence be considered.

Coming from a vulnerability analysis, the first step includes a screening of the scenarios in accordance to their level of vulnerability. Then it is possible to assess whether or not mitigating efforts are necessary to reduce the identified vulnerabilities. Some vulnerabilities might be associated with unacceptable consequences given the type and magnitude of strain, and thus directly have

to managed.[7] However, for most vulnerabilities a notion of the probability for a threat or hazard exploiting the vulnerability is desirable. Otherwise, overly robust and non cost-effective systems might be the result.

The second step is thus to broaden the picture by addressing the probability of threats or hazards exploiting the identified vulnerabilities, i.e. going from the vulnerability analysis towards a risk analysis. Theoretically, it is straightforward to incorporate the probability of threats and hazards exploiting the vulnerabilities in a technical infrastructure, for example by using generic failure rates of components. However, often the generic failure rates are not suitable for quantifying the probability of common cause failures and malicious attacks[8]. This in addition to the difficulty in finding a true probability for the failure of each and every component in technical infrastructure, which is usually dependent on a number of factors such as: age, geographical location and level of maintenance. As such, there are several inherent difficulties in finding a "true" probability (c.f. Hansson, 2005). Given that knowledge of both the consequences and the probability of the threat or hazard exploiting the vulnerability exist, it is straightforward to use the result from vulnerability analysis in a risk analysis context, in analogy with section 2.2.

The last step is to take a risk and vulnerability management perspective. Here known hazards and threats, i.e. more likely scenarios that can affect the system, should be addressed in order to complement the vulnerability analysis. This equates to, in the author's perspective, performing a risk analysis of the system. In a management perspective other types of questions become important; "What can be done and what options are available? What

[7] The consequences that arise might not be acceptable to the society, leading to a decision of mitigating efforts although with a vague conception of the probability of occurrence. This line of reasoning has similarities with the "Precautionary principle". An example of the use of the precautionary principle is the avoidance of constructing high-voltage lines and equipment near residential areas due to the potential harm electro-magnetic fields in the low frequency range may have on humans, a subject which has been heavily debated.

[8] For example, what is the probability that a group of civilians actively sabotages a substation, rendering 25 000 customers without electricity? This incident happened in Malmö, Sweden, the 7 October 2006. A group of civilians threw in a floor lamp in a transformer station, short-circuiting the transformer station. The probability for this type of incident could be covered by the generic failure rate, however the generic failure rate does not hold information on a sufficient level of detail to find and assign a probability to the incident.

are the tradeoffs in terms of all relevant costs, benefits and risk? … What are the impacts of current decisions on future options" (Haimes, 2009b). Here, clearly, a new set of issues arises that leads to a need of other methods and theories, such as multi-criteria decision analysis and cost-benefit analysis, beyond the scope of the present thesis. However, it is argued that the proposed methods for vulnerability analysis are of great value in the effort to attain valid inputs to such management questions.

5.2 Response System Capabilities

Technical infrastructures are viewed as being socio-technical systems, as much of the complexity associated with these types of systems stems from the interaction between technical systems and the actor systems (e.g. Verwater-Lukszo and Bouwmans, 2005; Appicharla, 2006). The technical system is loosely defined here as the components that build up the physical systems, enabling the transportation of desired goods in technical infrastructures. Actor system is here loosely defined as the system that is needed for the management, operation, maintenance and restoration of the technical systems. As such, they have a major impact on the vulnerability of a technical infrastructure. As in Little (2004 and 2005) it is argued that a holistic view of socio-technical infrastructures is needed. One aspect of addressing this holistic view is to develop methods and simulation models, enabling analysis from different perspectives. As Little (2004) and Thissen and Herder (2003) point out, this is a research topic that needs to be further addressed.

In appended paper IV a method for the analysis of response system capabilities is presented and its applicability tested in an empirical study of the Swedish railway system. The response system is the actors and resources required to restore a technical system after strain. The response system capability is an essential aspect of the technical infrastructures vulnerability, as it to a large extent defines the system's ability to return to normal operation after different types and magnitudes of strain. For the development of the method, both theories from system thinking and resilience engineering were used.

The fundamental idea of system thinking is to study systems as wholes rather than their elements in separation, as a way to address complexity (e.g. Senge, 1994; Checkland, 2006). As such, a system is defined to consist of a number of elements and relationships between these elements. This approach has several similarities to that of network theoretical studies, opening up for the possibility of studying socio-technical systems with the use of a network analytical approach. Emergency response system networks have been studied

with this approach (Uhr, 2009). An important aspect of the system thinking approach is the definition of a system boundary. A system boundary represents the distinction between what is part of the system and what is part of its environment, and the boundary must be defined with respect to the elements that have an influence on the problem situation being studied.

The second theoretical background for the development of the method is resilience engineering. Resilience engineering is described by Hollnagel et al. (2006, p.4) as "the ability of systems to anticipate and adapt to the potential for surprise and failure". There exist several definitions of resilience (eg. Haimes 2009a), and the field of resilience engineering is still under formation. The definition adapted here is the one proposed by McDaniels et al. (2008, p. 310): "[complex system's] capacity to absorb shocks while maintaining function". McDaniels and colleagues further refers to two key properties of resilience: *robustness*, a systems ability to withstand a certain amount of stress without suffering degradation or loss of function, and *rapidity*, a system's speed of recovery of function from an undesired event back to a desired level of function. These properties match the discussion in section 2.2, i.e. vulnerability as the antonym to robustness and rapidity (and hence resilience).

Based on these two theories a method was developed (appended paper IV) and used for an empirical study of the Swedish railway system. The focus in the empirical study was to assess the time it takes for the actor system to restore the technical system when it is affected with strains of varying type and magnitude. The introduction of *response curves* is central to the presented assessment method. A response curve depicts, in general, the time it takes to restore a system with respect to varying magnitudes of strain, and consequently there will be different response curves for different types of strains and for different actors. The response curves can be used for comparing and assessing the response capacity, in a proactive manner before actual incidents reveal critical limitations, and thus provide a basis for decision-making regarding risks and vulnerabilities of socio-technical systems. The response curves also give valuable input regarding restoration times to the method for structural vulnerability analysis of interdependent infrastructures (appended paper V). In this context, the response curves can be used for determining the restoration time, both for single value description as well as for the correlation between repair time and magnitude and type of strain affecting the technical infrastructures.

Chapter 6

Summary of Appended Papers

6.1 Paper I – Global Vulnerability Analysis

Johansson, J., Jönsson, H., Johansson, H., (2007). Analysing the Vulnerability of Electric Distribution Systems: A Step Towards Incorporating the Societal Consequences of Disruptions, *International Journal of Emergency Management*, Vol. 4, No. 1, pp.4–17.

The paper presents a method for global vulnerability analysis of technical infrastructures, incorporating societal aspects of disruptions. The method was used for an empirical analysis of the electrical distribution systems (10-20kV) in two municipalities in Sweden. The system was modelled in accordance with the approach presented in section 3.4. Power in-feed nodes and customer nodes (i.e. power consumption nodes) were differentiated. The functional model consisted of a search algorithm checking whether customer nodes had an unbroken path to one or several in-feed node, if so it was assumed that the customers could be served (no capacity constraints). The paper proposed a new performance measure called Customer Equivalent Connection Loss (CECL). Customer equivalents were introduced as a mean to be able to differentiate between customers. Two new network analytical measures where introduced, Societal Vulnerability Coefficient (SVC) and Design Coefficient (DC), in order to facilitate the comparison of the vulnerability regarding both different types of strains (termed perturbations in the paper) to one system and of different systems through single measures. The proposed method and measures are argued to be useful when analysing the vulnerability of technical infrastructures for different magnitudes and types of strains.

Author's contributions: The author played a *medium role* in the planning and preparation of the research, empirical data collecting, method development, analysis and writing of the paper and a *minor role* in computer program implementation.

6.2 Paper II – Critical Components

Jönsson, H., Johansson, J., Johansson, H., (2008). Identifying Critical Components in Technical Infrastructure Networks, *Journal of Risk and Reliability*, Vol. 222, Part O, pp. 235-243.

This paper presents a novel method for identifying and ranking critical components in technical infrastructures. The method was exemplified for a small fictional system and used for an empirical analysis of an electrical distribution system in a city (10kV). The modelling approach was in accordance with section 3.4. In addition to the functional model in appended paper I, the capacity of power in-feed nodes and power out-take nodes was also considered. The criticality of a component or a set of components is defined as the vulnerability of the system to failure of these components or set of components. The method was developed with the aim to enable analysis of full-scale technical systems with respect to several simultaneous failures. The analysis of critical components gives rise to a respectable amount of scenarios to consider. A screening method based on the introduced concept of synergistic consequences was proposed. Synergistic consequence is the consequence that cannot be accounted for when adding the consequences of individual failures for a failure set. A metric, based on the concept of synergistic failures, for ranking components in accordance with their criticality, given the failure set size, was also presented. It is concluded that the proposed method facilitates the identification of critical components, and sets of components, for large-scale technical infrastructures.

Author's contributions: The author played a *medium role* in the planning and preparation of the research, empirical data collecting, method development, analysis and writing of the paper and a *major role* in computer program implementation.

6.3 Paper III – Risk and Vulnerability Management

Johansson, J., Svensson, S., (2008). Risk and Vulnerability Management of Electrical Distribution Grids, *Nordic Distribution and Asset Management Conference* (NORDAC 2008), Bergen, Norway, September 8-9.

The paper discusses the concept of risk and vulnerability management of electrical distribution systems, and puts it in a context with other legislative and regulatory frameworks. In 2006, amendments to the Swedish Electricity Act came into force, stipulating that electrical distribution systems owners[9] must; on a yearly basis perform risk and vulnerability analysis and derive appropriate mitigation plans. The paper discusses the process for risk and vulnerability management and highlights important aspects for this process. Important issues that require further research and input from stakeholders are also illuminated, still valid today. The authors conclude that risk and vulnerability management offers a systematic and transparent approach of identifying and devising mitigation strategies for both the technical infrastructure and the organisation supporting it. It should be noted that the *ex ante* Network Performance Assessment Model (NPAM) for tariff regulation as discussed in the paper was aborted in 2009, and will be replaced with an *ex post* regulation in 2012.

Author's contributions: The author played a *major role* in the planning and preparation of the research, analysis and writing of the paper and a *medium role* in empirical data collecting.

[9] In Sweden, there exist three major electrical distribution owners at the sub-transmission level and about 160 smaller electrical distribution companies at the distribution level that are affected by the discussed legislation (SFS 1997:857). The Swedish transmission system owner (TSO) is not affected by this legislation, but must perform risk and vulnerability analysis in accordance with (SFS 2006:942).

6.4 Paper IV – Socio-Technical Systems

Wilhelmsson, A., Johansson, J., (2009). Assessing Response System Capabilities of Socio-Technical Systems, *The International Emergency Management Society* (TIEMS2009), Istanbul, Turkey, June 9-11.

In this paper, technical infrastructures are put in a socio-technical perspective. The focus is on method development for the analyses of actor capabilities for restoring critical infrastructure after strains, taking its standpoint from the theories of system thinking and resilience engineering. The method was applied in a preliminary study of the Swedish railway system. The objective for the empirical study was to assess the time required for response systems to restore technical infrastructures after varying types and magnitudes of strain. The concept of response curves was introduced in order to facilitate the analysis. It is argued that the proposed method is useful in the effort of identifying response system capabilities, and especially their capacity limits. The empirical analysis in the paper was rather limited, and should thus be viewed in the light of being a preliminary study to test the feasibility of the proposed method. However, it is argued that the method is useful in the effort of analysing socio-technical systems, especially when combined with the simulation based method for vulnerability analysis of technical infrastructures as presented in paper V.

Author's contributions: The author played a *major role* in method development and a *medium role* in the planning and preparation of the research, empirical data collecting, analysis and writing of the paper.

6.5 Paper V – Interdependent Infrastructures

Johansson, J., Hassel, H., Cedergren, A., (2010). Vulnerability Analysis of Interdependent Critical Infrastructure: Case study of the Swedish Railway System, *Submitted to International Journal of Critical Infrastructures.*[10]

The paper presents a modelling approach for interdependent technical infrastructures, in accordance with section 3.5, and uses three different methods for assessing structural vulnerability of the system, in accordance with section 4.3. The suggested approach was then applied for an empirical analysis of the railway system in southern Sweden. This system consists of seven interdependent subsystems, namely: train operation, railway track, traction power, signal, telecommunication, internal power, and external power. All of the systems were modelled with different structural and functional models. The functional models were either based on breadth first search algorithms or a train operation algorithm. The modelling approach enables the analysis of both functional and geographical dependencies. The mapping of the systems, i.e. describing the actual systems in terms of models, and gathering and compiling data about train operations turned out to be a bigger challenge than anticipated, although all the systems are owned and operated by the Swedish Railway Administration. It is concluded that the modelling approach is valid and appropriate for the analysis of large-scale interdependent technical infrastructures and that the three methods for structural vulnerability analysis gives complementing and valuable insights of the interdependent system's vulnerabilities.

Author's contributions: The author played a *major role* in the planning and preparation of the research, method development, computer program implementation and analysis, and a *medium role* in empirical data collecting and writing of the paper.

[10] Note that Hassel H. was formerly Jönsson H. and Cedergren A. was formerly Wilhelmsson A.

Chapter 7

Discussion

Most of the presented research has focused on method development. Three of the appended papers (I, II, V) are about structural vulnerability analysis of technical infrastructure, single as well as interdependent infrastructures. One paper (III) puts vulnerability analysis in the context of risk and vulnerability management and in relation with other regulatory frameworks for electrical distribution systems. One paper (IV) addresses an approach for a systematic assessment of response system capabilities for restoring technical infrastructures for large magnitudes of strain. This chapter discusses the presented methods, empirical studies, and the main results from the appended papers.

7.1 Methods and Modelling

Several different methods have been developed in the presented research. The origin of inspiration for the proposed methods in appended paper I, II and V was Network Theory. However, early in the research it was concluded that by only considering strictly topological features of technical infrastructures for vulnerability analysis was not enough, the fidelity and applicability of the results were not considered good enough. This lead to the expansion of the strictly network analytical approach with both inhomogeneous component descriptions and the incorporation of functional models of the studied systems. The separation of the system model into two parts, structural and functional models, enables the research to be used for several different technical infrastructures, not only those for which empirical studies were carried out. What changes is the description of the functional models, whereas the proposed structural vulnerability analysis methods remain the same. The separation of the system models also introduces a common interface for the modelling of interdependent infrastructures, namely the structural model for each of the modelled infrastructures.

In order to assess the structural vulnerability of technical infrastructures, three different approaches were introduces: global vulnerability analysis, critical component analysis, and geographical vulnerability. These three approaches are argued to give valuable and complementing information about the technical infrastructure's vulnerability. The aim for all of the methods is to give as comprehensive picture of the system's vulnerability as possible when exposed to strains of varying type and magnitudes of strains. This in turn leads into the delicate balance of abstractions versus fidelity of both the structural models and the functional models. A high level of abstraction makes it possible to cover large parts of the scenario space (i.e. finding all the vulnerabilities inherent in the systems) but where the result will suffer in detail and credibility. A high level of fidelity, on the other hand, will lead to results with more detail and a higher level of credibility but where only a small part of the scenario space can be covered. Where to strike the balance between abstraction and fidelity is ultimately dependent on the aim of the analysis, i.e. "there exists no free lunch". In the presented research the aim has been (1) to cover as much as possible of the scenario space, and at the same time (2) attain results with high enough level of detail and credibility so that they actually describes the studied system's vulnerability

Global vulnerability analysis gives valuable information regarding the vulnerability of the infrastructure for small up to very large magnitudes of strains. It also enables the study for what types of strain that the system is vulnerable to and enables the comparison of the vulnerability of different systems. The shortcoming of this type of analysis is that only a sample of the system's vulnerability is gained, and it is not possible draw conclusions regarding the system's vulnerability with certainty. Another shortcoming is that going from the applied strains to threats and hazards that could exploit these vulnerabilities is not straightforward.

Critical component analysis is an exhaustive search for those components or sets of components that give rise to large consequences if they fail. This exhaustive search has the benefit that conclusion regarding the vulnerability of the system, for the given failure set sizes, can be drawn with certainty. Identifying threats and hazards that correspond to the applied strains is also rather straightforward. The shortcoming of the method is that only a very small part of the scenario space can be evaluated. The goal of the presented analysis of critical components has been to go beyond the so called N-1 design criterion often used for the design of technical infrastructures. Critical component analysis gives rise to an extensive amount of scenarios to evaluate in order to draw conclusions regarding which components that are critical and for which magnitudes of strain they are critical. In appended paper II, the

concept of synergistic consequences was introduced and measures for ranking components based on this concept. There might however, be other types of importance measures and criticality ranking methods that could be used for the identification of what constitutes the most critical components in the system.

For geographical vulnerability analysis, the magnitude of strain depends on the cell size being used for the analysis. The analysis complements the two other proposed vulnerability analysis methods, since it identifies geographical areas or volumes where the spatial close co-location of components give rise to high consequences if they falter by geographically confined strains. The choice of the size of the cell can be tightly connected to the type of hazard or threat that could exploit the vulnerability. The shortcoming of this type of analysis is that the result is highly dependent of the type and size of the cell size, and how these are organized in a grid.

In appended paper I, a comparison of the global vulnerability for two different electricity distribution systems was made and measures for simplifying the comparison introduced. Analysing and comparing the vulnerability of systems, both regarding the same kind of systems and different types of systems, would give valuable insights of what makes a system vulnerable. This insight could in turn be used to improve the robustness and resilience of technical infrastructures.

As stated earlier, the aim for the proposed methods is to give as comprehensive picture of a system's vulnerability as possible. The research approach has been coloured with the overarching goal to enable a comprehensive and exploratory analysis of the vulnerability without having any preconceived ideas of the types and magnitudes of strains that may affect the system. Once it has been established for what scenarios the system is vulnerable, more in-depth analysis could be beneficial. The more in-depth analysis could be in one or several of the directions: (1) analysing the identified scenarios with more accurate and advanced "engineering models" in order to achieve results with higher fidelity, (2) analysing the societal consequences that arise given the scenario, (3) identifying threats and hazards that could exploit the scenario specific vulnerability, and (4) deriving mitigation strategies.

In appended paper III it was discussed how vulnerability analysis constitutes a part of a risk and vulnerability management scheme. The paper also put it into context with other regulatory frameworks, affecting the management of electrical distribution systems in Sweden. However, the paper did not clearly

explicate methods of how to combine vulnerability analysis and risk analysis in a unified approach. It is argued that complementing methods and perspectives are necessary in order to analyse and understand the complexities of technical infrastructures. As input in a risk and vulnerability management scheme of technical infrastructures both risk based methods, such as reliability methods and maintenance methods, as well as vulnerability based methods, such as those presented in the present research, should be used in order to achieve a holistic and transparent view of the complexities associated with technical infrastructures.

A method for the proactive assessment of response system capabilities of socio-technical infrastructures with respect to restoration times was presented in appended paper IV. The method is based on theories from both system thinking and resilience engineering. In the paper, a method for the identification of the response system as well as the concept of response curve was introduced. Response curve is a concept to quantitatively assess and compare response system capacities with the use of incidents and hypothetical scenarios. Response curves is argued to give valuable insights of the capacity of response systems, revealing for which magnitudes and types of strains the capacity is sufficient and for which it is insufficient. The aim is to evaluate the response system in a proactive manner, i.e. identifying possible deficiencies before incidents reveal them. The method was evaluated in a preliminary empirical study of the Swedish railway system. However, more studies are necessary in order to improve the suggested method and further evaluate its feasibility and applicability.

The modelling approach as presented in Chapter 3 enables the analysis of both structural and functional vulnerability analysis. In the presented research (appended paper I, II and V), the focus has been on the development of methods for structural vulnerability analysis. In order to comprehensively analyse the complexities associated with technical infrastructures regarding risks and vulnerabilities, methods for functional vulnerability analysis and how methods for structural vulnerability analysis can be incorporated with these should be addressed.

7.2 Empirical Studies

The over-arching goal of the presented research is to facilitate structural vulnerability analysis of technical infrastructures. The main focus has been on assessing the vulnerability of socio-technical infrastructures most fundamental part, namely the physical network. In order to evaluate the feasibility and applicability of the proposed methods, empirical studies have been carried out. Three different electrical distribution systems and the railway system in the southern part of Sweden have been analysed. A preliminary study of response system capabilities has also been carried out for the Swedish railway system.

Although several empirical studies have been carried out in the present thesis, it would be beneficial if the proposed models and methods would be further evaluated. This would more concretely address the validity and applicability of the proposed research methods. One such study would be to analyse a technical infrastructure with different level of detail of the functional model, for example analysing an electrical distribution system using (1) only topological properties (2) search algorithms with capacity constraints (3) load flow calculations. These types of studies would further clarify the tradeoffs involved in the balance between abstraction and fidelity. Another type of study could be to assess and compare the vulnerability of different types of technical infrastructures, using the proposed vulnerability methods. These types of studies would give valuable insights on how and why the vulnerability is different, and lead to normative input on the design of technical infrastructures.

A major issue when it comes to vulnerability analysis of technical infrastructures is attaining empirical data. This stems from both the extensive amount of data that needs to be collected and processed and confidentiality concerns about access to data regarding technical infrastructures. An issue only further enlarged when it comes to the study of interdependent technical infrastructures, as pointed out by several researchers (e.g. de Bruijne and van Eaten, 2007; Min et al., 2007; Kröger, 2008). In the presented research, there have been some obstacles concerning this issue. When it comes to the study of interdependent infrastructures, the Swedish Railway system was chosen. This choice was in part due to the fact that they both own and operate several different types of technical infrastructures, making access to data plausible. Still, to collect and process the data in or order to build the models of the studied technical infrastructures has been a major part of the research, and the time required constantly underestimated throughout the research process.

Chapter 8

Conclusions

In this last chapter, conclusions regarding the presented research are given. It starts with a short summary of methods and results, followed by an overview of the main results, and ends with suggestions for future research.

8.1 Summary of Thesis

In the thesis, definitions and general discussions of the concepts of vulnerability, risk, resilience, and their relationship was given. It was argued that, in contrast to risk, vulnerability is about taking a different point of view of the analysis. The vulnerability of a system is manifested through its inherent states. Finding these states and the corresponding consequences is the aim of a vulnerability analysis. Assessing the probability of threats and hazards, if possible, exploiting the identified vulnerabilities is argued to give a risk analysis. This could be done by complementing the vulnerability analysis with an exposure analysis.

To analyse the vulnerability of technical infrastructures in a proactive manner, a modelling approach of the system is necessary. It was argued for an approach of separating the structural and the functional properties of the modelled system. This approach has some beneficial aspects. Firstly, it separates the methods for the vulnerability analysis from the modelling approach. Secondly, it clarifies whether strains affect the structural or the functional part of the system. Thirdly, it offers an approach for modelling interdependent technical infrastructures.

In order to assess the structural vulnerability of technical infrastructures, three methods were presented: global vulnerability analysis, critical component analysis, and geographical vulnerability analysis. These methods all address the issue of finding the states of a system and assess the corresponding consequences, i.e. analysing the vulnerability. The requirement for the

method is that the system can be modelled as a network and that a functional model exists in order to estimate the consequences. As such, it was argued that most technical infrastructure can be modelled by the suggested approach and the methods for vulnerability analysis remain the same.

The use of vulnerability analysis as part of a risk and vulnerability management scheme was also addressed. An important part of technical infrastructure vulnerability is its ability to return to normal operation after being affected by strains, i.e. the resilience of the system. This requires a socio-technical view of technical infrastructures. A method for assessing response system capabilities through the concept of response curves was introduced. The method, among other things, enables the analysis of restoration times and response system capacity limits for technical infrastructures under various types and magnitudes of strains.

The empirical studies of the electrical distribution systems and the interdependent railway system, showed the applicability and feasibility of the proposed modelling approach and methods. The global vulnerability analyses showed how systems react to different types and magnitudes of strain. The analyses of critical components showed the methods applicability to systematically identify failure sets that give rise to large consequences. The geographical vulnerability analysis presented a way to assess the vulnerability of a system for geographically confined strains.

8.2 Main Research Contributions

The conducted research can give valuable guidance for the management of critical infrastructures for several actors. For private utility owners, the methods for vulnerability analysis of single technical infrastructures should be regarded as valuable. Taking account of the impact of dependencies should also be of major interest. Public actors, such as MSB, PTS (The Swedish Post and Telecom Agency), and Svenska Kraftnät (The Swedish TSO), have the overall responsibility of securing robust and resilient infrastructures and should benefit from the conducted research, since they provide services that the society heavily depends upon. The research is argued to give guidance towards understanding and analysing technical infrastructure vulnerabilities. When it comes to the analysis of interdependent technical infrastructures on a national level, which have fragmented ownership and no clear boundaries of responsibility exist, the feasible approach would be to utilize cooperative forums that already exist in Sweden. In order to analyse the vulnerabilities of interdependent technical infrastructures, several actors has to be involved and there have to be a certain level of agreement between the actors. The

proposed modelling approach, where models of individual infrastructures can be developed within different actors' area of responsibility and then merged into an interdependency model, is argued to be a feasible approach towards analysing the vulnerability of our society's interdependent critical infrastructures. On a regional or a municipal level, several actors should also benefit from the proposed research, e.g. when analysing the vulnerability of interdependent technical infrastructures in a city.

The main research contributions are in short:

- A modelling approach for both individual as well as interdependent technical infrastructures, enabling the analysis of both structural and functional vulnerability.

- Three structural vulnerability analysis methods, all giving different views of the technical infrastructures vulnerability: global vulnerability analysis, critical component analysis, and geographical vulnerability analysis.

- Several empirical analyses have been conducted, demonstrating the feasibility and applicability of the proposed modelling approach and the proposed methods for structural vulnerability analysis.

8.3 Future Research

As always when coming to the end of a research project, there exist several areas worthy of further research. Regardless in which of these research directions future research will be carried out, there still is plenty to be done in this highly interesting and very important area of proactive management of technical infrastructures. The author does not foresee that the demand for methods and tools in this area of research will be easily satisfied. The following list gives a brief overview of directions for future research.

- Methods for functional vulnerability analysis should be addressed. The proposed modelling approach of technical infrastructures could remain the same, while expanding the research in the direction of developing methods for the assessment of functional vulnerability of technical infrastructures. The combination of both structural and functional vulnerability analysis would most certainly be a fruitful approach to achieve a comprehensive view of the vulnerabilities inherent in our infrastructures.

- Complementing the vulnerability analysis with exposure analysis would make it easier to draw conclusion regarding strains, of different types and magnitude, probability of occurrence, thus providing complementing and valuable input to mitigation activities for reducing risks and vulnerabilities.

- The method for assessing response system capabilities was only used in a preliminary empirical study of the Swedish railway system. In order to further develop and validate the proposed method, further empirical studies would be beneficial.

- The use of vulnerability analysis as a complementary part to risk analysis should be further researched. It is argued that they give complementing views, and in order to draw conclusions that are more robust regarding their respective applicability, further research is necessary.

- The proposed modelling approach for interdependent technical infrastructures has only been used for one empirical study. Future research should address refinement of this approach and further empirical studies should be carried out in order to further validate the approach. The research field of vulnerability analysis of interdependent technical infrastructures is still at a rudimentary stage, and the need for modelling approaches and methods for this highly important area is believed, by the author, to accelerate.

- Comparative studies regarding the appropriate level of detail for functional models should be carried out. This would give guidance in the balance of fidelity versus abstraction in the efforts of conducting comprehensive vulnerability analyses.

- The societal consequences that arise when technical infrastructure services are disrupted were rather rudimentarily treated in the presented research. Further research is necessary in coupling the output of engineering models and the societal consequences that arise.

- A major issue regarding vulnerability analysis of technical infrastructures is the sheer amount of scenarios that has to be analysed. One approach is to reduce the scenario space for which the evaluation of consequences is necessary, as long as important information about the vulnerability of the system is not lost. Methods for limiting the search space, such as genetic algorithms, are therefore interesting.

- Using the proposed methods with respect to a changing system would open up for possibility to analyse the vulnerability of a system for longer time perspectives, hence following the vulnerability trajectory. How this should be specifically addressed is a subject for further research.

- The proposed methods can also be used to evaluate different optional system configurations in a planning or in a restructuring phase, for either new or existing systems. Further development of guiding measures and indicators readily describing the vulnerability of the system should thus be addressed.

References

Albert, R. and Barabási, A-L., (2002). Statistical mechanics of complex networks, *Review of Modern Physics*, Vol. 74, No. 1, pp. 47–97.

Albert, R., Albert, I. and Nakarado, G.L., (2004). Structural vulnerability of the North American power grid, *Phys. Rev. E*, Lett. 59, art. No. 025103.

Amaral, L.A.N., Ottino, J.M., (2004a). Complex networks – Augmenting the framework for the study of complex systems, *The European Physical Journal B*, Vol. 38, No. 2, pp. 147-162.

Amaral, L.A.N., Ottino, J.M., (2004b). Complex systems and networks: challenges and opportunities for chemical and biological engineers, *Chemical Engineering Sciences*, Vol. 59. No. 8-9, pp. 1653-1666.

Amin, M., (2004). Balancing market priorities with security issues, *Power and Energy Magazine IEEE*, Vol. 2, No. 4, pp. 30-38.

Apostolakis, G. E., Lemon, M., (2005). A Screening Methodology for the identification and Ranking of Infrastructure Vulnerabilities Due to Terrorism, *Risk Analysis*, Vol. 25, No. 2, pp. 361-376.

Appicharla, S. K., (2006). System for Investigation of Railway Interfaces, *Proceedings of 1st IET International Conference on System Safety*, London, U.K.

Aven, T., (2007). A Unified Framework for Risk and Vulnerability Analysis Covering both Safety and Security, *Reliability Engineering and System Safety*, Vol. 92, pp. 745-754.

Axelrod, R., Michael, D.C., (2000). *Harnessing Complexity: organizational implications of a scientific frontier*, Basic Books, 2000, New York, USA.

Balducelli, C., Bologna, S., Pietro, A., Vicoli, G., (2005). Analysing inter-dependencies of critical infrastructures using agent discrete event simulations, *Int. J. Emergency Management*, Vol. 2, No. 4, pp. 306-318.

Boin, A., McConnel, A., (2007). Preparing for Critical Infrastructure Breakdowns: The limits of Crisis Management and the Need for Resilience. *J. Contingencies and Crisis Management*, Vol. 15, No. 1, pp. 50-59.

Booker, G., Sprintson, A., Singh, C., Guikema, S., (2008). Efficient Availability Evaluation for Transport Backbone Networks, *Proceedings of 2008 International Conference on Optical Network Design and Modeling* (ONDM), pp, 1-6.

Box, G., (1976). Science and statistics, *Journal of the American Statistical Association*, Vol. 71, pp. 791-799.

Brown, T., Beyeler, W., Barto, D., (2004). Assessing infrastructure interdependencies: the challenge of risk analysis for complex adaptive systems, *Int. J. Critical Infrastructure*, Vol. 1, No. 1, pp. 108-117.

Buckle, P., Mars, G., Smale, S., (2000). New approaches to assessing vulnerability and resilience, *Australian Journal of Emergency Management*, Vol. 15, No. 2, pp. 8-14.

CCMD, (2003). *Crisis and Emergency Management: A Guide for Managers of the Public Service of Canada*, Canadian Centre for Management Development, Canada.

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,* Vol. 41, pp. 337-358.

Chassin, D.P. and Posse, C., (2005). Evaluating North American electric grid reliability using the Barabasi-Albert network model, *Physica A*, Vol. 355, No. 2-4, pp. 667-677.

Checkland, P. (2006). *Systems Thinking*, Systems Practice, John Wiley & Sons Ltd, Chichester, UK.

COM (Commission of the European Communities), (2006). *Directive of the council: on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection*, COM(2006) 787 final, Brussels.

Crondstedt, M., (2002). Prevention, preparedness, response, recovery – an outdated concept, *Australian Journal of Emergency Management*, Vol. 17, No. 2, pp. 10-13.

Crucitti, P., Latora, V., Marchiori, M., (2005a). Locating Critical Lines in High-Voltage Electrical Power Grids, *Fluctuation and Noise Letters*, Vol. 5, No. 2, pp. 201-208.

Crucitti, P., Latora, V., Porta, S., (2005b). Centrality Measures in Spatial Networks of Urban Streets, *Phys. Rev. E*, Lett. 73, art. No. 036125.

Crucitti, P., Latora, V., Marchiori, M., Rapisarda, A., (2004a). Error and attack tolerance of complex networks, *Physica A: Statistical Mechanics and its Applications*, Vol. 340, No. 1-3, pp. 388-394.

Crucitti, P., Latora, V., Marchiori, M., (2004b). A topological analysis of the Italian electric power grid, *Physica A: Statistical Mechanics and its Applications*, Vol. 338, No. 1-2, pp. 92-97.

Crucitti, P., Latora, V., Marchiori, M., Rapisarda, A., (2003a). Efficiency of scale-free networks: error and attack tolerance, *Physica A: Statistical Mechanics and its Applications*, Vol. 320, pp. 622-642.

Crucitti, P., Latora, V., Marchiori, M., (2003b). A model for cascading failures in complex networks, *Phys. Rev. E*, Lett. 69, art. No. 045104.

de Bruijne, M., van Eeten, M., (2007). Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment. *Journal of Contingencies and Crises Management*, Vol. 15, No. 1, pp. 18-29.

Demšar, U., Špatenková, O., Virrantaus, K., (2008). Identifying Critical Locations in a Spatial Network with Graph Theory, *Transactions in GIS*, Vol. 12, No. 2, pp. 91-82.

Dilley, M., Boudreau, T., (2001). Coming to terms with vulnerability: a critique of the food security definition, *Food Policy*, Vol. 26, No. 3, pp. 229-247.

Einarsson, S., Rausand, M., (1998). An approach to vulnerability analysis of complex industrial systems, *Risk analysis*, Vol. 15, No. 5, pp. 535-546.

Eusgeld, I., Henzi, D., Kröger, W., (2008). *Comparative Evaluation of Modeling and Simulation Techniques for Interdependent Critical Infrastructures: Scientific Report*, Laboratory for Safety Analysis, Institute for Energy Technology, ETH Zûrich.

Eusgeld, I., Kröger, W., Sansavini, G., Schläpfer, M., Zio, E., (2009). The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures, *Reliability Engineering & System Safety*, Vol. 94, pp. 954-963.

Executive Order, (1996). 13010-Critical Infrastructure Protection, *Federal Register*, Vol. 61, No. 138, pp. 37347-37350.

FEMA, (1997). *Multi Hazard – Identification and Risk Assessment – A Cornerstone of the National Mitigation Strategy*, Federal Emergency Management Agency, USA.

Fischer, G., Molin, S., (2001). *Isstormen i Kanada (The Ice-storm in Canada),* FOI Total Försvarets forskningsinstitut, ISSN 1650-1942, in Swedish

Forrester, J., (1971). *Principles of systems: text and workbook: chapters 1 through 10 by Jay W. Forrester*, Wright-Allen Press Inc., Cambridge, Massechusetts, 2nd preliminary edition, Fifth printing, October 1971, Ch. 3, pp. 4.

Gao, H-S., Guo, J., (2009). Application of Vulnerability Analysis in Electric Power Communication Network, *Proceedings of the Eight International Conference on Machine Learning and Cybernetics*, Baoding, China.

Glover, J. D., Sarma, M., (1994). *Power System Analysis and Design*, PWA Publishing Company, 1994, Boston, USA.

Grubesic, T.H., Matisziw, T.C., Murray, A.T., Snediker, D., (2008). Comparative Approaches for Assessing Network Vulnerability, International Regional Science Review, Vol. 31, No. 1, pp. 88-123.

Gursesli, O., Desrochers, A.A., (2003). Modeling infrastructure interdependencies using Petri nets, *IEEE International conference on Systems, Man, and Cybernetics*, Vol. 2, pp. 1506-1512.

Haimes YY, Jiang P., (2001). Leontief-Based Model of Risk in Complex Interconnected Infrastructures, *Journal of Infrastructure Systems*, Vol. 7, No. 1, pp. 1-12.

Haimes, Y.Y., Longstaff, T., (2002). The Role of Risk Analysis in the Protection of Critical Infrastructures Against Terrorism, *Risk Analysis*, Vol. 22, No. 3, pp. 439-444.

Haimes, Y.Y., (2006). On the Definition of Vulnerabilities in Measuring Risks to Infrastructures, *Risk Analysis*, Vol. 26, No. 2, pp. 293-296.

Haimes, Y.Y., (2009a). On the Definition of Resilience in Systems, *Risk Analysis*, Vol. 29, No. 4, pp. 498-501.

Haimes, Y.Y., (2009b). On the Complex Definition of Risk: A System-Based Approach, *Risk Analysis*, Vol. 29, No. 12, pp. 1647-1653.

Hansson S.O., Helgesson, G., (2003). What is stability?, *Synthese*, Vol. 136, No. 2, pp. 219-235.

Hansson, S. O. (2005), The Epistemology of Technological Risk, *Techné: Research in Philosophy and Technology*, Vol. 9, No. 2, pp. 68-80.

Hollnagel, E., Woods, D.D., Leveson, N., (Eds.), (2006). *Resilience Engineering: Concepts and precepts*, Ashgate Publishing Limited, Aldershot, UK.

Holme, P., (2004). *Form and function of complex networks*, Licentiate thesis, Department of Physics, Umeå University, Umeå, Sweden.

Holmgren, Å., (2004). *Vulnerability Analysis of Electrical Power Delivery Networks*, Licentiate thesis, Department of Transport and Economics, Royal Institute of Technology, Stockholm, Sweden.

Holmgren, Å., (2006). *Quantitative Vulnerability Analysis of Electric Power Networks*, Doctoral thesis, Department of Transport and Economics, Royal Institute of Technology, Stockholm, Sweden.

Houck, D.J., Kim, E., O'Reilly, G.P., Picklesimer, D.D., Uzunalioglu, H., (2004). A network survivability model for critical national infrastructures. *Bell Labs Technical Journal*, Vol. 8, No. 4: pp. 153–172.

Jenelius, E., (2007). *Approaches to Road Network Vulnerability Analysis*, Licentiate Thesis, Department of Transport and Economics, Royal Institute of Technology, Stockholm, Sweden.

Jenelius E, Mattsson, L-G., (2008). The vulnerability of road networks under area-covering disruptions, *Proceedings of INFORMS Annual Meeting*, Washington D.C.

Johansson, J., Hassel, H., (2010). An Approach for Modelling Interdependent Infrastructures in the Context of Vulnerability Analysis, *Reliability Engineering and System Safety.* (Submitted)

Johansson, J., Hassel (former Jönsson), H., (2008). A Model for Vulnerability Analysis of Interdependent Infrastructure Networks, *Proceedings from the joint Annual Conference of European Safety and Reliability Association and Society for Risk Analysis (ESREL2008 & 17th SRA-Europe Conference)*, Valencia, Spain.

Johansson, J., (2007). Risk *and Vulnerability Management of Large-Scale Technical Infrastructures: Electrical Distribution Systems*, Licentiate Thesis, Department of Industrial Electrical Engineering and Automation, Lund Institute of Technology, Lund University, Media-Tryck Lund University, Lund, Sweden.

Johansson, J., Lindahl, S., Samuelsson, O., Ottosson, H., (2006). The Storm Gudrun a Seven-Weeks Power Outage in Sweden, *Proceedings of Third International Conference on Critical Infrastructures* (CRIS2006), Alexandria, VA, USA.

Kaplan, S., Garrick, B.J., (1981). On the quantitative definition of risk, *Risk Analysis*, Vol. 1, No. 1, pp. 11-27.

Kaplan, S., Haimes, Y.Y., Garrick, B.J., (2001). Fitting Hierarchical Holographic Modeling into the Theory of Scenario Structuring and a Resulting Refinement to the Quantitative Definition of Risk, *Risk Analysis*, Vol. 21, No. 5, pp. 807-819.

KBM, (2005). *Hot- och Riskrapport 2005,* KBM:s Temaserie 2005:11, Edita, Västerås, Sweden.

Kelly, C., (1999). Simplifying disasters: developing a model for complex non-linear events, *Australian Journal of Emergency Management*, Vol. 14, No.1, pp 25-27.

Kinney, R., Crucitti, P., Albert, R., Latora, V., (2005). Modeling cascading failures in the North American power grid, *The European Physical Journal B (EPJ B)*, Vol. 46, No. 1, pp. 101-107.

Kröger, W. (2008). Critical infrastructures at risk: A need for a new conceptual approach and extended analytical tools, *Reliability Engineering & System Safety*, Vol. 93, pp. 1781-1787.

Laprie J.C., Kanoun, K., Kaäniche, M., (2007). Modelling Interdependencies Between the Electricity and Information Infrastructures, *Lecture Notes in Computer Science*, Vol. 4680, pp. 54-67.

Larsson, S., Ek, E., (2004). The blackout in Southern Sweden and Eastern Denmark, September 23, 2003, *Power Engineering Society General Meeting*, IEEE, Vol. 2, pp. 1668-1672.

Latora, V. Marchiori, M., (2001). Efficient behavior of small-world networks, *Phyical Review E*, Lett. 87, art. No. 198701.

Latora, V., Marchiori, M., (2005). Vulnerability and protection of infrastructure networks, *Physical Review E*, Lett. *71*, art. No. 015103.

Little, R.G., (2002). Controlling Cascading Failure: Understanding the Vulnerabilities of Interconnected Infrastructures, *Journal of Urban Technology*, Vol. 9, No. 1, pp. 109-123.

Little, R.G., (2004). *A socio-technical systems approach to understanding and enhancing the reliability of interdependent infrastructure systems*, International Journal of Emergency Management, Vol. 2, No. 1-2, pp. 98-110.

Little, R.G., (2005). Organizational Culture and the Performance of Critical Infrastructure: Modeling and Simulation in Socio-Technological Systems, *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, pp. 1-8, Hawaii, USA.

McCarthy, J.A., Brashear, J.P., Pommerening, C., Siegel, J.L., Creel, J.T., Ryan, T.P., Stafford, B., and Clark, L.C., (2005). *Critical Infrastructure Protection in the National Capital Region – Risk-Based Foundations for Resilience and Sustainability, Final Report*, Arlington, VA: George Mason University.

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*, Vol. 1, No. 3, pp. 298-308.

McDaniels T, Chang S, Peterson K, Mikawoz J, Reed D., (2007). Empirical Framework for Characterizing Infrastructure Failure Interdependencies, *Journal of Infrastructure Systems,* Vol. 13, No. 3, pp. 175-184.

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*, Vol. 18, No. 2, pp. 310-318.

Mili, L., Qiu, Q., Phadke, A.G., (2004). Risk assessment of catastrophic failures in power systems, *Int. J. Critical Infrastructures*, Vol. 1, No. 1, pp 38-63.

Min, H.J., Beyler, W., Brown, T., Son, Y., Jones A.T., (2007). Towards modeling and simulation of critical national infrastructure interdependencies. *IIE Transactions*, Vol. 39, pp. 57-71.

Murray, A.T., Matisziw, T.C., Grubesic, T.H., (2007). Critical Network Infrastructure Analysis: Interdiction and System Flow, *Journal of Geographical Systems*. Vol. 9, pp. 103–117.

Murray, A.T., Matisziw, T.C., Grubesic, T.H., (2008). A Methodological Overview of Network Vulnerability Analysis, *Growth and Change*, Vol. 39, No. 4, pp. 573-592.

Nedic, DP; Dobson, I; Kirschen, DS; Carreras, BA; Lynch, VE., (2006). Criticality in a cascading failure blackout model, *Electrical Power and Energy Systems*, Vol. 28, pp. 627-633.

Newman, M.E., (2003) The structure and function of complex networks, *SIAM Review*, Vol. 45, No. 2, pp.167–256.

Newlove, L.M., Stern, E.K., Svedin, L., (2000). *Auckland Unplugged*, Copy Print, 2000, Stockholm, Sweden.

Ottino, J. M., (2004). Engineering complex systems, *Nature*, Vol. 427, No. 6973, p. 399.

Patterson, S.A., Apostolakis, G.E., (2007). Identification of critical locations across multiple infrastructures for terrorist actions, *Reliability Engineering and System Safety*, Vol. 92, pp. 1183-1203.

Peerenboom, J.P., Fisher, R.E., (2007). Analyzing Cross-Sector Interdependencies, in *Proceedings of the 40th Hawaii International Conference on System Sciences (HICSS' 07)*, Hawaii, USA:

Pedersen P, Dudenhoeffer D, Hartley S, Permann M., (2006). *Critical Infrastructure Interdependency Modeling: A Survey of U.S. and International Research*. Idaho National Laboratory.

Porta, S., Crucitti, P., Latora, V., (2006). The network analysis of urban streets: A dual approach, *Physica A: Statistical Mechanics and its Applications*, 2006, Vol. 369, No. 2, pp. 853-866.

Porta, S., Crucitti, P., Latora, V., (2005). The Network Analysis of Urban Streets: A Primal Approach, *arXiv:physics/0506009v1*, pp. 1-19.

Rahman, H.A., Beznosov, K., Martí, J.R., (2009). Identification of Sources of Failures and their Propagation in Critical Infrastructures from 12 years of Public Failure Reports, *Int. J. Critical Infrastructures,* Vol. 5, No. 3, pp. 220-244.

Restrepo, C.E., Simonoff, J.S., Zimmerman, R., (2006). Unravelling Geographic Interdependencies in Electric Power Infrastructure, *Proceedings of the 39th Hawaii International Conference on System Sciences (HICSS' 06)*, Hawaii, USA.

Rinaldi, S.M., (2004). Modeling and Simulating Critical Infrastructures and Their Interdependencies, *Proceedings of the 37th International Conference on System Sciences (HICSS' 04)*, Hawaii, USA.

Rinaldi, S.M., Peerenboom, J.P., Kelly, T.K., (2001). Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies, *IEEE Control Systems Magazine*, Vol. 21, No. 6, pp. 11-25.

Robert, B., (2004). A method for the study of cascading effects within lifeline networks, *Int. J. Critical Infrastructures*, Vol. 1, No. 1, pp 86-99.

Robert, B., Morabito, L., (2010). An approach to identifying geographic interdependencies among critical infrastructures, *Int. J. Critical Infrastructures*, Vol. 6, No. 1, pp. 17-30.

Sansavini, G., Hajj, M.R., Puri, I., K., Zio, E., (2009). A deterministic representation of cascade spreading in complex networks, *Europhysics Letters*, Vol. 87, No. 1, pp. 48004p1-p2.

Senge, P. M., (1994). *The Fifth Discipline: The Art & Practice of The learning Organization*, Doubleday, New York, USA.

Strogatz, S., (2001). Exploring Complex Networks, *Nature*, Vol. 410, pp. 268-276.

Sun, K., (2005). Complex Networks Theory: A New Method of Research in Power Grid, *Proceedings of IEEE/PES Transmission and Distribution Conference & Exhibition: Asia and Pacific,* Dalian, China.

Thissen, W.A., Herder, P.PM, Critical Infrastructures: Challenges for Systems Engineering, Proceedings of IEEE International Conference on Systems, Man and Cybernetics, Vol. 2, pp. 2042-2047.

Tolone, W.J., Wilson, D., Raja, A., Xiang, W., Hao, H., Phelps, S., Johnson E.W., (2004). Critical Infrastructure Integration Modeling and Simulation, *Intelligence and Security Informatics*, Vol. 3073, pp. 214-225.

UCTE (Union for the Coordination of Transmission of Electricity), (2006). *Final Report: System Disturbance on 4 November 2006*, Boulevard Saint-Michael 15, B-1040 Brussels, Belgium.

Uhr, C., (2009). *Multi-organizational Emergency Response Management: A Framework for Further Development*, Doctoral Thesis, Department of Fire Safety Engineering and Systems Safety, Faculty of Engineering, Lund University, Lund, Sweden.

Verwater-Lukszo, Z., and Bouwmans, I., (2005). Intelligent Complexity in Networked Infrastructures, *Proceedings of IEEE International Conference on Systems, Man and Cybernetics*, pp. 2378-2383.

Watts, D. J., Strogatz, S. H., (1998). Collective dynamics of 'small-world' networks, *Nature*, Vol. 393, pp. 440−442.

Watts, D.J., (2004). *Six Degrees – The Science of a Connected Age*, Vintage, London, United Kingdom.

Weichselgartner, J., (2001). Disaster mitigation: the concept of vulnerability revisited, *Disaster Prevention and Management*, Vol 10, No. 2, pp. 85-94.

Winkler, R.L., (1996). Uncertainty in probabilistic risk assessment, *Reliability Engineering and System Safety*, Vol. 54, pp. 127-132.

Wisner, B., (2001). *Notes on Social Vulnerability: Categories, Situations, Capabilities, and Circumstances*, Environmental Studies Program, Oberlin College: 4.

Xiao, N., Sharman, N., Raj, R., Upadhyaya, S., (2008). Infrastructure Interdependencies Modeling and Analysis - A Review and Synthesis, *Proceedings of Americas Conference on Information Systems (AMCIS)*, Toronto, Canada.

Zimmerman, R., (2001). Social Implications of Infrastructure Network Interactions, *Journal of Urban Technology*, Vol. 8, No. 3, pp. 97-119.

Zimmerman, R., Restrepo, C.E., (2006). The next step: quantifying infrastructure interdependencis to improve security, *Int. J. Critical Infrastructure*, Vol. 2, No. 2/3, pp. 215-230.

Zio, E., (2007). From Complexity Science to Reliability Efficiency: an New Way of Looking at Complex Network Systems and Critical Infrastructures, *International Journal of Critical Infrastructures*, Vol. 3, No. 3-4, pp 488-508.

Zio, E., Sansavini G., (2007). Service Reliability Analysis of Tramway Network, *Proceedings of ESREL2007 Risk, Reliability and Societal Safety*, Stavanger, Norway.

Zio E, Sansavini G., Maja, R., Marchionni, G., (2008). An analytical approach to the safety of road networks. *International Journal of Reliability, Quality & Safety Engineering,* Vol. 15, No. 1, pp. 67–77.

Zio, E., (2009). Reliability Engineering: Old Problems and New Challenges, *Reliability Engineering and System Safety*, Vol. 94, pp. 125-141.

Appended Papers

I	Johansson, J., Jönsson, H., Johansson, H., (2007). Analysing the Vulnerability of Electric Distribution Systems: A Step Towards Incorporating the Societal Consequences of Disruptions, *International Journal of Emergency Management*, Vol. 4, No. 1, pp.4–17.
II	Jönsson, H., Johansson, J., Johansson, H., (2008). Identifying Critical Components in Technical Infrastructure Networks, *Journal of Risk and Reliability*, Vol. 222, Part O, pp. 235-243.
III	Johansson, J., Svensson, S., (2008). Risk and Vulnerability Management of Electrical Distribution Grids, *Nordic Distribution and Asset Management Conference* (NORDAC 2008), Bergen, Norway, September 8-9.
IV	Wilhelmsson, A., Johansson, J., (2009). Assessing Response System Capabilities of Socio-Technical Systems, *The International Emergency Management Society* (TIEMS2009), Istanbul, Turkey, June 9-11.
V	Johansson, J., Hassel, H., Cedergren, A., (2010). Vulnerability Analysis of Interdependent Critical Infrastructure: Case study of the Swedish Railway System, Submitted to *International Journal of Critical Infrastructures*.

I

Analysing the vulnerability of electric distribution systems: a step towards incorporating the societal consequences of disruptions

Jonas Johansson*, Henrik Jönsson and Henrik Johansson

Lund University Centre for Risk Analysis and Management (LUCRAM)
Lund University
P.O. Box 118, SE-221 00 Lund, Sweden
E-mail: jonas.johansson@iea.lth.se
E-mail: henrik.jonsson@brand.lth.se
E-mail: henrik.johansson@brand.lth.se
*Corresponding author

Abstract: Reliable electrical power supply is a prerequisite for the modern society, and if it fails, it can cause severe consequences in terms of economic losses and even fatalities. It is thus important to analyse the vulnerability of the electric power system. Network analysis has previously been used to analyse the vulnerability of electric transmission systems. Recent events in Sweden, however, have shown that perturbations in distribution systems can also cause severe societal consequences. Thus, we argue that vulnerability analysis at the distribution level is equally important. Furthermore, previous work has focused on the technical aspects of the system, and in this paper we take a step towards incorporating the societal aspects of vulnerability by suggesting new network analytic measures. We analyse the distribution systems in two Swedish municipalities using the proposed measures. We conclude that the proposed measures can increase the value of using network analysis when analysing societal vulnerability to perturbations in electric distribution systems and that such analysis also can be useful in emergency mitigation and preparedness planning.

Keywords: societal vulnerability; network analysis; power system; infrastructures.

Reference to this paper should be made as follows: Johansson, J., Jönsson, H. and Johansson, H. (2007) 'Analysing the vulnerability of electric distribution systems: a step towards incorporating the societal consequences of disruptions', *Int. J. Emergency Management*, Vol. 4, No. 1, pp.4–17.

Biographical notes: Jonas Johansson is a PhD student at the Department of Industrial and Electrical Engineering of Lund University and has an MSc in Electrical Engineering. His main research area is interdependencies among large-scale infrastructures.

Henrik Jönsson is a PhD student at the Department of Fire Safety Engineering of Lund University and has an MSc in Risk Management and Safety Engineering and a BSc in Fire Safety Engineering. His main research area is risk and vulnerability analysis of complex systems.

Henrik Johansson is an Assistant Professor at the Department of Fire Safety Engineering of Lund University and has a PhD in Fire Safety Engineering and an MSc in Civil Engineering. His main research areas are vulnerability analysis of social and technical systems and decision analysis concerning investments in risk-reducing measures.

1 Introduction

Our society is heavily dependent on a number of technical infrastructures, and the tolerance for disruptions in the services provided by them is low. The electric power system is one of the most critical technical infrastructures. Electrical power outages often have paralysing effects on the society, causing large economic damage and can lead to injuries and fatalities. Power outages also render many other infrastructures incapable of functioning, thus causing secondary effects. In addition, the effectiveness of emergency response operations might be severely reduced because of power outages. In order to facilitate proactive vulnerability-reducing actions, both in terms of mitigation and preparedness planning, it is of utmost importance that methods for analysing the societal vulnerability to perturbations in electric power systems are available.

The emerging discipline of network analysis (Watts, 2004; Albert and Barabási, 2002; Barabási, 2002; Newman, 2003) has previously been used to study the vulnerability of complex networks (Albert *et al*., 2000; Holme *et al*., 2002; Albert *et al*., 2004; Crucitti *et al*., 2004a–c; Apostolakis and Lemon, 2005; Chassin and Posse, 2005; Kinney *et al*., 2005; Crucitti *et al*., 2003; Gorman *et al*., 2004). The methods can roughly be described as being based on different strategies for removing edges or nodes from the network, and at the same time measuring some property of the network. The measures are usually based on some kind of global property, characterising the performance of the network, *e.g.*, the average inverse geodesic length (Holme *et al*., 2002), global efficiency of the network (Crucitti *et al*., 2003; 2004c), the size of the largest connected subgraph (Albert *et al*., 2000; Holme *et al*., 2002), diameter of the network (Albert *et al*., 2000; Gorman *et al*., 2004) and connectivity loss (Albert *et al*., 2004). A significant portion of these methods has been used to analyse the vulnerability of electric power grids. In these studies, the power grid is modelled as a network, where the electrical properties are neglected. Instead, the topology of the grid is studied from either a static (*e.g.*, Albert *et al*., 2000; Crucitti *et al*., 2004c) or a dynamic perspective (*e.g.*, Crucitti *et al*., 2004a; Kinney *et al*., 2005) with the main difference being that the latter allows for a redistribution of flows in the network, which might capture cascading failures. Previous analyses have focused mainly on the transmission level but not on the distribution level of the electric power grid. An electric distribution system is, to some extent, built meshed but is radially operated. This structural property enables rerouting of the electric power through the altering of switches in case of perturbations. However, while making the system more redundant and robust, it also makes the structure more complex and harder to analyse. Recent events, for example, the storm Gudrun, which struck southern Sweden on 8 January 2005, have indicated that damage to the distribution level can cause severe societal consequences.[1] Therefore, we propose that network-based vulnerability analysis of power grids should be employed not only when analysing transmission and subtransmission grids, but also when analysing distribution grids.

Existing network analytic methods focus mainly on the technical aspects of the electric system, *i.e.*, the system's ability to withstand perturbations and recover from damages. We agree with the view proposed by Little (2002), who claims that: "although it may be the hardware … that is the initial focus of the discussions of infrastructure, it is actually the services that these systems provide that are of real value to the public". Therefore, what is of interest is not how vulnerable the electric power system is by itself, but how vulnerable the *society* is to perturbations in the electric system. A similar concern has also been put forward by Holmgren (2006). The applicability of existing network analytic methods must therefore be evaluated with respect to how valid their results are in terms of *societal vulnerability* to perturbations in the electric distribution system. We argue that many existing methods do not provide such valid measures. Therefore, the primary objective of this work is to propose new methods and measures for analysing the societal vulnerability to perturbations in electric distribution systems. The methods are aimed at facilitating both mitigation and preparedness planning. In addition, we present empirical results from analyses of the electric distribution systems in two municipalities in Sweden using the proposed methods and measures. Furthermore, we compare the results with analyses performed using previously suggested measures, such as connectivity loss. We then discuss the results, along with the applicability and limitations of the proposed methods. Finally, some suggestions for future research are given.

2 The concept of vulnerability

Even though the concept of vulnerability is used extensively in the research literature, its meaning remains ambiguous (Weichelsgartner, 2001; Buckle, 2000). Different researchers and research traditions use it differently and therefore we believe that it is important to give a formal definition of the concept. In this paper, we define vulnerability as the degree of loss or damage to the system when exposed to a perturbation of a given type and magnitude. This definition has similarities to the definition proposed by Buckle (2000) and also corresponds to how the concept is operationalised in network analysis, where networks are perturbed by attack strategies of given types and magnitudes. If the network performance is highly degraded, *e.g.*, there is a high degree of loss caused by small magnitudes of the perturbation, it is considered to be vulnerable. Closely related concepts are robustness and resilience, which taken together can be seen as the antonym of vulnerability. Robustness is a static property – ability to withstand a strain, while resilience is a dynamic property – ability to adapt and recover from changes and damages (Einarsson and Rausand, 1998).

3 Performance measures in electric power networks

In order to analyse and evaluate the vulnerability of an electric power network, a valid measure reflecting the network performance[2] has to be available. Several measures of network performance have previously been suggested, but measures developed to capture important aspects of a certain complex network are not always applicable for analysing other types of networks or when the aim of the analysis is different. It is thus crucial to investigate whether these measures are valid for analysing societal vulnerability of electric distribution systems.

3.1 Existing performance measures applied to the electric distribution system

In an electric distribution network, the nodes are highly heterogeneous, *e.g.*, have different functions; some nodes feed the electricity into the system, some directly supply customers, while others act only as transmission or branching nodes (*i.e.*, nodes where no electrical power is produced or consumed). Most of the performance measures, mentioned above, more or less assume homogenous nodes, *e.g.*, the average inverse geodesic length, the diameter and the size of the largest connected subgraph. These measures do not account for which type of node loses contact with the network. In reality, though, the performance is highly dependent on which type of node loses contact; if an in-feed node loses contact with the network, no electricity is fed into the network (assuming there is only one in-feed node), thus no customers have power supply. On the other hand, if a supply node loses contact, only the customers connected to it are affected. Therefore, performance measures that do not distinguish between different types of nodes are not well suited for analysing societal vulnerability to perturbations in the electric distribution systems and are not considered further in this paper.

Connectivity Loss (CL), proposed by Albert *et al*. (2004), distinguishes among three types of nodes at the transmission level of the power system: generators, transmission nodes and distribution substations. The calculation of CL involves determining how many generators each distribution substation is connected to. When the network is exposed to perturbations, the distribution substations start losing connections to the generators. CL is defined as the proportion of lost connections between distribution substations and generators, averaged for all distribution substations. Albert *et al*. (2004) explains the measure as: "the ability of distribution substations to receive power from the generators". This measure is clearly more applicable for analysing the electric distribution system than the previously mentioned measures, given that in-feed points and generators are treated synonymously. However, if the purpose is to use it for analysing the societal vulnerability to perturbations in electric distribution systems, it has clear shortcomings. CL assumes that each distribution substation without power supply gives rise to the same negative consequences. In reality, though, the consequences will depend on a number of factors, such as the number of customers connected to the substation, the amount of lost power, and whether vulnerable customers are affected. Measures utilised for analysing the societal vulnerability of electric systems must address this issue.

Another shortcoming of CL is the vague interpretation of the measure. Assume, for example, that a network has a CL of 50%, which would imply that only half of all initial paths between generators or in-feed points and distribution substations are unperturbed. It is not clear what this implies in terms of negative consequences to the society. Are there, for example, any substations completely without connections to generators or in-feed points and thus without power supply? In fact, it is possible that all substations have power supply, since it is often sufficient for a substation to be connected to only one generator or in-feed point in order to have power supply. Therefore, it is difficult to relate CL to societal vulnerability.

3.2 Proposition of a new performance measure

We propose a new performance measure called Customer Equivalent Connection Loss (CECL), which is quite similar to CL. CECL is defined as the ratio of the sum of *customer equivalents* (CE) that have lost connection to *all* in-feed points (CE_{loss}) and the

total sum of customer equivalents (CE_{tot}) (see Equation 1). The CE is a weighted quantity aiming at capturing the societal consequences that arise because of the loss of the service provided by the infrastructure, *e.g.*, a hospital can be given a higher CE than a household.

$$\mathrm{CECL} = \frac{\mathrm{CE}_{\mathrm{loss}}}{\mathrm{CE}_{\mathrm{tot}}} . \tag{1}$$

Here, the assumption is that as long as there is a path between a distribution substation and *any* generator or in-feed point, it has power supply. CECL can thus be described as measuring an idealised case, since it measures the fraction of CE that undoubtedly has lost power supply (since there is no physical connection to any in-feed points). In practice, though, it might not suffice for a substation to have a connection to an in-feed point, in order to receive power, *e.g.*, since power lines and transformers have capacity limits. By focusing on the societal consequences instead of the technical components of the system (*e.g.*, the distribution substations), we argue that CECL provides a more valid measure of the societal vulnerability to perturbations in the power grids. In addition, CECL can provide an indication of the extent of the emergency needs arising from perturbations in the electric distribution system. Therefore, it is more useful for emergency management than the measures previously employed.

4 Proposition of two network analytic measures

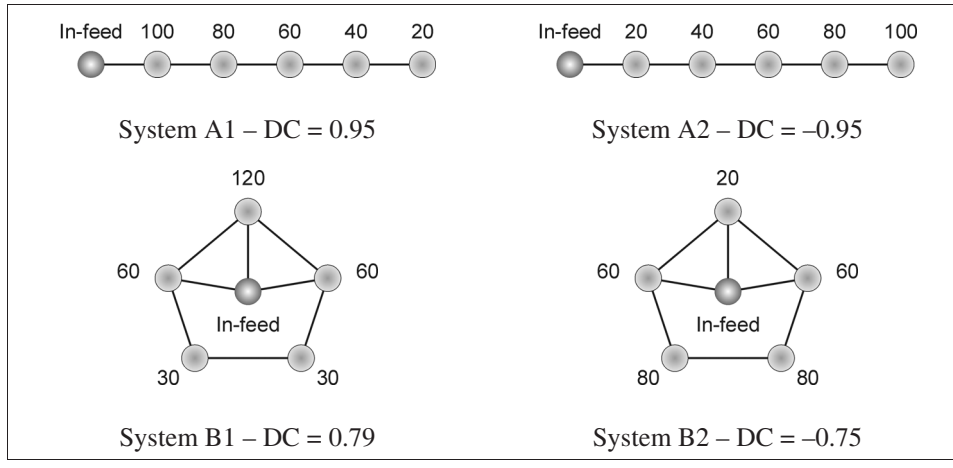
The result usually obtained from network-based vulnerability analyses is a plot of the performance measure as a function of the fraction of nodes or edges that have been removed. By studying this plot, conclusions regarding the vulnerability can be drawn, for example by comparing different systems. However, comparing such plots for different networks, and drawing conclusions from them, can be difficult tasks. Therefore, we suggest that such plots be complemented by a measure called the Societal Vulnerability Coefficient (SVC), which is a single measure expressed as a number between zero and one. This measure is simply the area beneath the curve shaped by the CECL as a function of the fraction of nodes or edges that have been removed. A vulnerable system, where the CECL swiftly rises to unity, has an SVC close to one. A robust system, on the other hand, is better at maintaining its function while perturbed, and therefore has an SVC closer to zero.

In addition to SVC, we propose a measure called Design Coefficient (DC). This measure is the correlation between the order in which a particular substation loses its connections to *all* generators and in-feed points when the network is perturbed, and the number of customers connected to that particular substation. The DC shows, in a wider sense, whether the system is designed to provide a more reliable power supply to important nodes, *e.g.*, nodes with many customers, relative to less important ones. Important substations should be the last ones to lose power when the network is perturbed, which is implied by a positive DC. Conversely, a negative DC indicates that the substations supplying many customers lose power early when the network is perturbed. The concept of DC is illustrated in Figure 1. It is important to note that this measure only focuses on the order in which substations lose power, not whether a large or a small fraction of nodes or edges have to be removed before the network starts deteriorating. Therefore, an extremely meshed and redundant system might have a lower

DC than an entirely radial system. The fraction of nodes/edges that has been removed when a particular substation, s_i, has lost its connections to *all* in-feed points is denoted as f_i. Since the order in which the different substations lose connection might differ between simulations (the strategies for removing edges/nodes might be random), one needs to consider the mean fraction of removed nodes/edges $\overline{f}_i$. Furthermore, the Customer Equivalent of a specific substation is denoted by CE_i. Then the DC is defined as the Pearson's correlation coefficient between $\overline{f}_i$ and CE_i for all substations where $CE_i > 0$ (Equation 2).

$$DC = r(\overline{f}_i, CE_i) \,. \tag{2}$$

Figure 1 Example of DC values for four different systems*



Notes: * The figure above each node denotes the number of customers connected to that node. The values are based on 1000 simulations with random node removal strategy. The only difference between System A1 and A2, and B1 and B2 is relocation of the customers, but it still makes DC go from a high positive value to a high negative value. Note that the DC value does not describe the overall robustness of the system; instead, it is a measure of how well the system topology is designed to correspond to how the customers are distributed in the network. This is apparent when comparing Systems A and B.

5 Empirical vulnerability analysis of two electrical distribution systems

The electric distribution systems, analysed in this paper, are located in two Swedish municipalities, both with a population of approximately 30 000. From here on, the two distribution systems are called System A and System B. The distribution systems consists of 10 and 20 kV substations, and all connections to higher voltages (50 kV or more) are defined as in-feed points. In this analysis, the CE for each substation is defined as the number of customers connected to it, *i.e.*, each customer is given a weight equal to one. The connected customers at each substation have been aggregated, *i.e.*, the 0.4 kV distribution networks are not considered. Distributed generation in these networks is negligible. In this analysis, all switches are assumed to be closed, thus enabling power to

flow through them at all times. This represents an ideal situation where the power can be rerouted instantly. In reality, however, such rerouting might be delayed since switches are manually operated. Some basic network characteristics are presented in Table 1.

Table 1 Basic network characteristics of the two electric distribution systems

Network characteristics	*System A*	*System B*
No. of in-feed nodes	7	8
No. of transmission nodes	191	442
No. of distribution substations	568	830
Total no. of nodes	766	1280
Total no. of edges	822	1342
Average node degree (Newman, 2003)	2.15	2.10
Average inverse geodesic length (Newman, 2003)	0.0453	0.0437
Clustering coefficient (Newman, 2003)	0.00218	0.00461

The two distribution grids differ in that System B is only a part of a larger distribution system, *i.e.*, it is not limited to the municipality under consideration. Instead it extends across the boundaries and connects to the distribution system in other municipalities as well. Switches are located in these boundaries, but in contrast to the other switches in the network, these are assumed open at all times (thus no power can flow through them). The side effect of simulating a partial distribution system is that boundary effects emerge. Nodes close to these boundaries will display a higher vulnerability than in reality, since there is a possibility that these might be fed from other municipalities.

5.1 Strategies to remove nodes and edges

Systems might be robust to certain perturbations but vulnerable to others, which Hansson and Helgesson (2003) have pointed out and also demonstrated by, for example, Albert *et al*. (2000) and Holme *et al*. (2002). By employing different strategies to remove nodes and edges, it is possible to study the vulnerability of the system for different types of perturbations. In the literature, random failures and targeted attacks are usually employed. A targeted attack can be simulated by removing nodes and edges in decreasing order of their criticality, *i.e.*, nodes and edges that inflict large damage to the system when removed are removed first. Several measures have been proposed to represent the criticality of nodes and edges, the most common measures being the highest node degree and highest node or edge betweenness. Since these measures aim at identifying the criticality of nodes and edges, they can also provide information about where the system has deficiencies.

In this paper, we take a static network analytic approach and utilise seven strategies for node and edge removal: random node removal, random edge removal, node removal in decreasing order of initial node degree, node removal in decreasing order of initial betweenness, edge removal in decreasing order of initial betweenness, node removal in decreasing order of recalculated betweenness, and edge removal in decreasing order of recalculated betweenness (Newman, 2003; Holme *et al*., 2002). If several nodes or edges have equal degree or betweenness, the removal is done randomly. The betweenness

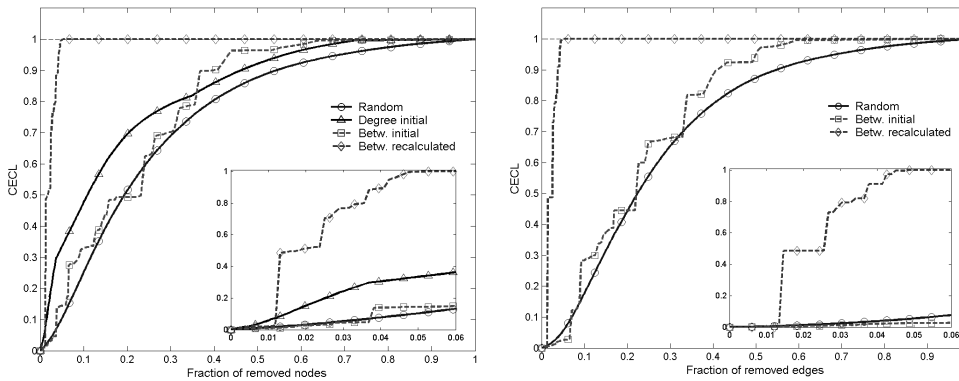
measure is based on the shortest paths between all in-feed points and distribution substations and is calculated as the sum of shortest paths traversing a specific node or edge, similar to the algorithm suggested by Newman (2001). However, instead of calculating the shortest paths between all pairs of nodes, which Newman's algorithm does, we calculate the shortest paths between *any* in-feed point or generator and all other nodes. That is, only the shortest path to the closest feeding point or generator is calculated for each node.

In the simulations, the in-feed nodes are not removed, the reason being that it is only the vulnerability of the distribution system that is of interest. The results from the simulations are based on averaged values of 1000 simulations for random removal and 100 simulations for the other strategies.

5.2 Analysis and interpretation of simulation results

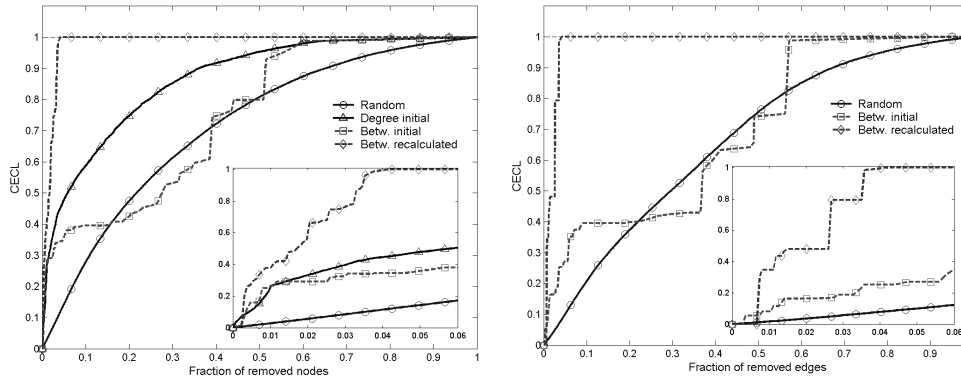
The most harmful removal strategy for System A is, as expected, the recalculated betweenness (Figure 2). For this strategy, all customers have lost power supply after the removal of 5.3% of the nodes or 5.2% of the edges. The strategy based on initial betweenness is only slightly more harmful than the random-based removal. Initial node degree removal is more harmful than initial betweenness and random removal but less harmful than recalculated betweenness.

Figure 2 CECL, for different removal strategies, as a function of the fraction of removed nodes (left) or edges (right) for System A



For System B, the most harmful removal strategy is the same as for System A, *i.e.*, recalculated betweenness (Figure 3). For this system, all customers have lost power after the removal of 4.2% of the nodes or 4.2% of the edges. The removal strategy based on initial degree is more harmful than random and initial betweenness. In Figure 3, the steep step-characteristics of the initial betweenness-based removal suggest that the system, when perturbed, evolve into a critical state where a small additional strain might cause consequences of large magnitudes.

Figure 3 CECL for different removal strategies as a function of the fraction of removed nodes (left) or edges (right) for System B

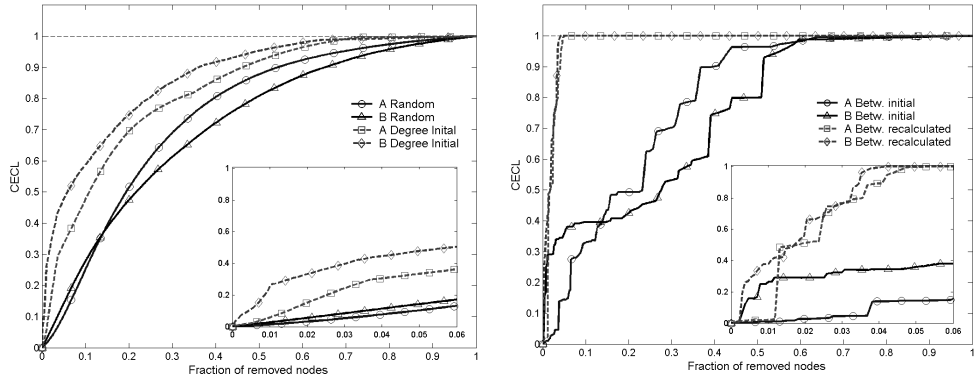


The node and edge-based removal strategies are very similar for both Systems A and B. This is due to the fact that the systems are mainly radially fed, *i.e.*, most nodes have a degree of two. In the remaining part of this paper, we focus on node-based removals, but much of the discussion is equally applicable for edge-based removals.

Surprisingly, initial betweenness turns out not to be a particularly harmful strategy for removal, at least not for System A where it is roughly as harmful as the random removal. For System B, the initial betweenness removal is quite harmful initially, but for larger fractions of removed nodes, it is not. There is an explanation why initial betweenness does not provide a good measure of node and edge criticality. This is because criticality is a dynamic property, since it depends on which components have been removed previously. Often, certain paths have high initial betweenness, *i.e.*, all nodes and edges in the path have high betweenness, which indicate that they are all critical. But after the removal of one of these components, the remaining components in the path are no longer critical, since the path is already cut. Thus, removals based on this measure might be harmful initially, but seldom for larger fractions of removed nodes or edges.

The performances of the two systems, according to CECL, are very similar, which is illustrated in Figure 4. The main reason for this is that the characteristics of the two systems are similar; both systems are electric distribution systems situated in mainly rural areas. It is straightforward to compare the vulnerability of the two systems for highest initial degree and recalculated betweenness removal, since the curve for System B is constantly above the curve of System A. Thus, System A is more robust to both types of perturbations, which is confirmed by comparing the SVC in Table 2. However, drawing conclusions concerning the other types of perturbations is harder. The SVC measure implies that System B is more robust to the other types of perturbations. However, Figure 4 shows that System B is more vulnerable than System A to small perturbations (less than about 13% removed nodes), but more robust to larger perturbations. Hence, it is important to note that the SVC measure cannot be used to draw conclusions of whether a system is vulnerable to small perturbations but robust to large ones, or vice versa. It is calculated for all magnitudes of the perturbations, *i.e.*, from no perturbation to total perturbation, and it does not consider the fact that very large perturbations might not be realistic for some systems.

Figure 4 Comparison of System A and System B for different removal strategies*



Note: * Random and initial degree removal of nodes are presented to the left. Initial and recalculated betweenness removal of nodes is presented to the right.

Table 2 SVC and DC presented for different strategies of node and edge removal, for Systems A and B

Measure	*Removal strategy*	*System A*	*System B*	*Comparison**
SVC	Random node	0.749	0.716	B
	Random edge	0.729	0.670	B
	Initial node degree	0.830	0.868	A
	Initial node betweenness	0.792	0.750	B
	Initial edge betweenness	0.772	0.701	B
	Recalc. node betweenness	0.979	0.983	A
	Recalc. edge betweenness	0.977	0.981	A
DC	Random node	0.354	0.467	B
	Random edge	0.365	0.502	B
	Initial node degree	0.274	0.279	B
	Initial node betweenness	0.315	0.469	B
	Initial edge betweenness	0.329	0.473	B
	Recalc. node betweenness	0.231	0.451	B
	Recalc. edge betweenness	0.209	0.414	B

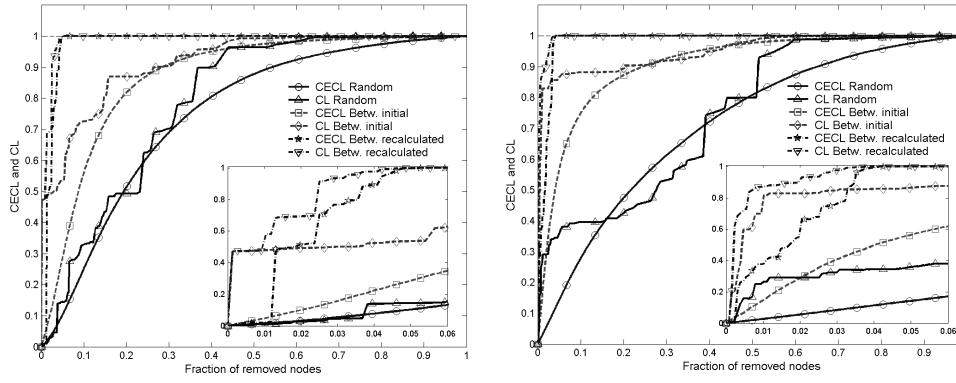
Note: * The letter in this column refers to the system that scores best on the particular measure

As can be seen in Table 2, the DC is higher for System B than for System A for all removal strategies. This implies that System B is designed to provide a more reliable power supply to substations, which many customers are connected, or equivalently, that System B has a better distribution of customers over the substations. However, this does not necessarily imply that System B is more robust than System A, *e.g.*, if System A would have a more redundant topology than System B, this might outweigh the fact the system has a low DC. Comparing the DC of the same system for different removal strategies shows for which type of perturbation the correspondence between system

topology and customer distribution is better. In Table 2, it can be seen that for both systems, the correspondence is better for random removal. For System A, the correspondence is worst for recalculated betweenness removal, while System B is least suited for initial node degree removal.

In Figure 5, we compare the two performance measures CECL and CL for System A and System B. It can be seen that the CL curve is constantly lying above the CECL curve (for the same removal strategy), which is expected, considering the definitions of the two measures. According to CECL, the network performance is reduced when a distribution substation has lost the connections to all in-feed points. According to CL, on the other hand, the network performance is reduced when a distribution substation loses a connection to any in-feed point, even if it still has connections to other in-feed points. CECL is a more realistic measure of network performance, since it accounts for the fact that redundant systems and systems with many in-feed points are more robust to perturbations. CL, on the other hand, does not account for this, since it measures the number of lost connection relative to the number of initial connections. The deficiency of CL is most clearly seen for betweenness removal in System A. Here, the network performance is reduced by almost 50% after the removal of only one node. The reason for this is that the network is divided into two main clusters, reducing the number of connections between distribution substations and in-feed points drastically. In reality though, all distribution substations have power supply since both clusters have multiple in-feed points, and consequently, CL overestimates the performance drop.

Figure 5 Comparison of CECL and CL for different strategies of node removal. System A is presented to the left and System B to the right.



6 Discussion

In this paper, we have taken a step towards expanding the notion of vulnerability of electric distribution systems. Our aim has been to develop methods that are more applicable than the ones previously suggested for societal vulnerability analysis. We have proposed three new measures, drawing on previous research which, instead of focusing only on technical aspects of the electric distribution system also incorporate aspects of societal vulnerability. In addition to being useful as tools for vulnerability analysis, the proposed methods can also constitute valuable tools when planning for effective and

efficient emergency response. When planning for emergencies, it is important to try to anticipate the *emergency needs*, *i.e.*, people's need for assistance, arising from different contingencies. The focus of this paper has been on global properties, such as fraction of customers affected by power outages in a municipality. Such properties describe the extent of the outages and thus give indication of the extent of the emergency needs. Even better indications of emergency needs might be obtained by investigating to which extent vulnerable groups (*e.g.*, elderly) and critical facilities (*e.g.*, hospitals, critical infrastructure) are affected.

In the empirical analysis, we have characterised the societal consequences from power outages as proportional to the number of customers without power supply. This is undoubtedly a reasonable assumption, although factors such as the vulnerability of the affected customers and the type of customer (hospital, industry, store, apartment, *etc.*) also influence the vulnerability. Such factors can be taken into account by assigning the customers different weights according to the definition of CE. Furthermore, we have used a static network analytic approach, where no redistribution of electric flow has been considered. Expanding these analyses in order to account for dynamic network analytic aspects is straightforward, using the insights from previous research (*e.g.*, Crucitti *et al*., 2004a; Kinney *et al*., 2005; Motter and Lai, 2002).

The calculation of SVC is intended to facilitate the comparison of different systems or different removal strategies. SVC translates the curve, shaped by the CECL as a function of fraction of removed nodes or edges, into a single value. It is important to note that by doing this, some information about the vulnerability of a system might be lost. There are aspects of vulnerability that cannot be captured in a single value, *e.g.*, some systems are robust to small perturbations but very vulnerable to large perturbations or perturbations exceeding a certain threshold. Furthermore, some systems might be vulnerable to small perturbations but able to withstand larger perturbations quite well, while other systems deteriorate linearly with increasing magnitude of the perturbations. Such information is concealed when the curve is translated into a single value. In this paper, SVC has been calculated from no perturbation to total perturbation (where all nodes or edges have been removed). Often, it is not interesting to study perturbations above certain levels, since such strains are not realistic for some systems. A possible remediation is to set a threshold, *e.g.*, maximum perturbation of 10%, and calculate the SVC up to this point.

There are several possible areas for further research in connection with the findings of this paper. Firstly, more sophisticated strategies for removing nodes and edges should be developed. Today, some generic strategies are employed, providing general information about the vulnerability of the electric distribution system. Often, there is an interest in analysing the vulnerability of the system to more specific threats, such as storms and hurricanes. In these cases, it is important that the strategies employed reflect the real-world perturbation under consideration. Removal strategies need to account for the fact that many perturbations are neither random (which is assumed in random removal) nor deterministic (which is assumed in targeted attacks). Secondly, more comparisons between different systems, using the proposed methods and measures, should be performed with the purpose of establishing values that represent good designs and values that represent poor designs. For example, using the DC measure to compare the design efficiency of different types of electrical networks, *i.e.*, transmission, subtransmission, urban and rural distribution systems. Thirdly, in order to provide an

even better tool for emergency management, the analyses in this paper should be complemented with exposure analyses, aiming to establish how probable different types and different magnitudes of perturbations are in the area of concern. Finally, more research should be made focusing on local characteristics of a network. Local characteristics can identify high-risk areas, critical nodes and edges, and areas where emergency needs are especially likely to arise. By focusing more on local characteristics, network analysis can hopefully be more useful in practice.

7 Conclusion

In this paper, we have taken a network analytic approach and suggested methods for analysing the societal vulnerability to perturbations in electric distribution systems. We have suggested three measures, which capture important aspects of societal vulnerability. We conclude that the suggested measures – CECL, SVC, and DC – can increase the value of using network analysis when analysing societal vulnerability to perturbations in electric distribution systems and that such analysis also can be useful in emergency mitigation and preparedness planning.

Acknowledgements

The authors would like to thank the Swedish Emergency Management Agency (the FRIVA project) for funding the research on which the present paper is based. The authors would also like to thank Associate Professor Olof Samuelsson and Research Associate Christian Rosén for their valuable comments.

References

Albert, R. and Barabási, A-L. (2002) 'Statistical mechanics of complex networks', *Review of Modern Physics*, Vol. 74, No. 1, pp.47–97.

Albert, R., Albert, I. and Nakarado, G.L. (2004) 'Structural vulnerability of the North American power grid', *Physical Review E*, Vol. 59, No. 025103.

Albert, R., Jeong, H. and Barabási, A-L. (2000) 'Error and attack tolerance of complex networks', *Nature*, Vol. 406, No. 6794, pp.378–382.

Apostolakis, G.E. and Lemon, D.M. (2005) 'A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism', *Risk Analysis*, Vol. 25, No. 2, pp.361–376.

Barabási, A-L. (2002) *Linked: The New Science of Networks*, New York: Penguin Group.

Buckle, P. (2000) 'New approaches to assessing vulnerability and resilience', *Australian Journal of Emergency Management*, Vol. 15, No. 2, pp.8–14.

Chassin, D.P. and Posse, C. (2005) 'Evaluating North American electric grid reliability using the Barabasi-Albert network model', *Physica A*, Vol. 355, Nos. 2–4, pp.667–677.

Crucitti, P., Latora, V. and Marchiori, M. (2004a) 'A model for cascading failures in complex networks', *Physical Review E*, Vol. 69, No. 045104.

Crucitti, P., Latora, V. and Marchiori, M. (2004b) 'A topological analysis of the Italian power grid', *Physica A*, Vol. 338, No. X, pp.92–97.

Crucitti, P., Latora, V. and Marchiori, M. (2004c) 'Error and attack tolerance of complex networks', *Physica A*, Vol. 340, Nos. 1–3, pp.388–394.

Crucitti, P., Latora, V., Marchiori, M. and Rapisarda, A. (2003) 'Efficiency of scale-free networks: error and attack tolerance', *Physica A: Statistical Mechanics and its Applications*, Vol. 320, pp.622–642.

Einarsson, S. and Rausand, M. (1998) 'An approach to vulnerability analysis of complex industrial systems', *Risk Analysis*, Vol. 18, No. 5, pp.535–546.

Gorman, S.P., Schintler, L., Kulkarni, R. and Stough, R. (2004) 'The revenge of distance: vulnerability analysis of critical information infrastructure', *Journal of Contingencies and Crisis Management*, Vol. 12, No. 2, pp.48–63.

Hansson, S.O. and Helgesson, G. (2003) 'What is stability?', *Synthese*, Vol. 136, pp.219–235.

Holme, P., Kim, B.J., Yoon, C.H. and Han, S.K. (2002) 'Attack vulnerability of complex networks', *Physical Review E*, Vol. 65, No. 056109.

Holmgren, Å. (2006) 'Quantitative vulnerability analysis of electric power networks', Doctoral thesis, Department of Transport and Economics, Royal Institute of Technology, Stockholm.

Kinney, R., Crucitti, P., Albert, R. and Latora, V. (2005) 'Modeling cascading failure in the North American power grid', *The European Physical Journal B*, Vol. 46, No. 1, pp.101–107.

Little, R.G. (2002) 'Controlling cascading failure: understanding the vulnerabilities of interconnected infrastructures', *Journal of Urban Technology*, Vol. 9, No. 1, pp.109–123.

Motter, A.E. and Lai, Y-C. (2002) 'Cascade-based attacks on complex networks', *Physical Review E*, Vol. 66, No. 065102.

Newman, M.E. (2001) 'Scientific collaboration networks. II. Shortest paths, weighted networks, and centrality', *Physical Review E*, Vol. 64, No. 016132.

Newman, M.E. (2003) 'The structure and function of complex networks', *SIAM Review*, Vol. 45, No. 2, pp.167–256.

Watts, D.J. (2004) *Six Degrees – The Science of a Connected Age*, London: Vintage.

Weichelsgartner, J. (2001) 'Disaster mitigation: the concept of vulnerability revisited', *Disaster Prevention and Management*, Vol. 10, No. 2, pp.85–94.

Notes

1 The storm did not cause significant disturbances at the transmission level and only minor damage at the subtransmission level; however, it caused severe damage at the distribution level (50–10 kV). It affected 600 000 customers in Sweden with outage times up to a month in the most severely affected areas.

2 Network performance is normally used as a description of how well the network is performing, *i.e.*, high values indicate well-functioning systems. However, when studying vulnerability, the focus is often on the negative consequence or degree of loss in the system, *i.e.*, high values indicate large negative consequences. Therefore, some of the performance measures presented in this paper, and the proposition of a new performance in particular, take the latter stance.

II

Identifying critical components in technical infrastructure networks

H Jönsson[1], **J Johansson**[2]*, and **H Johansson**[1]
[1]Department of Fire Safety Engineering and Systems Safety, Lund University, Lund, Sweden
[2]Department of Industrial Electrical Engineering and Automation, Lund University, Lund, Sweden

The manuscript was received on 15 October 2007 and was accepted after revision for publication on 17 December 2007.

DOI: 10.1243/1748006XJRR138

Abstract: A new method for identifying and ranking critical components and sets of components in technical infrastructures is presented. The criticality of a component or a set of components is defined as the vulnerability of the system to failure in a specific component, or set of components. The identification of critical components is increasingly difficult when considering multiple simultaneous failures. This is especially difficult when dealing with failures of multiple components with synergistic consequences, i.e. consequences that cannot be calculated by adding the consequences of the individual failures. The proposed method addresses this problem. In exemplifying the method, an analysis of an electric power distribution system in a Swedish municipality is presented. It is concluded that the proposed method facilitates the identification of critical sets of components for large-scale technical infrastructures.

Keywords: critical components, infrastructure networks, vulnerability, electric power systems, network analysis

1 INTRODUCTION

The reliability of technical infrastructures is crucial for many of the services that are taken for granted today. The present paper presents a method that can be used to identify critical components or sets of components in such a system. A critical component is a component that, if it should fail, can cause large negative consequences for the system's ability to provide its intended services. Here, failure should not only be seen as an unplanned event, but should also include a component being unavailable by other reasons, such as maintenance. Electric power distribution systems are used as an example of technical infrastructures. However, the method is applicable to a wide range of systems, such as water distribution systems and telecommunication systems. Nevertheless, electrical power distribution systems are probably among the most important infrastructures, from a societal perspective, since so many households, companies, and other technical infrastructures are dependent on electricity. Furthermore, there are numerous examples of disruptions of electric power systems causing severe consequences that illustrate the importance of such systems. Examples of these power outages include the prolonged power outages in the central areas of Auckland, New Zealand, in 1998 [**1**], the large-scale outages in the eastern USA in 2003 [**2**], and the disruptions following the blackout in Sweden 2003 [**3**].

Network analysis has previously been utilized to analyse the vulnerability of technical infrastructure systems [**4**–**10**]. The focus in these studies has often been on analysing global properties of systems, i.e. the system's overall vulnerability to perturbations. However, analysing local properties (properties of the components or groups of components) is also of great importance if the purpose is to reduce a system's vulnerability. One such type of analysis is to identify critical components, which is the focus in this paper. Previous research on critical components in technical infrastructure networks includes, for example, [**11**–**14**].

In brief, components or sets of components are defined as critical if they cause large consequences when they fail. According to this definition the criticality of components is only related to the

**Corresponding author: Industrial Electrical Engineering and Automation, Lund University, Box 118, Lund 22100, Sweden. email: jonas.johansson@iea.lth.se*
Extended version of a paper originally presented at ESREL 2007.

consequences of failures, not the probability of those failures. Identifying critical components is usually a straightforward task when only considering single failures. However, the task can be much more difficult when considering multiple simultaneous failures. A single component failure or multiple simultaneous component failures are henceforth referred to as failure sets. It is especially difficult to identify failure sets with synergistic effects. In the present context, synergistic effects imply that the negative consequences owing to a failure set are greater than the sum of the consequences due to individual failures of each of the components that are included in the set. In other words, failure of two components causing major negative consequences, implies a synergistic effect if each of the components failing by itself would not cause any significant consequences. In technical infrastructure networks, components that by themselves can cause large consequences if they fail can often be found in the centre of the network, also called the hub, or in places in the network where there is only one way to connect various parts of the network, i.e. there are no alternative paths between the network parts. However, identifying failure sets with synergistic effects is not easy, especially when the system is composed of a large number of components. Therefore, the method presented here aims at facilitating the identification and ranking, according to the level of criticality, of such components (and also failure sets without synergistic effects) in technical infrastructure systems. The aim is thus not to quantify the likelihood of any single or multiple failure but rather to facilitate the identification of parts of the system where it is especially important that components are robust and reliable or to indicate where redundancy should be considered. Critical components or sets of components, once identified, should be studied in further detail in order to complement the criticality ranking with an assessment of the likelihood of failure or simultaneous failures, for example, by considering the possibility of common cause failures.

The approach is exemplified by presenting analyses of a simple fictional network and a power distribution system in a Swedish municipality. The consequences of component failures are calculated using a capacity model of an electrical distribution system.

2 THE CONCEPTS OF VULNERABILITY AND CRITICALITY

Vulnerability is a widely used concept in many research areas, but its definition is often ambiguous and sometimes misleading [**15–18**]. Here, vulnerability is defined as the system's overall susceptibility to a specific hazardous event, i.e. the magnitude of the damage given the occurrence of that event. It is important to note that vulnerability must be related to a specific hazardous event in order to be meaningful, see for example reference [**16**] and [**19**]. A system might thus be vulnerable to certain events but be robust and resilient to others [**20**].

Criticality is a concept that is related to vulnerability and can be viewed as a characteristic of a component or set of components in a system. Criticality has some different denotations in the research literature. One interpretation is that components are seen as critical if they are essential for the system's function [**11**,**12**,**21**] and another interpretation is to also include the probability of the component failure in the criticality measure [**13**,**14**,**22**].

In the present paper the criticality of a component or set of components is considered to be the vulnerability of the system to failures in these components, i.e. the magnitude of the consequences caused by the failures. The more vulnerable the system is to the failure of a specific component or set of components, the more critical are the component/components.

3 CRITICALITY OF FAILURE SETS

A failure set is defined as a specific combination of failed components and is characterized by a size, which indicates the number of components that fail simultaneously. Each failure set can lead to several negative consequences depending on contextual factors such as the time of year and demands on the system. In this paper varying contextual factors such as the time of year, are disregarded and the power system modelling is deterministic. Thus, each failure set is only associated with one consequence.

Sets of different sizes are treated and compared separately when ranking the failure sets. This is because sets of larger sizes obviously have the potential of giving rise to consequences of greater magnitudes but also, in general, are more infrequent. The size of failure sets to consider is ultimately the analyst's choice and depends on how many simultaneous failures are deemed feasible. There is also a practical issue since the time required to analyse all possible combinations of failed components increases rapidly when the failure set size is increased. (The number of possible failure sets is $t!/((t-n)!\cdot n!)$, where t is the total number of system components and n is the size of the failure sets.) Therefore, it might not be practically feasible to analyse failure sets larger than three or four components for system's consisting many components.

In many systems there might be components or failure sets that are very critical but where this is, more or less, obvious. One example of such an

obvious component is an in-feed transformer in an electric distribution system which constitutes the only point of in-feed to a part of the network. When ranking failure sets in descending order of criticality, these components might occupy a considerable part of the top rankings. This is because these components are critical in themselves and thus cause large consequences independent of which other components fail simultaneously. Consider, for example, a system containing 1000 components, including one component that gives rise to the maximum consequence if it fails. This component will be a member of the top 999 and top 498 501 failure sets when ranking failure sets of size two and three, respectively. However, such failure sets are often of limited interest since their criticality is, in fact, an effect of the criticality of a single component in the set, which has already been identified as critical. Thus, a lot can be gained if these failure sets can be screened out.

A possible screening strategy is to rank failure sets according to the magnitude of their *synergistic consequences*. Assume that a failure set, F, contains n components, $c_1, \ldots, c_n$, and that $n > 1$, thus $F = \{c_1, \ldots, c_n\}$. The components in the failure set can be divided into proper subsets S. This division can be performed in several ways. Let V_i denote a set containing the subsets S for a specific division of F and let p denote the number of ways in which the divisions can be performed. A specific subset that belongs to V_i is denoted S^i_j. Denote the number of such subsets m, thus the subsets of V_i is $S^i_1, \ldots, S^i_m$. Since the subsets are constructed by a division of F, all components contained in the subsets are also in the failure set and each component can only be contained in one subset for each division. A failure set has synergistic consequences if, and only if, the negative consequences owing to the failures, $C(F)$, are greater than the sum of the consequences for the proper subsets of F, for all possible divisions $V_1, \ldots, V_p$

$$
\begin{aligned}
&C(F) > \sum_{j=1}^{m} C(S^i_j) \forall V_i : \\
&F = \{c_1, \ldots, c_n\}, n > 1 \\
&S^i_j \subset F, S^i_1 \cap \ldots \cap S^i_m = \varnothing, S^i_1 \cup \ldots \cup S^i_m = F, j = 1, \ldots, m \\
&V_i = \{S^i_1, \ldots, S^i_m\}, i = 1, \ldots, p
\end{aligned} \tag{1}
$$

A synergistic consequence of a failure set, $C_{\text{syn}}(F)$, is defined as the difference between the consequences of the failure set in question and the largest sum of the consequences of the subsets for all possible divisions V (see equation (2))

$$
C_{\text{syn}}(F) = C(F) - \max_{V_i} \left(\sum_{j=1}^{m} C(S^i_j) \right) \tag{2}
$$

The fraction of the synergistic consequences for a failure set is calculated as

$$
f_{\text{syn}} = \frac{C_{\text{syn}}(F)}{C(F)} \tag{3}
$$

What signifies a synergistic consequence is that it cannot be calculated using the consequences of the individual subsets of the failure set in question. Instead, synergistic consequences are the consequences arising owing to the fact that all the failures in the set occur simultaneously, i.e. the consequences that arise *in addition* to the consequences caused by the individual subsets. For example, synergistic consequences of size 3 failure sets cannot be calculated by adding up the consequences of its size 2 and 1 subsets. Thus, such critical failure sets cannot be identified only by considering combinations of components that are critical in themselves.

Ranking failure sets according to the magnitude of their synergistic consequences implies that some failure sets causing large consequences, but whose consequences to a large extent stem from subsets that in themselves cause large consequences, are screened out. Such screening is plausible since these subsets have already been identified when systematically going through failure sets of smaller sizes.

4 CRITICALITY OF COMPONENTS

In addition to identifying and ranking failure sets, it is also desirable to establish a criticality ranking of *individual components*. When evaluating the vulnerability of a system to failure sets in the present paper, the consequences are deterministic in the sense that the failure of the components in the set always leads to the same consequences. An individual component, however, can be a part of several failure sets causing different levels of consequences. One specific component might therefore cause no significant consequences if failing at the same time as one component from a specific group of components, whereas if it fails at the same time as a component not belonging to the specific group of components the consequences might be vast. This needs to be taken into account when establishing a measure of a specific component's criticality.

When considering two simultaneous failures the criticality of a specific component is seen as the vulnerability of the system to failures in the specific component *and* one other component. There are many failure sets of size 2 that include a specific component, and each failure set is associated with a consequence. Thus, the vulnerability of the system can be described by a set of failure sets including a

description of the consequences owing to each failure set. Vulnerability measures, which facilitate the comparison of different components' criticality, can then be derived from the set of failure sets. In this paper, one of the measures used is the *average consequences* of all failure sets that contain a specific component. This measure can be interpreted as the average consequences owing to the failures of a specific component *and* another component chosen at random (for failure sets of size 2).

In the previous section, failure sets larger than 1 were screened according to the synergistic parts of their consequences, C_{syn}. However, although this screening is conducted many failure sets might remain, leading to a tedious volume of data interpretation. It would thus be desirable to calculate a measure that indicates which components are the main contributors to the synergistic consequences for a certain failure set size. Such a metric is presented in equation (4)

$$\text{Con}_{\text{size}=n}(c_i) = \frac{\sum C_{\text{syn}}(F|c_i \in F, n)}{\sum C_{\text{syn}}(F|n)} \tag{4}$$

where c_i is a specific component and n the size of the failure set. $\sum C_{\text{syn}}(F|c_i \in F, n)$ is the sum of the synergistic consequences of all failure sets of size n that contain the components of interest, c_i. $\sum C_{\text{syn}}(F|n)$ is the sum of the synergistic consequences of all failure sets of size n. The measure expresses the contribution of a specific component's synergistic consequences to the total synergistic consequences for a certain failure set size. Thus, a component that is contained in many failure sets with large synergistic consequences would score high on this measure, indicating that this component deserves further attention.

5 ELECTRIC DISTRIBUTION SYSTEM MODELLING

In exemplifying the approach described above, a network analytic approach is used to create a model of an electric power grid using nodes and edges. Three different types of nodes are considered: in-feed nodes (where the electricity is fed into the network), load nodes (where customers are connected), and transfer nodes (nodes without customers or in-feed).

It is important to note that modelling power systems as networks means that a number of simplifications are made. First, there is the problem of choosing the level of detail for the model. The main focus is to obtain a manageable model that is still a plausible representation of the real system. This means that a component in the network model might refer to a number of real components that are lumped together. For example, an edge might represent more than a cable or a line. It can also include breakers, fuses, and other protection devices that might malfunction and cause failures with the same consequences (i.e. the line goes out of service). Furthermore, a node can represent more than one type of component, such as bus bars, relays, and transformers.

Second, in network analysis it is common that the electrical properties of the power system are neglected, i.e. no physical model of the system is used. Instead the performance of the power network is often evaluated by measuring some structural property of the network. In this paper a physical model is used, which takes into account the loads of the distribution substations and the capacities of the in-feed nodes, i.e. a capacity model. The system behaviour, and thus the consequences of component failures, is affected by the fact that customers' power demand varies with time. In the present paper only one demand condition is considered; the peak power demand calculated from the aggregated yearly energy demand at each substation, i.e. in some sense the worst case. Furthermore the capacity of in-feed nodes corresponds to the nominal power rating of the in-feed transformers. If another type of technical infrastructure system had been analysed here, the model used to calculate the consequences would be different. Nevertheless, as long as the negative consequences owing to component failures can be estimated, the same approach to identifying critical components can be used.

For the capacity modelling algorithm, two conditions have to be met in order for a specific distribution substation to have power supply. First, there has to be an unbroken path between the substation and at least one in-feed node. Second, the in-feed node/nodes must have enough capacity left to feed the distribution substation. However, the capacities of the edges are neglected.

Many existing vulnerability analysis methods based on network analysis do not consider the societal consequences of failures and service interruptions. Instead the consequences are often evaluated from purely topological characteristics of the networks. However, it is argued that the value of power systems is constituted by the value of the services that these systems provide to the society [**9**]. This view is also proposed by Little [**23**]. Thus the consequences owing to failures in the power system should be evaluated with regards to the deterioration of these services. In a previous paper a measure called customer equivalents (CE) was suggested, which enables the assignment of different weights to different customers [**9**], depending on the societal consequences that arise when different customers lose power supply. The idea of CE is similar to the approach proposed by Apostolakis and colleagues [**13**,**24**], which is based on multi-attribute utility theory.

6 EXAMPLE OF A SMALL SYSTEM

In this section the previously described method is exemplified by applying it to a simple, fictional electric distribution network. It consists of 1 in-feed node, 5 load nodes, and 7 edges, i.e. 13 components in total (see Fig. 1). Each load node supplies 1 CE and no customers are connected to the in-feed node. The consequences are calculated as the fraction of CE without power supply. The capacity of the in-feed node is not a constraining factor.

Three sizes of failure sets are considered; 1, 2, and 3. Even for this small network there are 78 failure sets of size 2 and 286 failure sets of size 3: however only a few of these are synergistic; 4 and 10 sets, respectively. In Fig. 2 scatter plots of all synergistic failure sets of size 2 and size 3 are presented. The figures show that some failure sets give rise to large consequences where the synergistic fraction is small. This indicates that a large part of the total consequences can be referred to a subset of the failure set. Consider, for example, the {4 8} set, which means that components 4 and 8 have failed, see Fig. 2. In this case the failures cause a power loss to nodes 3, 4, 5, and 6, and most of the consequences can be referred to the individual failure of component 4, since this leads to a loss of power supply to components 4, 5, and 6. Only the power loss to node 3 constitutes a synergistic effect. In Fig. 2 it can also be seen that the failure set {7 8 9} is highly critical (maximum consequence) with a 100 per cent synergistic consequence, i.e. none of the consequences of the failure set can be referred to any of its subsets. This set can be contrasted with {4 7 8}, which leads to the same consequences but only has 20 per cent synergistic consequences, because most of the consequences derive from the critical subsets {4 7} and {4 8}, which in turn to a large extent is due to the critical component {4}. These scatter plots can thus be valuable when identifying failure sets of special interest, i.e. sets with large consequences *and* with a large synergistic fraction.

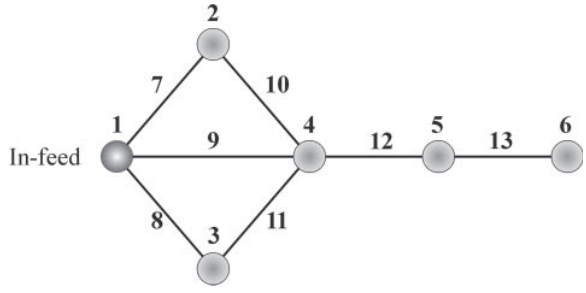


Fig. 1 Example network. The numbers in the figure correspond to the component number of the specific node or edge

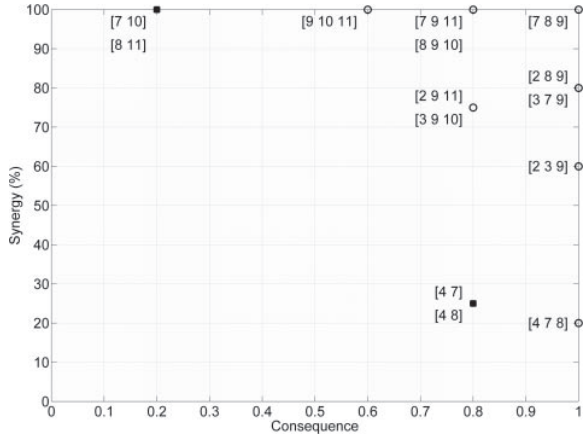


Fig. 2 Consequence-synergistic scatter plot of synergistic failure sets of size 2 (filled squares) and size 3 (circles). The consequences of the failure sets, $C(F)$ are presented on the horizontal axis and the percentage of the synergistic consequences is presented on the vertical axis

Table 1 Ranking of the criticality of failure sets*

Size = 1		Size = 2			Size = 3		
F	$C(F)$	F	$C(F)$	f_{syn} (%)	F	$C(F)$	f_{syn}(%)
{1}	1.0	{4 7}	0.8	25	{7 8 9}	1	100
{4}	0.6	{4 8}	0.8	25	{2 8 9}	1	80
{5}	0.4	{7 10}	0.2	100	{3 7 9}	1	80
{12}	0.4	{8 11}	0.2	100	{7 9 11}	0.8	100
{2}	0.2				{8 9 10}	0.8	100
{3}	0.2				{2 9 11}	0.8	75
{6}	0.2				{3 9 10}	0.8	75
{13}	0.2						

*The components in the failure set, F, are presented in brackets followed by the total consequence of the failure set, $C(F)$, and the fraction of the synergistic consequence, f_{syn}. Only the synergistic failure sets are presented for size 2 and 3 failure sets.

In Table 1 the information from the scatter plots is presented in table format along with the criticality of size 1 failure sets. For failure sets of size 3, only those failure sets with a consequence higher than 0.7 and a synergy higher than 70 per cent are listed. The table shows that component 1 is the most critical component individually, followed by component 4, which is obvious when considering the structure of the network. Component 1 is not represented in the larger failure sets, since all failure sets containing component 1 are screened out. Without the screening, component 1 would be contained in the top 12 failure sets (size 2) and top 66 failure sets (size 3), since it is so critical in itself. This would, to a large extent, conceal other interesting findings, such as the {7 8 9} set.

In Table 2 the criticality of individual components is presented. The average consequences, described in section 4, are used as the criticality metric. The table shows that some components are very critical in themselves, such as components 1 and 4. Ensuring

Table 2 Criticality of components in single and multiple failures. $\overline{C}$ is the *average consequences* of all failure sets that contain a specific component and rank is the criticality ranking of the components. A lower number implies a more critical component

	1 failure		2 failures		3 failures	
Comp.	C	Rank	$\overline{C}$	Rank	$\overline{C}$	Rank
1	1	1	1	1	1	1
2	0.2	5	0.433	5	0.633	3
3	0.2	5	0.433	5	0.633	3
4	0.6	2	0.7	2	0.782	2
5	0.4	3	0.5	3	0.603	5
6	0.2	5	0.367	7	0.518	12
7	0	–	0.3	9	0.558	8
8	0	–	0.3	9	0.558	8
9	0	–	0.267	13	0.572	7
10	0	–	0.283	11	0.524	10
11	0	–	0.283	11	0.524	10
12	0.4	3	0.5	3	0.603	5
13	0.2	5	0.367	7	0.518	12

Table 3 Component contribution to the synergistic consequences

Comp.	2 failures		3 failures	
	Contr. (%)	Rank	Contr. (%)	Rank
1	0	–	0	–
2	0	–	29.4	4
3	0	–	29.4	4
4	50	1	2.9	5
5	0	–	0	–
6	0	–	0	–
7	50	1	41.1	2
8	50	1	41.1	2
9	0	–	100	1
10	25	2	30.9	3
11	25	2	30.9	3
12	0	–	0	–
13	0	–	0	–

that such components are robust should be the primary concern in any vulnerability reduction activity. However, for this type of ranking it is difficult to draw conclusions regarding the failure set sizes for which a component becomes critical.

In Table 3 the contribution of different components to the synergistic consequences is presented. In this table it is easier to identify the failure set sizes for which a component becomes critical. Component 9, for example, does not contribute to any consequences unless there are three simultaneous failures. In fact, this component is represented in all synergistic failure sets of size 3 but not in any of the smaller sizes. If three simultaneous failures are deemed possible this component deserves special attention.

This example has shown the applicability of the proposed approach on a small network where the results are, to a large extent, comprehensible and in some cases obvious. However, when considering real, large-scale networks, it is more difficult to identify critical components and failure sets without employing a systematic approach.

7 ANALYSIS OF AN ELECTRIC DISTRIBUTION SYSTEM

In this section an analysis of a large-scale 11 kV electric distribution system in a Swedish municipality is presented by using the proposed method. The system is composed of 352 nodes and 451 edges, i.e. 803 components in total. The system is located in an urban area where all cables are underground. There are three 130/11 kV in-feed points. The transformers, eight in total, at these locations are modelled as in-feed nodes. Each bus bar in the HV/MV (high voltage to medium voltage) substations is modelled as a node and the bus bar breakers are modelled as edges. The MV/LV (medium voltage to low voltage) substations are modelled as single nodes. The aggregated nominal power rating for HV/MV transformers is 320 MVA and the aggregated peak power demand is 177 MVA, distributed to 47 523 customers.

The distribution system is radially operated but built meshed, which allows for reconfigurations to take place in case of failures. In this analysis any normally open sectionalizers and breakers are modelled as closed. This assumption leads, in some way, to an idealized system representation since it assumes that reconfigurations are instantaneous, i.e. the longer-term consequences are in focus here.

At each load node (i.e. MV/LV substations) the aggregated number of customers and the power demand is known. There are load nodes with single customers that have a high power demand as well as load nodes with many customers that have relatively low power demands. Since both these parameters are important indicators of the consequences that arise when the power supply is interrupted, the CE of a specific node is calculated using a combination of the number of customers and the power demand of that particular node. For load node i the CE is calculated as

$$\mathrm{CE}_i = \frac{(N_i/\overline{N} + P_i/\overline{P})}{2} \tag{5}$$

where N_i is the number of customers and P_i is the power demand at load node i. N_i and P_i are normalized by their corresponding average values, $\overline{N}$ and $\overline{P}$. Thus, a load node with an average number of customers and an average power demand has 1 CE. An overview of the distribution system is given in Fig. 3.

Failure sets of size 1, 2, and 3 are considered in this analysis. In total there are 322 003 sets of size 2 and 85 974 801 sets of size 3. Of these, 3116 and 16 408

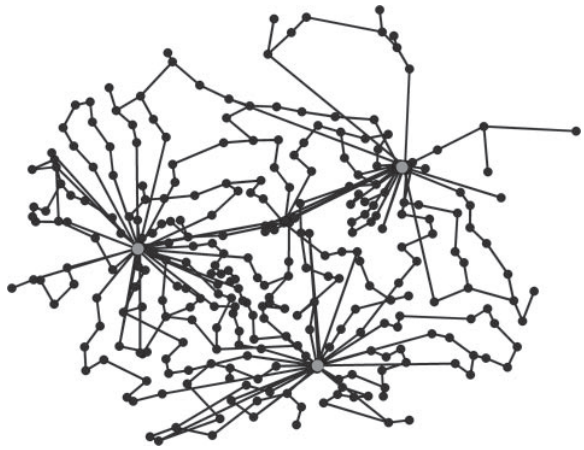


Fig. 3 Overview of the electric distribution system. The larger circles indicate in-feed nodes and the smaller circles indicate load nodes and transfer nodes

sets have synergistic consequences, respectively. In Fig. 4 scatter plots of the synergistic failure sets are presented together with the 1000 highest non-synergistic failure sets. It is interesting to notice that the failure sets with the highest consequences are synergistic for both failure set sizes. Furthermore, the highest consequence that can arise for the studied network is 0.075 (3078 customers and 15 MW) for two simultaneous failures and 0.12 (6775 customers and 17.5 MW) for three simultaneous failures. Thus, in addition to identifying critical components, this approach also gives a notion of the system's overall vulnerability to simultaneous failures.

Although a large portion of the failure sets have been screened out, many still remain. The scatter plots facilitate the selection of which failure set to study in further detail. In Table 4 the most interesting failure sets (both high consequence and high synergy fraction) of size 2 and 3 are presented. In order to limit the number of failure sets presented here (an in-depth analysis would consider a much larger number of failure sets), these have been chosen in accordance with the following criteria. For failure sets of size 2, sets with consequences larger than 0.0488 and synergy fraction larger than 79 per cent have been selected. For failure sets of size 3, sets with consequences larger than 0.1020 and synergy fraction larger than 36 per cent have been selected.

Each of the selected failure sets in Table 4 contains at least one bus bar at the 130/11 kV substations, indicating that these are highly critical components for the system. This result complies with common knowledge of electrical distribution systems. None of the 130/11 kV transformers are listed as highly critical components, since the in-feed capacity is roughly twice as high as the peak power demand

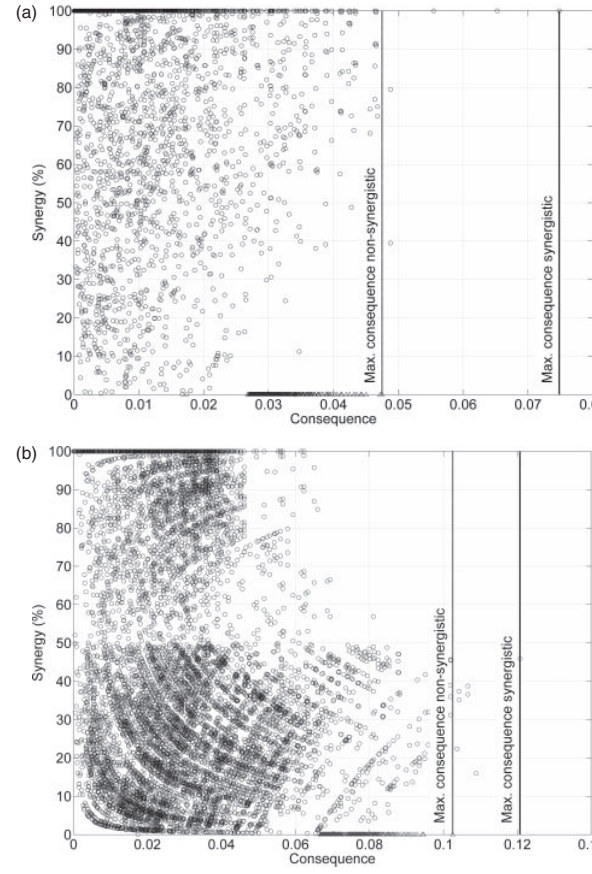


Fig. 4 Consequence-synergistic scatter plot of synergistic failure sets of size 2 (a) and size 3 (b). The consequences of the failure sets, *C(F)*, are presented on the horizontal axis and the percentage of the synergistic consequences is presented on the vertical axis. Synergistic failure sets are represented with a circle and the 1000 highest non-synergistic failure sets are represented with a triangle

Table 4 Ranking of failure sets according to their criticality*

Size = 1		Size = 2			Size = 3		
F	$C(F)$	F	$C(F)$	f_{syn} (%)	F	$C(F)$	f_{syn} (%)
{65}	0.0277	{350 351}	0.0748	100	{336 337 344}	0.1207	45.9
{197}	0.0198	{337 344}	0.0652	100	{208 337 344}	0.1066	36.6
{198}	0.0195	{336 337}	0.0554	100	{337 344 620}	0.1066	38.8
{275}	0.0174	{53 333}	0.0488	79.5	{337 344 619}	0.1043	37.4
{279}	0.0167	{53 609}	0.0488	79.5			

* The components in the failure set, F, are presented in brackets followed by the total consequence of the failure set, $C(F)$, and the fraction of the synergistic consequences

and therefore the remaining transformers are able to supply the customers even if up to three of them should fail.

If the bus bars and the transformers at the 130/11 kV substations are regarded as highly reliable and screened out, other interesting failure sets can be identified. For example, the simultaneous failure

Table 5 Criticality of components in single and multiple failures

Rank	1 failure		2 failures		3 failures	
	Comp.	C	Comp.	$\overline{C}$	Comp.	$\overline{C}$
1	65	0.0277	65	0.0290	65	0.0304
2	197	0.0198	197	0.0212	197	0.0226
3	198	0.0195	198	0.0209	198	0.0224
4	275	0.0174	275	0.0187	275	0.0201
5	279	0.0167	279	0.0180	279	0.0194

Table 6 Component contribution to the synergistic consequences

Rank	2 failures		3 failures	
	Comp.	Contr. (%)	Comp.	Contr. (%)
1	337	5.11	337	18.11
2	343	4.08	343	9.53
3	336	2.88	333	6.57
4	344	2.71	344	5.60
5	333	2.06	336	4.29

of components 53 and 198 will cause substations supplying many customers (but carrying a relatively low load) to lose power supply, leading to a consequence of 0.048. Another example is failure set {478 779} that contains two cables that render nine substations without power when they malfunction, causing a total consequence of 0.047. The first failure set that consists of three cables, {417 423 609}, has a rank of 784 and the consequence 0.062, i.e. roughly half the consequences of the most critical size 3 failure set.

In Table 5 the five most critical components are presented for the three different failure set sizes. As in the previous example, the average consequences are used as a criticality measure. In the table it can be seen that the components that are critical in single failures are also critical when considering multiple failures. The reason is that only a small fraction of failure sets that are synergistic; therefore the consequences of the single failures will pervade the average consequences of the failure sets as well. Since the network is highly meshed, Table 5 consists of nodes with a high CE.

In Table 6 the five components that contribute the most to the synergistic consequences is presented. All these components are bus bars at the in-feed stations. The reason for this is that the bus bars are the starting point for the meshed cable network, which interconnects the different in-feed stations.

8 DISCUSSION

In the present paper, a method for identifying and ranking critical components and sets of components in technical infrastructure systems is proposed. The method implies a systematic evaluation of the consequences of component failures in order to determine their criticality. The method has been used to analyse an electric power system, which has been modelled using a network analytic approach and a capacity model. The proposed method can be used along with other physical modelling techniques as well (e.g. power flow models). In addition, it is argued that the method can be applied to other technical infrastructures, such as water distribution and telecommunication systems, by using different representations of the physical system. Many technical infrastructures can be represented as networks and the network modelling technique used in this paper can provide a foundation for modelling other systems, although appropriate adaptations have to be conducted in order to capture the essentials of the system's behaviour in response to component failures.

In the paper, the distribution level of an electric power system has been analysed. However, it might be even more valuable when applied to the transmission or sub-transmission levels of the power system. At these levels, a more refined physical model should be used. Primarily, the capacity limits of lines need to be accounted for. In this paper, only the capacities of the in-feed nodes and the demands from the load nodes have been considered. Incorporating these line capacity limits in the modelling is not difficult but will increase computational time.

The criticality of a component, or set of components, has been defined as the vulnerability of the system to failures in the component or set of components. It is important to note that only the consequences of failures are included in the notion of criticality. When making decisions regarding vulnerability and risk reductions, the likelihood of failures needs to be taken into account. The criticality measure can be used to establish a priority ranking for which components need to be especially robust and reliable – the more critical the component or the set of components is, the more robust it needs to be. Theoretically, it is straightforward to incorporate the probability of failures in criticality measures, for example by using generic failure rates. However, often the generic failure rates are not suitable realistically to quantify the probability of simultaneous failures, especially for common cause failures and malicious attacks. Instead of trying to identify the phenomena that lead to common cause failures and trying to derive which components might be affected, it is argued that a more practically feasible approach is to first identify the component failures that cause severe consequences for the system as a whole and then consider whether these components can fail simultaneously, for example, from a common cause.

The number of failure sets increases rapidly when considering failure sets of larger size. Evaluating all possible combinations of failures is practically impossible in many systems. Therefore, ways of reducing the number of failure sets that need to be analysed, without losing important information about the system's vulnerability to failures, have to be developed.

9 CONCLUSION

The proposed method facilitates the identification of critical failure sets and components for large-scale technical infrastructures, such as electrical power systems. By using the method it is possible to gain insights about the system that otherwise might be overlooked. In addition to identifying critical components, other valuable information about the system's vulnerability can be gained, such as the maximum consequences due to individual or simultaneous failure of components.

ACKNOWLEDGEMENTS

This research has been financed by the Swedish Emergency Management Agency, which is greatly acknowledged. The authors would also like to thank Research Assistant Christian Rosén and Associate Professor Olof Samuelsson for their valuable comments.

REFERENCES

1 **Newlove, L. M., Stern, E.,** and **Svedin, L.** *Auckland unplugged*, 2000 (Copy Print, Stockholm).
2 **U.S.-Canada Power Systems Outage Task Force.** Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations, 2004 (US Department of Energy, Washington, DC).
3 **Larsson, S.** and **Ek, E.** The blackout in Southern Sweden and Eastern Denmark, 23 September 2003. Proceedings of IEEE PES General Meeting, 2004, Denver.
4 **Albert, R., Albert, I.,** and **Nakarado, G. L.** Structural vulnerability of the North American power grid. *Phys. Rev. E*, 2004, **69**(025103), 1–4.
5 **Crucitti, P., Latora, V.,** and **Marchiori, M.** A topological analysis of the Italian power grid. *Physica A*, 2004, **338**(1–2), 92–97.
6 **Chassin, D. P.** and **Posse, C.** Evaluating North American electric grid reliability using the Barabasi–Albert network model. *Physica A*, 2005, **355**(2–4), 667–677.
7 **Kinney, R., Crucitti, P., Albert, R.,** and **Latora, V.** Modeling cascading failure in the North American power grid. *Eur. Phys. J. B*, 2005, **46**(1), 101–107.
8 **Holmgren, Å.** Using graph models to analyze the vulnerability of electric power networks. *Risk Analysis*, 2006, **26**(4), 955–969.
9 **Johansson, J., Jönsson, H.,** and **Johansson, H.** Analysing the vulnerability of electric distribution systems: a step toward incorporating the societal consequences of disruptions. *Int. J. Emergency Mgmnt*, 2007, **4**(1), 4–17.
10 **Albert, R., Jeong, H.,** and **Barabasi, A.-L.** Error and attack tolerance of complex networks. *Nature*, 2000, **406**, 378–382.
11 **Crucitti, P., Latora, V.,** and **Marchiori, M.** Locating critical lines in high-voltage electrical power grids. *Fluctuation and Noise Lett.*, 2005, **5**(2), 201–208.
12 **Gorman, S. P., Schintler, L., Kulkarni, R.,** and **Stough, R.** The revenge of distance: vulnerability analysis of critical information infrastructure. *J. Contingencies Crisis Mgmnt*, 2004, **12**(2), 48–63.
13 **Apostolakis, G. E.** and **Lemon, D. M.** A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism. *Risk Analysis*, 2005, **24**(2), 361–376.
14 **Jenelius, E., Petersen, T.,** and **Mattson, L.-G.** Importance and exposure in road network vulnerability analysis. *Transp. Res. Part A*, 2006, **40**, 537–560.
15 **Buckle, P.** and **Mars, G.** New approaches to assessing vulnerability and resilience. *Aust. J. Emergency Mgmnt*, 2002, **15**(2), 8–14.
16 **Dilley, M.** and **Boudreau, T. E.** Coming to terms with vulnerability: a critique of the food security definition. *Food Policy*, 2001, **26**, 229–247.
17 **Weichselgartner, J.** Disaster mitigation: the concept of vulnerability revisited. *Disaster Prevention Mgmnt*, 2001, **10**(2), 85–94.
18 **Haimes, Y. Y.** On the definition of vulnerability in measuring risks to infrastructures. *Risk Analysis*, 2006, **26**(2), 293–296.
19 **Wisner, B., Blaikie, P., Cannon, T.,** and **Davis, I.** *At risk: natural hazards, people's vulnerability and disasters*, 2nd edition, 2004 (Routledge, London).
20 **Hansson, S. O.** and **Helgesson, G.** What is stability? *Synthese*, 2003, **136**, 219–235.
21 **Latora, V.** and **Marchiori, M.** Vulnerability and protection of infrastructure networks. *Phys. Rev. E*, 2005, **71**(015103), 1–4.
22 **Einarsson, S.** and **Rausand, M.** An approach to vulnerability analysis of complex industrial systems. *Risk Analysis*, 1998, **18**(5), 535–546.
23 **Little, R. G.** Controlling cascading failure: understanding the vulnerabilities of interconnected infrastructures. *J. Urban Technol.*, 2002, **9**(1), 109–123.
24 **Michaud, D.** and **Apostolakis, G. E.** Methodology for ranking the elements of water-supply networks. *J. Infrastructure Systems*, 2006, **12**(4), 230–242.

III

Risk and Vulnerability Management of Electrical Distribution Grids

Jonas Johansson and Stefan Svensson
Grontmij AB / Lund University, IEA and SWECO Energuide AB
jonas.pf.johansson@grontmij.se / jonas.johansson@iea.lth.se
and stefan.ng.svensson@sweco.se

ABSTRACT

Risk and vulnerability management can serve a very important purpose as a decision support tool for investments and planning of electrical distribution systems. In 2006 amendments to the Swedish Electricity Act came into force, stating that every distribution system operator has to, on a yearly basis, perform a risk and vulnerability analysis regarding security of supply to customers. Furthermore, the act also declares that risk mitigating efforts should be addressed and reported to the enforcing authority, i.e. encompassing a risk and vulnerability management approach. The present paper will discuss the concept of risk and vulnerability management for electrical distribution systems and how it interplays with other regulatory frameworks. Similarities and differences between the concepts of risk and vulnerability, as proposed by the authors, are also discussed. The paper covers both how such an analysis can be performed, using consumer and network structure information combined with network operational and performance data, and how the results can be incorporated and utilised in the overall management of electrical distribution systems. Important issues that require further research and input from stakeholders are also illuminated. Such issues are for example how to define appropriate risk acceptance criteria and the impact of the regulatory framework concerning quality of supply for distribution system operators.

1. INTRODUCTION

Incidents in the Swedish electrical distribution system during the last couple of years, such as the storms Per and Gudrun and the blackout of 2003, coupled with the greater demand for a higher quality of supply from the customer side has lead to a new perspective of the regulatory framework concerned with regulating electricity distribution system operators (DSOs). The new perspective is not only present for the electricity sector but encompasses many sectors of the society.[1] This perspective concerns the need to evaluate and understand the impact of threats and hazards to the society's social and technical systems. The vision from a regulatory point of view must be that these analyses for different sectors will result in a complete and transparent picture of risks in the society, from a municipal level all the way up to a national level. One specific type of regulatory change, in order to address the above stated perspective, is the demand for risk and vulnerability analysis, often accompanied by a demand for mitigation strategies for identified risk and vulnerabilities. By encompassing both

[1] For example the following Swedish acts and regulations contain requirements of risk analysis: "Plan- och bygglagen" (risks should be considered in community planning). "Miljöbalken" (risk analysis should be conducted regarding environmental impact). "Lag (2006:544) om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap" (municipalities and county councils must conducts risk and vulnerability analysis). "Förordning (2006:492) om krisbederskap och höjd beredskap" (Government authorities must conduct risk and vulnerability analysis).

the analysis and the mitigation of risk and vulnerabilities, risk and vulnerability management is addressed. For the electricity distribution sector this is concretised in an amendment to the Electricity Act. Another important regulatory framework that has a direct impact on the management of electrical distribution systems in Sweden is the Network Performance Assessment Model (NPAM) and the amendment of the interruption compensation paragraph and the 24-hour function demand to the Electricity Act.

The purpose of the paper is to discuss the regulatory framework concerning quality of supply and to present and discuss a risk and vulnerability management scheme for DSOs. The implications of the regulatory frameworks for distribution system management are discussed in the next section. Section 3 discusses the concept of risk and vulnerability, as used in this paper. In section 4 a risk and vulnerability management scheme is introduced and discussed. The paper ends with a discussion and some concluding remarks.

2. DISTRIBUTION SYSTEM REGULATION CONTEXT

Since electrical distribution systems are natural monopolies, due to the deregulation of the electricity sector in Sweden 1996, regulatory frameworks are necessary in order to ensure a safe, reliable, and cost effective distribution system, seen from a societal perspective. In 2005 the Network Performance Assessment Model (NPAM) came into force as the main tool for the regulatory body, Swedish Energy Markets Inspectorate (SEMI), to address the issues of cost effectiveness and fair tariffs for customers in a deregulated market. In 2002 and 2003 snow blizzards as well as system deficiencies caused large-scale disruption to the power supply of many customers. The storm Gudrun in 2005 caused disruption in the power supply of 650 000 customers in southern Sweden, some customers without power supply of up to seven weeks. The storm Per in 2007 left 440 000 customer without power. These disruptions highlighted how much the society depends on electricity, which was recognized by the Swedish cabinet in proposition 2005/06:27. The proposition sets performance goals for the reliability of electrical power supply; one stating that the maximum allowable time for the disruption of supply to any customer is 24 hours. The proposition also put forward an amendment to the Electricity Act in order to highlight the need of a regulated risk and vulnerability management process. These amendments to the electricity Act together with NPAM provide SEMI with three main tools to steer the electricity distribution market towards these goals: the quality deduction parameter in the NPAM, customer compensation for long-term interruptions and risk and vulnerability management. In Figure 1, an overview of the described tools and the impact for DSOs is shown.

The NPAM is used in the process of setting maximum allowed revenue levels for DSOs, partially based on the quality of supply. The NPAM theoretically calculates an optimal level for the quality of supply, using Monte Carlo simulations of reinforced radial grids with a cost parameter, which is based on consumer surveys of interruption evaluations, for every DSO. This theoretical value is compared with the actual value of quality of supply for the DSO. If the actual value of quality of supply is lower than the theoretical, a reduction is made from the DSO's maximum allowed revenue. If the actual value is higher, no adjustment of the maximum allowed revenue is made (Solver, 2005). If the DSO is subject to reduction of the maximum allowed revenue, an increase in quality of supply may allow the DSO to maintain or increase its revenue proportionally at the same time as avoiding fines.

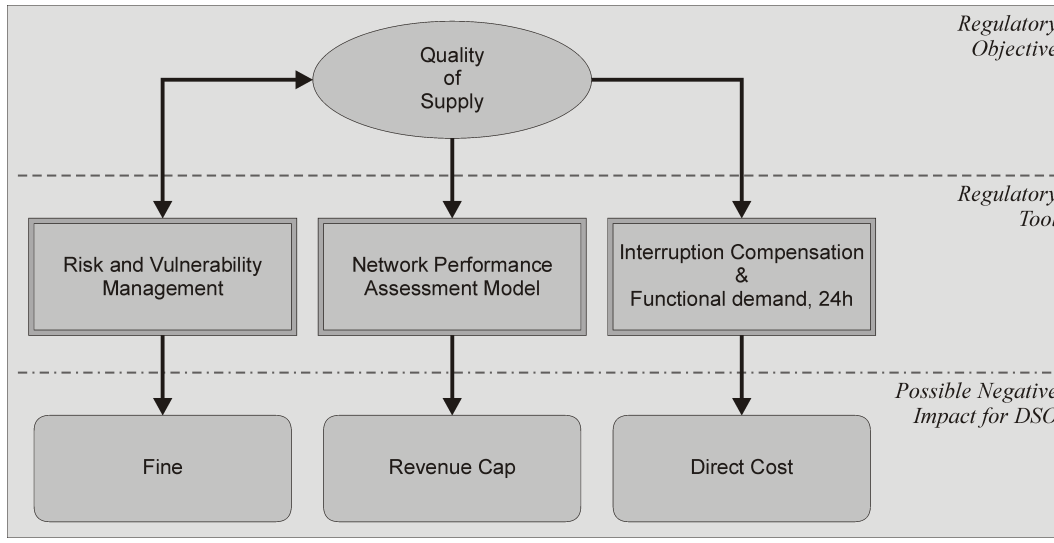


Figure 1. The regulatory context for the regulation of quality of supply and the impact for DSOs.

The Electricity Act (Ellag 1997:857, Ch.10, §9–§16), addresses compensations for long-term interruptions, which directly constitutes a possible cost for the DSO. The interruption compensation is directed to each affected customer. The compensation increases as a step function with the first step at 12 hours and 12.5% (or 900 SEK, whichever higher) of the yearly tariff and then a new step every 24 hours with a 25%-point increase (or 1800 SEK per step, whichever higher), reaching a maximum of 300% of the yearly tariff after 288 hours. This regulatory tool puts focus on single interruptions and the areas of the grid that are in larger need of attention. As from the year of 2011 a DSO is also responsible for making sure that an interruption is not longer than 24 hours (Ellag 1997:857, Ch.3, §9), i.e. a functional demand that asserts that the DSO supplies a certain level of function. The penalty for not fulfilling this requirement is not clearly defined in the act.

The NPAM and the interruption compensation tools give a positive correlated effect on improvement of quality of supply, opening the possibilities of larger revenue in the same time as the cost of compensations to customers goes down, subject to the constraint that the theoretically calculated quality of supply in NPAM is valid. The framework surrounding the mandatory risk and vulnerability analyses is not yet set, but in order to become a useful tool SEMI will probably associate failure to fulfill the requirements with some sort of fine. The analyses provides SEMI with a tool that ensures that DSO:s have a focus on reliability in their grid and necessary improvements in order to ensure customers a certain level of quality of supply.

Since the requirements for the risk and vulnerability analyses are not yet set by SEMI, there is room for interpretations of the requirements regarding the report the DSOs have to submit to SEMI. There are two requirements stated in the act: 1) a risk and vulnerability analysis regarding security of supply for the electricity network and 2) a mitigation plan that depicts how the security of supply will be improved. Furthermore, the act also states that the network operators should inform customers of their security of supply. The modifications affect those companies who operate networks with voltages below 220 kV, i.e. sub-transmission operators and DSOs. As stated above the failure to meet these requirements will probably result in a fine (STEM, 2005). The two requirements together form the basis of a risk and vulnerability management approach, which is the main focus of this paper. How these regulations interplay and the impact for DSOs is further discussed in section 5.

3. DEFINING RISK AND VULNERABILITY

The concepts of risk and vulnerability can be seen as different perspectives addressing the same issue, i.e. evaluating and understanding the impact of hazards and threats.

In accordance with Kaplan & Garrick (1981) the quantitative risk for a technical system can be analysed by answering the three questions:

1. "What can happen?"
2. "How likely is it that that will happen?"
3. "If it does happen, what are the consequences?"

By answering the three questions for a specific scenario, the risk can be quantified for that scenario. In order to assess the total risk, *all* possible scenarios have to identified and quantified. In theory this may seem like a simple task, but in practice it is not as easy and requires both extensive knowledge of the system and skill of how to perform the analysis. Especially the issues of completeness, i.e. identifying all or close to all possible scenarios that could happen in the system, and the issue of correctly assessing the consequences and the likelihood are of greatest concern for the validity of the analysis. For a description of risk terminology and different risk assessment methods, see IEC (1995).

One of the arguments against risk analysis is that it tends to focus on the identification of hazard, and thereby mitigation strategies against the hazards, and not making the system less vulnerable to the hazards (e.g. McEntire, 2003 and Haimes, 2006). Vulnerability has some differing denotation and meanings in the literature. Many definitions explicate vulnerability as the system's overall susceptibility to loss due to a negative event, i.e. the magnitude of the damage given a specific strain, and that it should be related to a specific hazardous event (e.g. Dilley and Boudreau, 2001). The authors share this view in conjunction with the view that vulnerability should be regarded as a property that arises from the possible vulnerable states of the system (Haimes, 2006).

The N-1 criterion, often used in the design of electrical power systems, can be seen as a vulnerability criterion. The N-1 criterion states that the system should tolerate the failure of any component regardless of what caused it to fail, and still maintain its function, i.e. deliver electricity to customers. The strain to the system, stemming from a hazard or threat, is thus one component failure. The vulnerability for one component failure is then described by all the possible scenarios (possible states of the system) and the consequences for each of these. The system is not vulnerable to the strain, i.e. one component failure, if not any of the scenarios give rise to any consequences.

If the system is vulnerable, then combining the vulnerability with the probability of a hazard or threat exploiting the vulnerability, e.g. the likelihood of that component failing, yields the risk. Vulnerability analysis, as presented here, is thus a concept to be used as a complementary part to risk analysis. Since vulnerability analysis takes another point of view in comparison to risk analysis, i.e. identifying vulnerable states of the system in comparison to identifying threats and hazards to the system, it is argued that they complement each other.

It may not be appropriate to define risk as "probability *times* consequence", as is often done; since according to such a definition, low consequence, high probability scenarios (e.g. low amount of customers affected but frequent) and high consequence, low probability scenarios (e.g. high amount of customers affected but infrequent) would be equated, given that the two scenarios result in the same risk in accordance with the definition. However, the preferences from a societal and a system owner point of view might be different. For example, there might

be aversion to high consequence, low probability events, requiring another weighting function when comparing risks, which takes this preference into account.

The benefit of performing a vulnerability analysis is that it forces the analyst to describe the system and the states for which adverse effects might arise. The focus of the analysis is thus shifted towards the system and its resilience and robustness and away from the tendencies of only identifying threats that could affect the system in a harmful way. By only focusing on risk, and omitting the analysis of vulnerabilities, there might be a tendency to focus on hazards and threats and the likelihood for the occurrence of these, thus missing inherent vulnerable properties of the system. The approach of firstly focusing on vulnerable states of the system might very well be a fruitful one when it comes to identifying risks and vulnerabilities.

4. RISK AND VULNERABILITY MANAGEMENT

Risk and vulnerability management consists of two integral parts: risk and vulnerability assessment and risk and vulnerability mitigation (e.g. Haimes, 2006; IEC, 1995), see Figure 2.

In the assessment part questions like these are asked: What is the system vulnerable to? What can go wrong? How likely is it that that happens? What will the consequences be? In this part relevant vulnerabilities and risks are thus identified. In the mitigation part questions like these are asked: What should be done? What can be done and what options are available? What are the tradeoffs for different options regarding costs, benefits and risks? What are the impacts of current decisions on future options? For this part the focus is on considering and implementing remedies against the identified vulnerabilities and risks that exceed acceptable levels.

Risk and vulnerability management can be an effective tool of managing, planning and operating electrical distribution systems. If correctly performed it gives the means to successfully address different vulnerabilities and risks that could affect the security of supply, stemming not only from a technical point of view but also incorporating organizational issues.

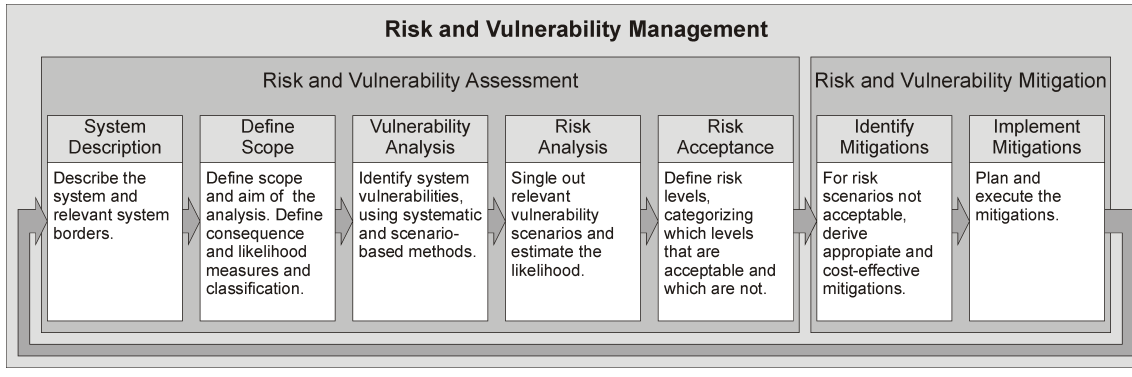


Figure 2. Risk and vulnerability management consists of two integral parts: Risk and Vulnerability Assessment and Risk and Vulnerability Mitigation.

Risk and Vulnerability Assessment

The aim of the assessment it to identify relevant risks and vulnerabilities in a predictive manner, especially those not easily identifiable. Plotting the cumulative number of events versus consequence for both natural disasters and man-made systems, normally, yields a power law distribution (e.g. Amin, 2004), see Figure 3. The figure illustrates that incidents with small negative consequences tend to have a higher frequency of occurring, and incidents with large negative consequences tend to have a much lower frequency of occurrence. For electric distribution systems this corresponds to relatively frequent but with a limited power and outage time (normally easily identifiable in yearly metrics such as SAIDI and SAIFI) in contrast to seldom but with widespread and prolonged power outages (such as the effects of the storm Gudrun and the transmission system outage in Sweden 2003).

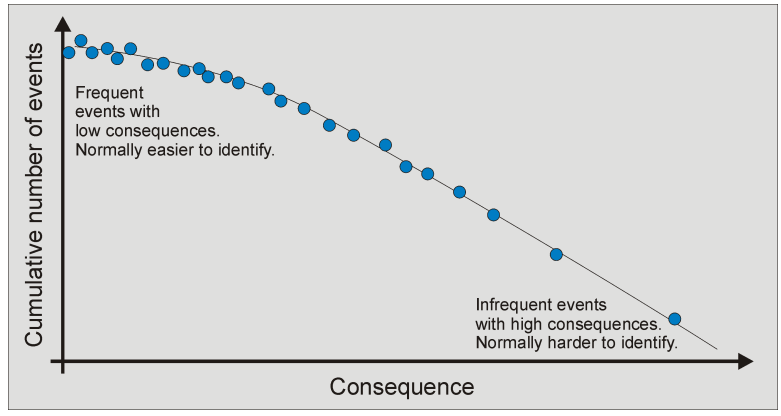


Figure 3. Illustration of the power law distribution of cumulative events and consequences found for both natural disasters and man-made systems.

The risk and vulnerability assessment part begins with defining the system, the aim, and the scope of the analysis. The scope and detail of the analysis should be proportional to the scope and detail of the mitigation activities. At the same time the scope should also correspond to the expectations of customers, enforcing authorities and the resources of the DSO. Should the analysis be performed only for the MV-network, or also for the LV-network? At what operating state should the analysis be performed, summer condition or winter condition? Should several operating states be considered? Should organizational issues such as securing the availability of repair resources be addressed? Questions like these must be answered in order to concretize the validity of the analysis. It is important to decide the detail level of the analysis in order for it to correspond to the detail level in the mitigation phase. Furthermore, the analysis should be transparent and flexible enough so that it can be iteratively refined and expanded, e.g. starting with a more rudimentary risk and vulnerability analysis with the aim to improve it on, say, a yearly basis. Another important part of the scope is to define the consequence measure so that it reflects the actual value at risk for the DSO and fulfills the requirements, if any, set out by the enforcing authority. For distribution systems several measures are possible to use in order to describe the consequences: customers not supplied, type of customer, power not delivered, interruption time, energy not supplied, cost of interruption for customer, cost of interruption for DSO and so forth. The basic three consequence measures that should be considered are: number of customers not supplied, power not supplied and interruption time since from these it is possible to derive other desirable consequence measures in further in-depth analysis, for example energy not supplied.

In order to more readily classify and communicate different types of risks and vulnerabilities it might appropriate to derive frequency and consequence classifications. The frequency classification could for example be: 1 event per 1000 years, 1 event per 100 years, and 1 event per 10 years, yielding three discrete classes. The consequence classification could for example be: less than 1 MW or less than 1 hour interruption, 1-10 MW or less than 12 hours interruption, and above 10 MW or above 24 hours interruption. These kinds of consequence classification thus take several fundamental consequences into consideration. It is also possible to add monetary values. It is however important that the consequences in each class is considered comparable and that the number of classes is sufficiently large in order to clearly differentiate between different levels of risk at the end of the assessment process.

The vulnerability analysis aims at identifying system vulnerabilities that could lead to adverse effects. In order to most easily systematically evaluate how vulnerable the network is for different type of strains, a model of the system is necessary. All relevant aspects of the network, with the aim and scope of the analysis in mind, should be incorporated in the model, such as network structure, power rating of transformers and location of customers. The model is then used to perform a systematic vulnerability analysis regarding the security of supply by systematically removing components and estimating the consequences (see Johansson et al, 2007; Jönsson et al, In Press). Components can be removed one and one or several simultaneously in order to identify vulnerable states of the system. An analysis of three simultaneously removed components, for a distribution system consisting of 500 components, yields over 20 million scenarios, many of them with relatively low consequences. Such an analysis thus tries to identify a large amount of possible contingences that could affect the security of supply, i.e. addressing the issue of completeness as described in section 3. The results will highlight the strains that give rise to large consequences, i.e. identifying the systems vulnerability to those strains. The systematic vulnerability analysis focuses on direct strains that affect the electrical distribution network. It is also necessary to highlight other vulnerabilities such that could stem from organizational or a natural hazard perspective, which is most easily done by conducting a structured discussion meeting with personnel from the DSO. The focus of the meeting is to identify strains, not included in the systematic analysis, which could affect the security of supply. The vulnerability analysis thus results in a list of scenarios that, if they occur, will lead to consequences of varying magnitude.

Next step is to put likelihood into the equation, i.e. going from the vulnerability analysis to the risk analysis. First a screening of the identified vulnerability scenarios should be conducted, trying to single out the scenarios of greatest interest for further studies. This screening can be done both based on the consequences and on a first notion of the probability of the scenario occurring. For example it might be feasible to only further investigate those scenarios with a consequence that exceeds a certain threshold. Likewise, some scenarios are so extremely unlikely to occur that they can be assigned a minimal probability of occurring, thus not necessary for in-depth analysis in the risk analysis phase. Nevertheless, they should be highlighted if the associated consequences are not negligible. The screening of vulnerability scenarios is a very delicate phase of the analysis, since the aim is to reduce the number of scenarios for further analyses and at the same time not discarding scenarios that might potentially yield a high level of risk.

The remaining vulnerability scenarios after the screening process are subject to more in-depth estimations of the likelihood of occurrence. There are several possible sources of knowledge available in order to estimate the probability of a scenario occurring. The DSO's expert knowledge of the system should be inherent in any analysis. Complementary information sources to use are generic fault statistics (e.g. He, 2007) and, if available, other sources of information such as incident reports and status inspection of equipment. The span of

frequency should be sufficiently wide to include incidents of low frequency of occurring, e.g. 1 per 1000 year, to high frequency of occurring, e.g. 1 per year.

Both the estimation of consequences and the estimation of likelihood for any given scenario should be coupled with a metric describing the uncertainty of the estimations. These metrics are important to clearly single out scenarios that possibly could lead to higher consequences and have a greater likelihood of occurrence. If the risk is not negligible, these scenarios should be subject to further in-depth analysis in order to reduce the uncertainty. If it is not possible to reduce the uncertainty to a desirable level, they should be treated as potential high-risk scenarios.

Up to this stage, relevant vulnerabilities and risks, with regards to the defined scope of the analysis, have been identified by using a systematic and transparent approach. The next step is to define risk acceptance levels, i.e. defining what risks are acceptable and which are not. Risk acceptance is closely interlinked with the costs and benefits that come with the risk, and must thus be considered when defining the acceptance levels (e.g. Kaplan & Garrick, 1981). For DSO's some guidance is given by the regulatory context, as discussed in section 2.

Risk and Vulnerability Mitigation

It is possible that the analyses reveal that there are no unacceptable risks for the system at hand, which is by itself very valuable information. Most likely, though, risks will exist that are identified as not acceptable. For these risks, mitigation strategies with the aim to reduce the risk have to be developed. These mitigation strategies can reduce either the consequence or the likelihood, or both, in order to bring the risk to an acceptable level. There is usually several possible ways to reduce the risk, which can be compared by carrying out a cost-benefit analysis in order to derive the most cost-effective solution for reducing the risk. It is also possible to derive the most cost-effective solutions for reducing the total risk of the system, bearing in mind that this puts requirements on scenario disjointness as put forward by Kaplan et al (2001).

The last step of the risk and vulnerability management process, and the most important, is to plan and implement the identified risk mitigating solutions. The prior analysis should be used in order to determine a suitable order of implementation. The cost analysis can be used in this step to schedule an appropriate level of investments. The mitigations should be carefully documented and updated, in order to be useful as input in the iterative risk and vulnerability management process.

The proposed risk and vulnerability management (RVM) process, with respect to sequence and content, can prove to be an effective decision support tool for managing distribution systems. The approach, if properly conducted, yields a tool that can encompass both technical and organizational vulnerabilities and risks facing the utility. It also offers a tool for schedule planning and economic investment planning of cost-effective risk and vulnerability mitigations. The results from the analysis and the management process are also very useful when addressing awareness of the distribution systems capabilities to withstand strains to authorities and to the public, which is an important aspect.

5. DISCUSSION

The key performance issue for a DSO is coupled to interruptions of the supply of electricity to its customers, since many economic risks are present here. If the DSO opts to focus on reducing theses risks, the RVM scheme offers a systematic support tool in identifying and choosing which actions to take.

A key feature of the RVM is the systematic structure and content of the steps in the process, see figure 2, making it repeatable and, depending on how different steps are performed, flexible in order to fit the progress of the company and company needs. Another benefit in using RVM for Swedish DSOs is the legislative demand for reporting the results of the analysis together with a mitigation plan to SEMI. In order for the RVM scheme to be an effective tool it should encompass both technical and organisational aspects of operations, relevant to the security of supply. It is also possible to use the scheme for the identification and management of other organisational risks. The well-defined structure also allows easy division of required work and splitting up problems into smaller sub-problems without loosing the overall aim and structure of the management process.

A well-structured documentation of the network and its components is a requirement to yield the best possible result. This requirement may seem hard to fulfil, but it can also work as an incentive for acquiring and documenting the information, which very well may benefit other areas of the business.

Risk and vulnerability management is, as previously stated in the article, a part of the legislation affecting the electrical distribution market. The penalties for 12-hour interruption and the constraints from the NPAM on the key performance indicators SAIDI[2] and SAIFI[3] also significantly affect the market. These tree tools together define in which way SEMI can steer the electricity distribution market. The penalty for interruption is a direct way for lifting the lower level of quality of supply and limiting long interruptions. The tool steers the DSO towards a higher quality of supply for *all* customers. The NPAM provides a tool more directed towards improving the overall quality of supply for a network in proportion to the cost efficiency of the DSO. The parameters in the NPAM are more focused on cost efficiency, but nevertheless it does set a limit where quality of supply improvement is no longer beneficiary for the DSO. Up to this level however the NPAM puts a revenue premium on improving the quality of supply, were as the penalties for interruption only can be an avoided cost for the DSO. To gain best possible internal benefit from the RVM for the DSO it is important to consider the impacts of these regulatory constraints when defining the acceptance levels for risks. Other important inputs when defining acceptance levels are total internal cost, in perspective of the customers' expected level of quality of supply.

The functional requirement of no customer interruptions longer than 24 hours, coming in to force 2011, will set a minimum acceptance level for quality of supply for individual customers. The NPAM will forcibly set another acceptance level, based on the inherent parameters in the model regarding cost and reliability of supply, for the overall quality of supply for the DSO. The penalties regarding customer interruptions longer than 12 hours must also be accounted for in order to derive an appropriate acceptance level. The acceptance level regarding interruption costs may very well vary between different DSOs, depending on their

---

[2] System Average Interruption Duration Index

[3] System Average Interruption Frequency Index

risk preferences. How to define clear acceptance levels is thus an important question, without an easy answer. How these regulations interplay and their effect of managing distribution systems are not easily concluded and hence require further research and investigations, and succinctly lies outside the scope of this article. The interaction between NPAM and acceptance levels for RVM, the penalties coupled to customer interruptions together with the function requirement will be at the centre of this work.

Acceptance levels derived from unison definitions encompassing the whole horizon of the DSO operations will provide an objective base in defining risks. An objective measure of risk allows decision makers to compare different investment alternatives, both between organisational and network structure development, making it useful tool in the decision process in general. As previously stated the RVM is useful in many aspects of the enterprise and can be utilized in many levels of the organisation in order to both support decisions and to derive correct actions from a holistic point of view. With an appropriate definition of scope and granularity of the assessment, the identified risk scenarios will directly point out where the problems are and what type of mitigating efforts to consider. For a larger organisation it is possible to identify which part of the organisation or person who should be appointed problem owner and responsible for suggesting and implementing possible mitigations, an important aspect for an effective management scheme. With a wider scope of the analysis, incorporating both the technical network as well as organizational aspects it is possible to compare these risks and thus deriving the most cost-effective mitigating effort.

From a regulatory point of view it should be of interest that the reports from different DSOs share the same scope and classification system of frequency and consequence. This is the basic prerequisite in order for the regulating authority to readily compare the risks each of the DSOs has identified. What type of classification system to utilize for this purpose is outside the scope of the present paper and should thus be a subject for further research.

6. CONCLUSIONS

In the present paper a discussion of risk and vulnerability management for DSOs has been presented. The regulatory context regarding electrical distribution system consisting of risk and vulnerability management, NPAM, and recent changes to the Electricity Act, and how they interplay, has also been discussed. Furthermore, a rather thorough description of how to conduct and benefit of risk and vulnerability management at a DSO level and important issues thereof was presented. Risk and vulnerability management can be an important decision support tool for the management of electrical distribution systems, if correctly performed. Important issues subject to further research is to clarify exactly how the regulatory tools interplay and their overall effect regarding the management of distribution systems and, from a regulatory point of view, what scope for the analysis and classification of risk to be used in order to more easily compare risks for different DSOs in a transparent manner. Another important issue subject for further research is the definition of appropriate risk acceptance criteria.

7. ACKNOWLEDGEMENT

This research has been financed by the Swedish Emergency Management Agency, which is greatly acknowledged. Furthermore the support from Grontmij AB and SWECO Energuide AB are also recognized. The authors also express their gratitude to Associate Professor Olof Samuelsson and Tekn. Lic. Henrik Jönsson for their valuable comments.

8. REFERENCES

[1] Amin, M., (2004). Balancing market priorities with security issues, *Power and Energy Magazine*, IEEE, Vol. 2, No. 4, pp. 30-38.

[2] Dilley, M., Boudreau, T., (2001). Coming to terms with vulnerability: a critique of the food security definition, *Food Policy*, Vol. 26, No. 3, pp. 229-247.

[3] Haimes, Y. Y., (2006). On the Definition of Vulnerabilities in Measuring Risks to Infrastructures, *Risk Analysis*, Vol. 26, No. 2, pp. 293-296.

[4] He, Y., (2007). Distribution Equipment Reliability Data, *Elforsk rapport 07:59*.

[5] IEC (International Electrotechnical Commission), (1995). Dependability management - Part 3: Application guide – Section 9: Risk assessment of technological systems, *International standard 60300-3-9*.

[6] Johansson, J., Jönsson, H. & Johansson, H., (2007). Analysing the Vulnerability of Electric Distribution Systems: a Step Towards Incorporating the Societal Consequences of Disruptions, *International Journal of Emergency Management*, Vol. 4, No. 1, pp. 4-17.

[7] Jönsson, H., Johansson, J. & Johansson, H., (In Press). Identifying Critical Components in Technical Infrastructure Networks, *Journal of Risk and Reliability*.

[8] Kaplan, S., Garrick, B.J., (1981). On the quantitative definition of risk, *Risk Analysis*, Vol. 1, No. 1, pp. 11-27.

[9] Kaplan, S., Haimes, Y., Garrick, J., (2001). Fitting Hierarchical Holographic Modeling into the Theory of Scenario Structuring and a Resulting Refinement to the Quantitative Definition of Risk, *Risk Analysis*, Vol. 21, No. 5, pp. 807-819.

[10] 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*, Vol. 1, No. 3, pp. 298-308.

[11] Solver, T., (2005). Reliability in Performance-Based Regulation, *Licentiate Thesis*, Electrical Power Systems, KTH.

[12] STEM (Statens Energimyndighet), (2005). En leveranssäker elöverföring, *ER 2005:19*, ISSN 1403-1892.

IV

ASSESSING RESPONSE SYSTEM CAPABILITIES OF SOCIO-TECHNICAL SYSTEMS

Alexander Wilhelmsson

Lund University, LUCRAM, Sweden [1]

Jonas Johansson

Lund University, LUCRAM, Sweden [2]

Keywords

Critical Infrastructures, Socio-Technical, Resilience, Response System, Railway

Abstract

Our society is becoming more and more dependent upon the reliable function of a number of vital socio-technical systems. These systems are often being referred to as critical infrastructures, or lifeline systems, indicating their importance for supporting a nation's economy and social well-being. In the present paper a method is presented for assessing the capability of those actors involved in restoring socio-technical systems after strains affecting its technical systems. Parallel ongoing work by the authors, not presented here, emphasises on technical systems' interdependencies. Together, these approaches address the issue of vulnerability analysis of socio-technical systems. The presented method is derived from the theories of both systems thinking and resilience engineering. The method has been applied in a preliminary study of a socio-technical system, namely the Swedish railway system. The method systematically identifies the system elements by evaluating the system both under normal operation and under strain. The actors directly involved in the restoration of the technical system, referred to as the response system, are identified and selected for in-depth studies. The overall objective of the study is to assess the time required for the response system to restore the technical system after strains of varying magnitude, by introducing the concept of response curves. The curves reveal response system capabilities and their limits, i.e. the magnitude of strain for which the actors can no longer cope. It is concluded that the proposed method is both applicable and valid in the efforts of assessing response system capabilities of socio-technical systems.

Introduction

The society is becoming more and more dependent upon the reliable function of a number of vital systems, e.g. electrical power, telecommunications, water supply, banking and finance, and information technology (e.g. de Bruijne and van Eeten, 2007; Rinaldi et al., 2001). These systems are often being referred to as critical infrastructure systems or lifeline systems (McDaniels et al., 2007), indicating their importance for supporting a nation's economy and social well-being (Little, 2004). The increasing demands for flexibility and availability have

1 Department of Fire Safety Engineering and Systems Safety
LTH, Box 118, SE-221 00 Lund, Sweden Tel: +46 (0)46 288 09 39
e-mail: alexander.wilhelmsson@brand.lth.se Fax:+46 (0)46 222 46 12
2 Department of Industrial Electrical Engineering and Automation (IEA)
LTH, Box 118, SE-221 00 Lund, Sweden Tel: +46 (0)46 222 31 05
e-mail: jonas.johansson@iea.lth.se Fax:+46 (0)46 14 21 14

lead to continuous improvements of the efficiency of critical infrastructures. However, as a result of the increasing efficiency under normal operations, the infrastructures are becoming more and more interdependent (e.g. Amin, 2001; Stoop and Thissen, 1997), i.e. mutually dependent on one another. Because of these interdependencies, failure in one system can propagate to other systems leading to so called cascading failures (e.g. Little, 2002; Rinaldi et al., 2001), and result in not so easily foreseeable vulnerabilities.

Much of the complexity characterising critical infrastructures depends on the interactions between physical networks and actor networks, that "collectively form an interconnected complex network where the actors determine the development of the physical network, and the physical network structure affects the behaviour of the actors" (Verwater-Lukszo and Bouwmans, 2005, p.2379). Critical infrastructures can therefore be described as socio-technical systems. The approach presented in this paper, together with ongoing research by the authors focusing on vulnerability studies of the technical aspects of socio-technical systems, constitutes a comprehensive approach for assessing vulnerability of such systems.

A recent example illustrating the vulnerability of the railway system is an incident occurring during rush hour on October 15 2008 when a train between Malmö and Lund, Sweden, tore down a traction power line. Although a minor strain, it resulted in severe delays for all trains in the region, affecting thousands of travellers. Hundreds of passengers on board the trains were not allowed to evacuate because of the uncertainty whether the traction power was shut off or not. Passengers had to wait for about 4 hours before they were evacuated, which according to the Swedish Rail Administration is believed to depend on a lacking communication between those actors responsible for restoring the system. Hence, the consequence for the system as a whole is highly dependent upon the capacity and performance of these actors restoring the system. The example highlights an important aspect in assessing the vulnerability of a critical infrastructure; the system's ability to return to normal operation after different types and magnitudes of strain. The method presented in this paper aims at assessing this ability.

From a crisis management perspective the aim of the research is to give guidance in the mitigation and preparedness phases, i.e. appropriate actions and activities before an accident occurs in order to mitigate the likelihood and/or the consequences of an undesired event.

Analysis of socio-technical systems from a systems thinking approach

There are several problems with undertaking a study of a socio-technical system, mainly due to the large number of actors and technical elements involved. In order to take all relevant aspect and interdependencies characterising such complex system into consideration, it is the authors' opinion that the system's vulnerability should be analysed from a systems thinking standpoint.

Much of the emergency response and disturbance management are in the hands of different operation and maintenance actors, and it is therefore not fully satisfying only taking the technical aspect into consideration when assessing the vulnerability of technical infrastructures (e.g. Appicharla, 2006). Thissen and Herder (2003) argues that methods that can handle the socio-technical nature of infrastructure systems, enabling analysis from different perspectives, should be developed. According to Little (2005), analysis of the relationships between technology, people and organisations that are required to provide continued function of our vital infrastructure systems should be based on a holistic approach, which is a view shared by the authors. Furthermore, systems that consist of large numbers of elements and relations, with nonlinear interactions, time delays and unintended feedback loops that can lead to unpredictable behaviour are referred to as complex systems (Axelrod and Cohen, 2000). Thus, the socio-technical systems that are emphasised in this study can be viewed as complex systems in accordance with the definitions given above. In an effort towards taking all these aspects into consideration, the use of ideas from the area of systems thinking is advocated.

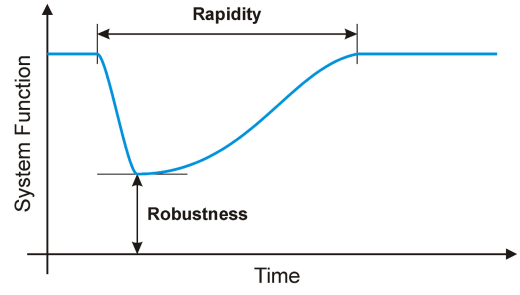
The fundamental idea behind systems thinking is to study systems as wholes rather than their elements in separation, in order to address complexity (Checkland, 2006). A system is defined as a number of elements with relations between these elements, forming a whole. A system boundary represents the distinction between what is part of the system and what is part of its environment, and the boundary must be defined with respect to the elements that have an influence on the problem situation being studied (Jackson, 2000).

Resilience engineering

Resilience engineering is broadly about creating ability for complex systems (e.g. socio-technical systems) to recover after being exposed to strain. This is in line with the purpose of the present study, therefore ideas from the area of resilience engineering is used. Resilience is described by Hollnagel et al. (2006, p.4) as "the ability of systems to anticipate and adapt to the potential for surprise and failure". However, as resilience engineering is a discipline under formation, numerous definitions of the concepts can be found in the literature, and according to Westrum in Hollnagel et al. (2006, p.65) the concept is "a family of related ideas, not a single thing". Another way of describing resilience is as a "[complex system's] capacity to absorb shocks while maintaining function." (McDaniels et al., 2008, p.310). This definition is adapted by the authors. For a more thorough overview and use of the concept of resilience, see e.g. Hollnagel et al. (2006).

McDaniels et al. (2008) refers to two key properties for describing resilience: robustness and rapidity, see Figure 1. Robustness refers to a system's ability to withstand a certain amount of stress without suffering degradation or loss of function. Rapidity refers to a system's speed of recovery of function from an undesired event and back to a desired level of function. McDaniels et al. (2008) also point out that resilience can be improved by both ex-ante and ex-post decision-making, stemming from both risk mitigation activities undertaken before an incident and response activities taken following the incident. Vulnerability is here seen as an antonym to the two aspects of resilience emphasised by McDaniels et al., i.e. a low degree of vulnerability corresponds to a high degree of robustness and rapidity. It is hence the authors' view that risk and vulnerability analysis are useful tools in the efforts to design more resilient systems.

Figure 1. Resilience curve for a system affected by strain. The inverted loss of system function is a measure of the robustness, and the system's speed of recovery to a desired system function is a measure of the rapidity (Figure based on McDaniels et al., 2008).

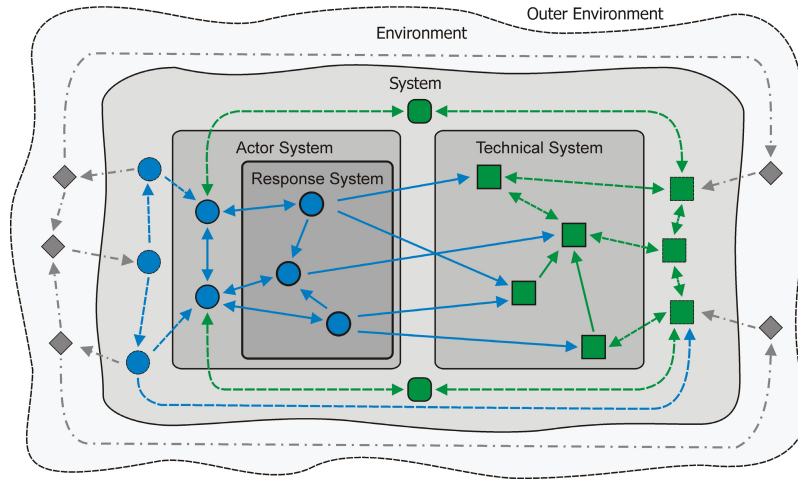


Method for identifying response system capabilities

As a first step for assessing the response system capability of a socio-technical system, corresponding to the rapidity aspect in accordance with the concept of resilience discussed in the previous section, the elements and interdependencies characterising the system must be fully described by the creation of a system model. The system model enables the identification of elements and relationships that are critical in many types of studies. The presented method is generic, and can therefore be used for different types of socio-technical systems. Later in this paper, a preliminary study is described where the method has been applied to a section of the Swedish railway system.

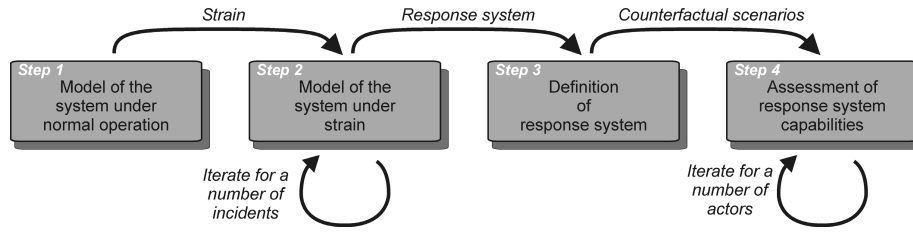
An important aspect of the system model is to explicate system boundaries. A system can be seen as an element of a larger system, and likewise, an element of the system can be decomposed into a number of smaller subsystems depending on the frame of reference. Therefore, when looking at the world in terms of systems, a number of hierarchical levels can be identified depending on the resolution of the study (Skyttner, 2005). Consequently, a consideration of the appropriate level of abstraction is essential (c.f. Rasmussen, 1985) when constructing a system model. In our general system model, four significant system boundaries can be identified. The first one is between the outer environment and the environment; this system boundary reveals what is regarded as possibly influential to the system behaviour and what is regarded as non-influential. The second system boundary is between the environment and the system, defining which parts that are regarded as part of the system and which parts that is regarded as possibly influential to the system behaviour. The socio-technical system is then divided into two subsystems, the actor system and the technical system, which are distinguished from the system by defining those elements that directly supports the function of the system. In addition, a fifth system boundary is defined with respect to the aim of the present study. This border is defined between the actor system and those actors that are directly involved in restoring the technical system under strain, i.e. the response system. For other methods focusing on response systems from a systems approach see e.g. Uhr et al. (2008).

Figure 2 Schematic view of a socio-technical system.



The method involves a systematic approach for identifying those actors who have a direct impact upon the restoration of the technical system. These actors are referred to as the response system and constitute a subset of the actor system, see Figure 2. The method for mapping the system, steps 1 and 2, and identifying and assessing the capability of the response system, steps 3 and 4, is described in Figure 3. The method involves iterative processes in order to capture all the relevant aspects of the system. Steps 3 and 4 can be substituted depending on the aim of the study.

Figure 3. The four steps forming the method.



Step 1. Model of the system under normal operation. The first step for assessing the response system's capability is to construct a model of the system under normal operation. This is achieved by identifying those elements that are considered most important for the purpose of the study, i.e. those elements that interact to produce the behaviour that is subject for investigation (Jackson, 2000). Although it is the response system that is in focus in the present paper, it is important to map a larger part of the system, since the actors are both highly interconnected with each other and connected to the technical part of the system. The main reason for the construction of a model of the system under normal operation is that the model facilitates the understanding of the system's behaviour (Jackson, 2000), and that it functions as a common mental model of the system for the participants in a study (c.f. Senge et al., 1994).

Step 2. Model of the system under strain. In this step an incident, e.g. some type of strain affecting the technical system, is described. Depending on the type and magnitude of strain affecting the system, the incident described may result in some degree of loss of the system's function. The actors necessary for restoration of the technical system are identified, and added to the actor system in the model that was created in step 1. A number of incidents are described through an iterative process, and for each incident additional actors are added to the system model. For each new incident, the number of actors that has not been identified in previous incidents will decrease and eventually reach zero, whereby the mapping process is considered complete.

Step 3. Definition of response system. Those actors that play an active part in the restoration of the technical system are referred to as the response system and constitute a subset of the actor system. The boundary between response actors and other actors, identified in step 2, is distinguished by the means of a definition of the response system. The response system is here defined as those actors who either have a professional role in restoring the system, or those who facilitate the restoration by carrying out actions that are directly aimed at restoring the system. It should be noted that under normal operation most of the response system is usually seen as a latent part of the system, i.e. most of the response actors do not have an active role in the system under normal operation, but become involved as the system deviates from this desired normal state.

Step 4. Assessment of response system capabilities. The overarching purpose of the present paper is to study the way that the system is restored and brought back into normal operation after being affected by strain. Thus, this step focuses on the response actors and in quantifying their capability, basing our view of response system capability in accordance with Jönsson et al. (2007). Since the system as a whole is known, the relationships that directly or indirectly may influence the response actors' capability are taken into account. By systematically running through incidents and counterfactual scenarios, the time for restoration given different types and magnitudes of strain affecting the technical system can be assessed. This information is used for creating response curves, which are more thoroughly discussed in the next section.

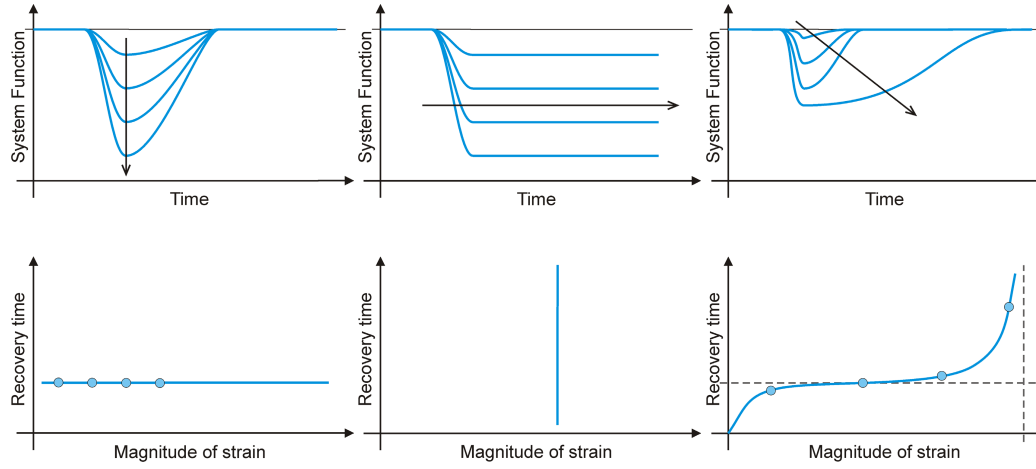
Response curves

The time required for the technical system to recover is highly dependent upon the response actors' ability to restore the system after strains of varying magnitude. This corresponds to the rapidity aspect, illustrated in Figure 1. In contrast to the system mapping that was carried out by qualitatively identifying elements and relations, the study of the response system addresses the issue of quantitatively assessing capabilities. For this estimation, some of the real incidents, which were used as a basis for the system mapping in the previous section, are here used as a starting point. The real incidents are used for developing hypothetical scenarios, using what Abrahamsson et al. (2008) refers to as counterfactual scenarios. Counterfactual scenarios are variations of real incidents. For example, in the case of a railway system the real incident could involve a derailment of one car; then a counterfactual scenario may be derailment of two cars. The counterfactual scenarios are then used to assess actors' ability of

repairing the technical system, and more specifically to estimate recovery times, with the main interest in finding the limit of the actors' capabilities.

For the representation of the recovery times, the authors introduce the concept of response curves. In general, a response curve depicts the time it takes to restore a system with respect to varying magnitudes of strain. Naturally there will be different response curves for different types of strains and for different actors. Figure 4 depicts response curves and how they are closely related to the concept of resilience. Here the system function degradation and the magnitude of strain are assumed to have a linear relationship, i.e. that all magnitudes of strain result in a corresponding linear loss of function, in order to simplify the reasoning. In reality, the linear relationship might not always be true, for instance some systems may tolerate a certain level of strain before the system function is affected. The figures show two asymptotic extremes (a and b), and one realistic response curve (c). In Figure 4a) the capacity of managing increasing strains is sufficient, and the time for recovery is thus constant for all magnitudes of strains. In Figure 4b), there is insufficient capacity of managing increasing magnitudes of strains (or actually managing the strain at all), leading to longer restoration times, which is indicated by the vertical line in the response curve. In Figure 4c), the expected resilience curve for a real incident and the corresponding response curve with the two asymptotes sketched as dotted lines are presented. These asymptotes depict where the recovery time is unaffected (the horizontal line), and the border of the actor's capacity (the vertical line), given the strain. The awareness of these asymptotes simplifies the interpretation of real response curves with respect to the response system's coping capability and where a limit is reached.

Figure 4. Resilience curve (above) and corresponding response curve (below) for a) recovery time independent of magnitude of strain, b) infinite response time for different magnitudes of strain, and c) the expected resilience and response curves for real incidents.



a) b) c)

There are several benefits with the use of response curves. First of all, the response curves make it easier to identify at which magnitude of strain the response organisation will reach a critical point in terms of capacity for restoring the system. Secondly, by combining different actors' response curves for the same type of strain, it can be differentiated which actor that is or will become a bottleneck for handling the strain. Thirdly, the possibility to compare response curves for the same actor, but for different types of strain, gives an indication of what types of strains the actor has been designed to respond to.

An approach similar to our proposed response curves is discussed by Woods and Wreathall (2008). Their approach is based on an analogy with stress-strain plots in order to characterise an organisation's ability to handle increasing demands, which has been applied to an emergency department by Wears et al. (2008). Stress-strain plots, i.e. the kind of plots resulting from analysing material structures' ability to withstand increasing loads of strain, are

characterised by two regions; an elastic region and a plastic region. In the elastic region the material stretches uniformly under increasing strains, whereas in the plastic region the material fractures and a failure point is eventually reached. They argue that the same patterns can be identified for organisations under strain. The response curves presented in this paper aims at illustrating a similar type of relationship between increasing strain and demand as discussed by Woods and Wreathall (2008), but here applied to the response system's ability to restore a technical system after increasing loads of strain. However, we are interested in the shape of the curve and not only the elastic and plastic regions as included in their work, i.e. we are interested in how the ability of the response system changes with respect to a variety of magnitudes of strain and not only the identification of a failure point.

Empirical study of the Swedish Railway system

The method presented in this paper has been used in a preliminary study for a section of the Swedish railway system. The railway section is a 258 km long double track railway between the cities of Gothenburg and Hallsberg, and is highly important for the functioning of the Swedish railway transport system since it connects the two largest cities in Sweden, Stockholm and Gothenburg. The Swedish railway system is administrated and operated by the Swedish Rail Administration, which is also responsible for traffic management. The trains utilizing the railway infrastructures are owned and operated by private companies.

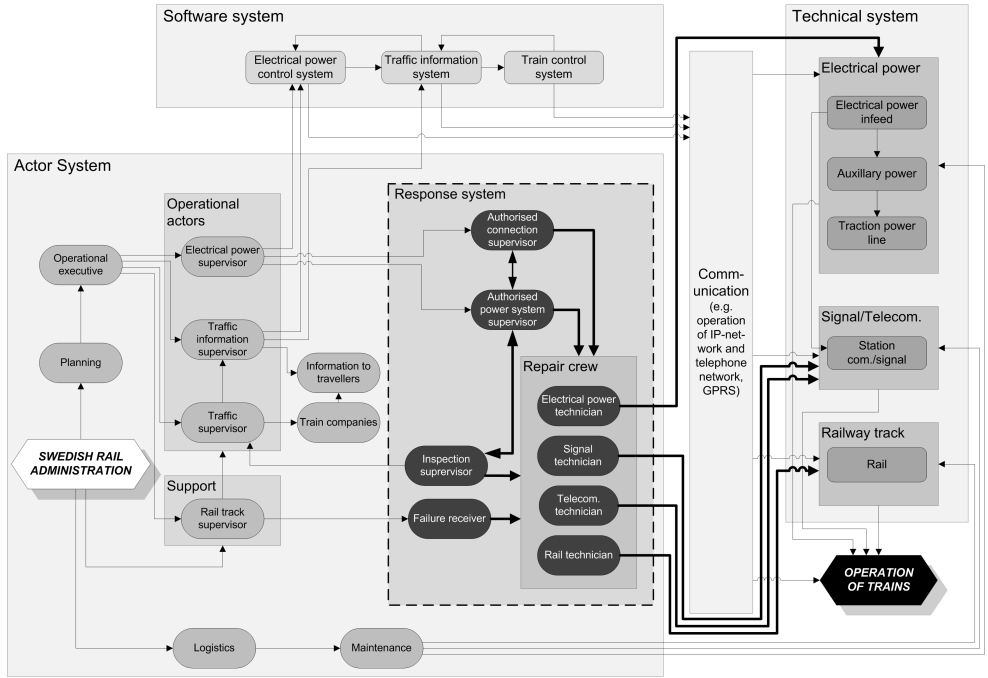
The empirical study was prepared by creating a record of incidents that have occurred on the railway section. These incidents were found by studying documentation of events that have lead to technical system degradations during the last three years. Since the number of incidents that have occurred on the specific railway section is limited, data from other incidents that have occurred elsewhere in the Swedish railway system was also included in this record. From this collection of data, relevant real incidents were categorized by type of event, magnitude of strain, affected technical system and restoration time, and were used to give an initial set of reference for the study.

The study followed the four steps, as illustrated in Figure 3, in a workshop session including 4 employees from the Swedish Rail Administration, representing different divisions within the company. The selection of the participants was based on two requirements: comprehensive view of the railway system and knowledge and experience from restoration of the technical railway system after incidents.

The first step, i.e. identification of elements (actors and technical systems) and their relations, forming the railway system under normal operation, was carried out after agreeing on the appropriate level of abstraction (c.f. Rasmussen, 1985). The identified elements and their relations were depicted in a system model, iteratively evolved until all participants agreed upon the acquired system model. The system model in this step broadly consists of the actors necessary for the normal daily operation of the railway system, the software management systems necessary for the operation as it is an interface between the actor system and the technical systems, and the technical systems required for the operation of trains.

The second step began by describing a real incident that has occurred on the studied railway section for the participants. The incident involved a strain consisting of a torn down traction power line, due to a tree that had fallen towards the railway track. Based on this description, the participants identified those actors who had been involved in the restoration of the technical systems. These actors and their relationships were added to the model of the system under normal operation, resulting in a model of the system under strain. The system model in Figure 5 consists of those elements and relationships that are necessary for the operation of the system both under normal operation and under strain. By using a systematic approach, the probability of accidentally excluding important elements and relationships in the next step of the study is minimised.

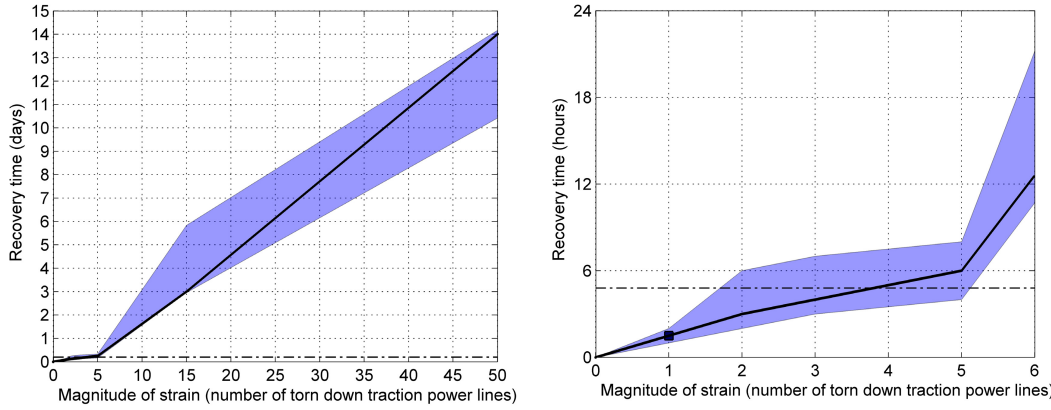
Figure 5. The system model for the system under strain. The Swedish Rail Administration is responsible for enabling a safe and reliable operation of trains. This requires operational actors, software management systems, and a technical infrastructure. In the case of a strain affecting the technical system, a response system is activated in order to restore the system to normal state of operation as quickly as possible.



Based on the definition of the response system given previously, a system boundary was drawn between those actors active under normal operation, and those actors who played an active role in restoring the system after the specific strain. In Figure 5, a dashed black border surrounds the response system. The response system consists of personnel responsible for on-site management and different types of repair crews.

After the identification of what constitutes the response system, the next step was to assess the response system's ability to restore the technical systems after strains, i.e. the construction of response curves. The incident used for the response system mapping, step 2, was then used as a basis for counterfactual scenarios. The counterfactual scenarios consisted of scenarios causing more strain on the traction power system, with respect to more traction power lines torn down. The participants estimated the response time for the counterfactual scenarios, taking into account resource capacities and other limiting factors. In Figure 6 the response curve from the preliminary study is presented. The figure shows the combined response curve for all the actors involved, i.e. it depicts the estimation of the time for the full recovery of all the technical systems for the given type of strain. In Figure 6a two clear regions can be identified, one between zero to five torn down traction power lines and one between five to fifty torn down traction power lines. The first region (strain zero to five) indicates were only the normal response teams for the given railway section is involved, and the second region (strain five to fifty) when response teams from other railway section are activated and utilised for the recovery of the technical systems. For the given maximum magnitude of strain, the response capacity of the entire Swedish Rail Administration is more than sufficient, resulting in the linear relationship with no apparent vertical asymptote that would reveal insufficient capacity of managing increasing magnitudes of strains. Figure 6b shows the response curve for the limited recovery time of up to 24 hours and the magnitude of strain of up to six torn down traction power lines. This figure more clearly reveals the capacity of the response system for the given railway section, and more significantly that there is an indication of a limitation of the response capacity when the magnitude of strain goes beyond five torn down traction power lines.

Figure 6. The response curve is a function of the estimated recovery time with respect to the magnitude of strain in a) from 0 to 50 and b) from 0 to 6 torn down traction power lines. The estimated most likely recovery time is shown as a black solid line, and estimated maximum and minimum recovery times are shown as a shaded field. The strain constitutes of trees falling on the railway section, tearing down traction power lines. The horizontal asymptote is a dashed black line. The base case incident is indicated as a black square in b).



a) b)

The preliminary study revealed that the approach of firstly mapping the system and then using response curves in workshop sessions with participants knowledgeable of the social-technical system under study is a sound approach. Further studies are required in order to draw more specific conclusions regarding the response systems' capabilities.

Discussion

The identification of elements and their relationships by using the systematic approach, based on systems thinking, results in a system model. This model is used in the present paper to draw a relevant system boundary around the response system. Due to the size and complexity of the system under study, it is nearly impossible to identify the entire system given a limited time frame. In the preliminary empirical study we therefore emphasised on mapping the technical system and the actors directly involved both under normal operation and under strain. The system mapping has two significant purposes; to make sure that all participants share a common mental model of the system under study and to facilitate the correct identification of the response system, including the relationships that can influence their behaviour. The application of the system mapping method, steps 1 and 2, during the workshop session confirmed the usefulness and strengthened our belief in the presented approach. However, in future studies it would be beneficial to cross-check the acquired system model with other employees from the Swedish Rail Administration. This approach would facilitate a way to test the validity of the acquired system model more stringently.

The response curves resulting from using steps 3 and 4 of the method reveal a number of interesting characteristics that can be valuable for preparedness planning of the response system capability of socio-technical systems. First of all, it is the authors' belief that most real response curves will have a region where the recovery time has a fairly linear relationship with increasing magnitudes of strain. In the most extreme case this region is a horizontal asymptote in accordance with Figure 4a. This region is important since it reveals the magnitude of strain for which the response system has a sufficient capacity, or, in other words, has been designed to handle. Secondly, at some magnitude of strain there is a point, or rather a region, where the response time drastically increases for a small additional increase of the magnitude of strain. In the most extreme case this region is a vertical asymptote as shown in Figure 4b. By including counterfactual scenarios with magnitudes of strain that are above those of normal, well known, incidents it is possible to identify this region. The region reveals where the response system reaches a limit for which it no longer can cope with the strain. The only remedy for this situation is if there is a possibility to use external capacity. Thirdly, a

region can be identified where a small initial increase in magnitude of strain will lead to an initial rapid increase in recovery time before a plateau is reached. This region indicates the time required before any restoration can be initiated, e.g. the time for transportation to the site, the need for a specific scarce type of resource in order to carry out the restoration, or the time for notification of response actors about the incident. Variations in the level of this plateau between different response actors and for different types of strain is valuable, e.g. for deployment or location of different actors and resources. The preliminary study revealed that two of these three significant indicators actually are present for real systems.

The response curves for different types of response actors and for different types of strains can be used for comparing and assessing for what types of strains there is appropriate capacity to handle and for which there is not, in a proactive manner before actual incidents reveal critical limitations. Such comparisons can also reveal where limitations can be expected due to a disproportional capacity for the restoration of different technical systems, and hence for which response actors additional resources should be allocated. Another important aspect of hypothetically testing response system capabilities is to reveal the importance of having sufficient capacities, which are unnecessary under normal operation but highly critical in the recovery from incidents. Consequently, the response curves can be used as a basis for decision-making regarding the adequate capacity for restoring the technical system after different types and magnitudes of strain.

Data collected from incident investigation reports often give an indication of the time required for restoring the system for a given type and magnitude of strain, and can therefore be used to benchmark against the results obtained from the counterfactual scenarios in order increase the validity of the study.

A potential weakness of the presented method is that it at the moment only is based on historical events. By varying the magnitude of these events above what has been experienced previously, by the use of counterfactual scenarios, valuable insights regarding response system capabilities are gained. However, by not assessing other credible, not yet experienced, events there is a possibility that weaknesses in the response system is overlooked. In future studies it would thus be beneficiary to also include hypothetical events, with the aim to increase the span of events in order to, for example, find events for which response system capabilities are insufficient.

The ability for generalization of the results from the study, which typically concerns a specific geographical location, needs to be further addressed. This can done by evaluating real incidents and counterfactual scenarios for other geographical locations, and then assess if the response and the consequence would be similar. It is then possible to evaluate if the results are valid for the railway system as a whole, and not only to the specific locations where the incidents actually took place.

In ongoing work by the authors (Johansson et al., 2008), the system model is used as a starting point, but here the emphasis is on studying the vulnerability of the interdependent technical railway systems, as identified in the system model. By systematically simulating failures in one or more technical systems simultaneously, the vulnerability of the technical system as a whole, due to dependencies between the subsystems, can be studied. For this purpose, the use of recovery times, as identified through the use of response curves, is very important in achieving a realistic measure of the system's overall vulnerability.

Future studies involve analysing organisational vulnerabilities. By using the system model as a starting point, the different actors' ability to cope with organisational strains, such as how the lack of certain actors or poor communication affects the rapidity to restore a system after a certain strain, can be studied. For this type of study, only a limited part of the technical components will be included, while all identified actors and their relationships will play an important role. The future aim is to be able to do a comprehensive analysis of the socio-technical system's vulnerability, bringing both the actor system and the technical system models together under the same umbrella.

Conclusions

The method presented in this paper offers a systematic approach, influenced by concepts from systems thinking and resilience engineering, for assessing the response system capability of socio-technical systems. The method involves construction of a system model, aiming at identifying all those elements that have an influence on the problem situation being studied. Based on this model, an accurate identification of those actors constituting the response system can be done. Given the focus of the present study, a comprehensive method addressing the assessment of response system capabilities was presented. The method includes the introduction of response curves, which illustrates the recovery time with respect to the magnitude of strain affecting the technical systems. These response curves facilitates the identification of both the response system capability for which the response system is designed for and the magnitude of strain for which the response capacity is insufficient, given by the two introduced asymptotes.

The present paper also includes a preliminary empirical study, aiming at evaluating the usefulness of the presented method. In order to reach more comprehensive conclusions about the response system capabilities of the Swedish Rail Administration, further studies are required. However, it is concluded that the preliminary study supports the validity and the applicability of the presented method.

Acknowledgements

The research behind the present paper has been financed by the Swedish Emergency Management Agency and the Swedish Rail Administration, which is greatly acknowledged. We also would like to extend our gratitude for valuable comments regarding the presented research to Assistant Professor Henrik Tehler, Associate Professor Olof Samuelsson, and Professor Kurt Petersen.

References

Abrahamsson, M., Jönsson, H. and Johansson, H. (2008). Analyzing emergency response using a Systems Perspective, Proceeding from PSAM9, 18-23 May, Hong Kong, China.

Amin, M. (2001). Toward Self-Healing Energy Infrastructure Systems, IEEE Computer Applications in Power, Vol. 14, No. 1, pp. 20-28.

Appicharla, S. K. (2006). System for Investigation of Railway Interfaces, 1st IET International Conference on System Safety 2006, 6-8 June, London, U.K.

Axelrod, R., and Cohen, M. D. (2000). Harnessing complexity, Basic Books, New York, USA.

Checkland, P. (2006). Systems Thinking, Systems Practice, John Wiley & Sons Ltd, Chichester, UK.

de Bruijne, M., and van Eeten, M. (2007). Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment, Journal of Contingencies and Crisis Management, Vol. 15, No. 1, pp. 18-29.

Hollnagel, E., Woods, D. D., and Leveson, N. (Eds.). (2006). Resilience Engineering: Concepts and precepts, Ashgate Publishing Limited, Aldershot, UK.

Jackson, M. C. (2000). Systems approaches to management, Kluwer Academic/Plenum Publishers, New York, USA.

Johansson, J., Jönsson, H. (2008). A Model for Vulnerability Analysis of Interdependent Infrastructure Networks, Joint Conference for European Safety and Reliability Association and Society for Risk Analysis Europe (ESREL2008 and 17thSRA-Europe), Valencia, Spain, 22-25 September.

Jönsson, H., Abrahamsson, M., and Johansson, H. (2007). An Operational Definition of Emergency Response Capabilities, in Proceedings of Disaster Recovery and Relief: Current and Future Approaches (TIEMS 2007), Trogir, Croatia.

Little, R. G. (2002). Toward More Robust Infrastructure: Observations on Improving the Resilience and Reliability of Critical Systems, Proceedings of the 36th Annual Hawaii International Conference on System Sciences 2003, pp. 58-66.

Little, R. G. (2004). A socio-technical systems approach to understanding and enhancing the reliability of interdependent infrastructure systems, International Journal of Emergency Management, Vol. 2, No. 1-2, pp. 98-110.

Little, R. G. (2005). Organizational Culture and the Performance of Critical Infrastructure: Modeling and Simulation in Socio-Technological Systems, Proceedings of the 38th Annual Hawaii International Conference on System Sciences 2005, pp. 1-8, Hawaii, USA.

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, Vol. 18, No. 2, pp. 310-318.

McDaniels, T., Chang, S., Peterson, K., Mikawoz, J., and Reed, D. (2007). Empirical Framework for Characterizing Infrastructure Failure Interdependencies, Journal of Infrastructure Systems, Vol. 13, No. 3, pp. 175-184.

Rasmussen, J. (1985). The Role of Hierarchical Knowledge Representation in Decisionmaking and System Management. IEEE Transactions on systems, man, and cybernetics, Vol. 15, No. 2, 234-243.

Rinaldi, S. M., Peerenboom, J. P., and Kelly, T. K. (2001). Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies, IEEE Control Systems Magazine, Vol. 21, No. 6, pp. 11-25.

Senge, P. M., Kleiner, A., Roberts, C., Ross, R. B., Smith, B.J. (1994). The Fifth Discipline – Fieldbook, Doubleday, USA.

Skyttner, L. (2005). General Systems Theory: Problems, Perspectives, Practice (2 ed.), World Scientific Publishing Co. Pte. Ltd, Singapore.

Stoop, J. A., and Thissen, W. A. H. (1997). Transport safety: trends and challenges from a systems perspective, Safety Science, Vol. 26, No. 1-2, pp. 107-120.

Thissen, W. A., and Herder, P. M. (2003). Critical infrastructures: Challenges for systems engineering. Proc. IEEE International Conference on Systems, Man and Cybernetics 2003, pp. 2042-2047, Washington DC, USA.

Uhr, C., Johansson, H. and Fredholm, L. (2008). Analysing Emergency Response Systems, Journal of contingencies and crisis management, Vol. 16, No. 2, pp. 80-90.

Verwater-Lukszo, Z., and Bouwmans, I. (2005). Intelligent Complexity in Networked Infrastructures. Proc. IEEE International Conference on Systems, Man and Cybernetics 2005,.pp. 2378-2383.

Wears, R. L., Perry, S. J., Anders, S., and Woods, D. D. (2008). Resilience in the Emergency Department. In E. Hollnagel, C. P. Nemeth and S. Dekker (Eds.), Resilience Engineering Perspectives - Remaining Sensitive to the Possibility of Failure (Vol. 1), Ashgate Publishing Limited, Aldershot, UK.

Woods, D. D., and Wreathall, J. (2008). Stress-strain Plots as a Basis for Assessing System Resilience. In E. Hollnagel, C. P. Nemeth and S. Dekker (Eds.), Resilience Engineering Perspectives - Remaining Sensitive to the Possibility of Failure (Vol. 1) , Ashgate Publishing Limited, Aldershot, UK.

Author Biography

Jonas Johansson is a PhD student at the Department of Industrial and Electrical Engineering at Lund University, with a M.Sc. in Electrical Engineering and a Degree of Licentiate of Engineering in Automation. Main research area is risk and vulnerability management of technical infrastructures and the impact of interdependencies between large-scale infrastructures.

Alexander Wilhelmsson is a PhD student at the Department of Fire Safety Engineering and Systems Safety at Lund University, with a B.Sc in Fire Safety Engineering and a M.Sc. in Risk Management and Safety Engineering. Main research area is crisis management of transport systems.

V

Paper V is submitted for review to a scientific journal. To avoid problems with the publication of the paper, it is not included in this public version of the thesis.

Abstract: Critical infrastructures provide essential services for the function of our society. Disruptions in one infrastructure have widespread effects, not only for the originating infrastructure but also through mutual dependencies for other infrastructures. Identifying vulnerabilities inherent in these system-of-systems is thus highly critical for the proactive management and avoidance of future crises. A modelling approach for interdependent technical infrastructures is proposed and three perspectives for the analysis of vulnerabilities are introduced, addressing the complexities associated with comprehensively analysing technical infrastructure. An empirical analysis of the railway system in southern Sweden is conducted, a system consisting of seven interdependent supporting systems. It is concluded that the proposed modelling approach and the three perspectives of vulnerability analysis give valuable insights for the proactive management of technical infrastructures.