Risk and Vulnerability Analysis of Large-Scale Technical Infrastructures

Electrical Distribution Systems

Jonas Johansson

LUND UNIVERSITY

Licentiate Thesis
Department of Industrial Electrical Engineering and Automation

2007

Department of Industrial Electrical Engineering and Automation
Faculty of Engineering
Lund University
Box 118
221 00 LUND
SWEDEN

http://www.iea.lth.se

ISBN:978-91-88934-45-1
CODEN: LUTEDX/(TEIE-1053)/1-111/(2007).

Printed in Sweden by Media-Tryck, Lund University
Lund 2007

Aut viam inveniam aut faciam

[I will either find a way or make one]

Abstract

The thesis treats the subject of risk and vulnerability analysis of large-scale technical infrastructures. In particular the focus is on the development of methods for vulnerability analysis of electrical distribution systems. The methods and the concepts behind them should nevertheless also be seen as applicable to other technical infrastructures.

Robust and reliable technical infrastructures are a prerequisite for modern society. If they fail to deliver their services, severe consequences arise. Two major crises in Sweden regarding the supply of electricity have clearly showed the magnitude of the consequences on society and its dependency on a reliable electricity supply and the emergency response necessary to return to normal. Furthermore, most technical infrastructures depend on a reliable power supply for their proper functioning. The power supply in turn relies on some of these for its proper operation and control. There is a need for methods aimed at assessing the vulnerability of the interconnected infrastructures the society depends upon.

In the thesis two approaches, or methods, of assessing the vulnerability of technical infrastructures are presented: global vulnerability analysis and critical components. The applicability of the methods was tested by empirical studies of three electrical distribution systems in Sweden. The result from the global vulnerability analysis clearly shows that distribution systems are highly vulnerable to some type of perturbations. The results from the analysis of critical components show that the methods can be used for finding and ranking components that are critical for the system and that they render a very feasible way to test the system for *N-k* contingencies.

The design approach of the methods was to use a network model and a corresponding physical model of the electrical distribution system. The network model contains the topological information. The physical model describes the behavior of the network. Performance measures have been developed to describe the consequences of perturbation to the network. The studies indicate that these measures are relevant for describing vulnerability of an electrical distribution system and in finding its critical components. The design approach of the methods constitutes an important step towards vulnerability analysis of interdependent infrastructures.

The results from applying the methods can be useful for emergency mitigation and preparedness planning. The results can further be visualized in the form of geographical vulnerability maps. These maps can facilitate the discussions between persons working in different fields.

Acknowledgements

There are several persons, companies, and organizations that deserve to be acknowledge as being a necessary support and contributors to the research behind this thesis.

First of all, I would like to thank all the people working at the department of Industrial Electrical Engineering and Automation (IEA), Faculty of Engineering at Lund University. I am especially grateful to Gustaf Olsson for having him as my first supervisor and that he accepted me as a PhD-student, to Olof Samuelsson for being my second supervisor and for always giving excellent feedback, and finally to Christian Rosén for being a support as an assistant supervisor and friend throughout the research project. Their support and guidance are greatly acknowledged. Special thanks to Olof Samuelsson and Christian Rosén for the proofreading of the thesis and their valuable comments are in place. I also would like to thank Sture Lindahl for always sharing his highly interesting and very valuable knowledge of electric power systems. I would like to thank all the undergraduate students for whom I was an assisting supervisor in their master thesis projects. Helping you was my pleasure. All the PhD-students at the department have my gratitude for creating a pleasant working environment. Especially Jonas Ottosson, Dan Hagstedt, and Tomas Berg for your friendship and all the fun we have had together.

All the people constituting the FRIVA-framework within LUCRAM deserves acknowledgement for the many interesting discussions and everything I have learned from you – your differing research disciplines, thoughts, and ideas have opened my mind. Kurt Petersen at the Department of Fire Safety Engineering has made an excellent job at steering FRIVA towards success. Henrik Johansson and Henrik Jönsson, at the same department deserve, special acknowledgement. Henrik Johansson for his enthusiasm and knowledge in the area of risk management. Henrik Jönsson for being the best research partner one could ask for. I now regard you as a friend. The three of us have spent many hours while writing two papers together. I greatly appreciate all the interesting discussions we have had and everything you have taught me. I hope that I gave something back to you.

I would also like to take the opportunity to thank all the companies that were

very forthcoming in supplying the empirical data necessary for the research. Further, I would like to thank all of you in the industry that have shown interest for my research and the feedback you have given me.

This work has been financed by Krisberedskapsmyndigheten (Swedish emergency management agency). Their support is gratefully acknowledged.

Finally,

my big family and my many friends – you mean everything to me. I love you.

Lund, 9 May 2007
Jonas Johansson

Contents

Chapter 1

Introduction

The technical and social developments in the last decades have led to a society that is heavily dependent on technical infrastructures. Everyday we, the modernized society, utilize numerous technical infrastructures without much reflection. The reason behind this development can readily be summarized in one word: efficiency. The downside is that disruption in one of these infrastructures leads to catastrophic consequences, as has been demonstrated through various incidents around the world. The infrastructures that surround us have grown into very complex and large-scale systems. The vulnerability of these is not easily analyzed. Furthermore, these infrastructures have become dependent of each other. This means that a disturbance in one infrastructure can lead to consequences in other infrastructures. Several significant questions arise: How vulnerable are these infrastructures? To what type of perturbations are they vulnerable? Are there components in these systems that could lead to severe consequences if they malfunction? How does the coupling between infrastructures affect the vulnerability? How do we quantify the risk of technical infrastructures for unlikely events? These questions form the basis for the research behind this thesis.

The storm Gudrun and the associated total devastation of electric power distribution systems and road networks in a large part of Sweden is a vivid example of the consequences when the unexpected happens. In (Bengtsson et al., 2007), statistical extreme value theory is used to evaluate how extreme the storm Gudrun was. The analysis is based on reports of storm damage in Swedish forests in the period 1965-2007. Although an extreme event, the analysis yields that the damage of this magnitude corresponds roughly to a 80-year storm. Could this crisis have been foreseen? The life expectancy of electrical distribution systems is about 50 years. Should distribution systems be designed to better cope with these types of disturbances? In the article by Bengtsson it is also stated that storm damage twice the size of Gudrun is not unlikely. With the threat of global warming and climate changes, storms with even higher severity and frequency might occur. The electrical blackout in

Sweden 2003, the Auckland power outage in 1998, and the luxury liner Norwegian Pearl that rendered 5 million Europeans without electricity in 2006[1] were all unlikely to happen. Nevertheless, they did happen.

Incidents, both with natural and technical causes, which lead to severe consequences, happen seldom. If the frequency of the incidents is plotted against the consequences they give rise to, they tend to follow a power law distribution (e.g. Amin, 2004). The tail of this power law distribution curve is of the greatest interest. In this area, the consequences are severe and the probability for occurrence is low. How do we identify such incidents and estimate the probability of their occurrence when limited or no historical data are available?

Clearly, an open mind to what can happen to technical infrastructures is needed. The aim of the present thesis is to narrow the gap between normal analysis of technical systems, where only small deviations are normally taken into account, and what can happen if the disturbances are larger and different from what is normally expected. How will the system react? What will the consequences be?

This licentiate thesis is a step in the efforts necessary to understand and analyze vulnerability of technical infrastructures and, in the long run, assess the risks and vulnerabilities associated with interdependent technical infrastructures. It should be noted that the aim of research is to develop a methodology that can assess the vulnerability of different technical infrastructures and where the electrical delivery system has been the reference system for the development of these methods.

1.1 Motivation

There are several motivations for the research behind the present thesis. My personal motivation is based on a never-ending desire to understand the form and function of complex systems and phenomena and the environment in which they exist. Economical, environmental, political, and legislation factors together with the ever-increasing demand for the services they provide to our society, such as energy and communication, have formed these highly complex systems. The interest in electrical distribution systems stems from

[1] The incident happened because a power line over the river Ems had to be de-energized in order for the luxury liner to pass under it. The electricity network was under strained conditions because of cold weather which meant that the disconnection of the line lead to cascading failures.

my background with a father who worked at an electrical distribution company and a M.Sc. in electrical engineering.

The storm Gudrun in 2005 led to severe disruptions of power supply to roughly 650 000 customers in large parts of southern Sweden. In order to put pressure on electricity network owners to limit disruptions of this kind, modifications to the existing electricity law was constituted and came into force the 1 of January 2006 (Ellag 1997:857). The additions concern compensation to customers for interruption and that network companies have to establish a risk and vulnerability analysis of their network on a yearly basis. The modifications affect those companies who operates networks with voltages below 220 kV, i.e. sub-transmission and distribution systems.

As of 1 January 2006, power distribution companies have to pay compensation to customers if the interruption time is longer than 12 hours. In Figure 1.1 the level of compensation, as expressed in percent of the estimated yearly network tariff, is shown. The maximum compensation is equal to 300% of the estimated yearly network tariff. As of 1 January 2011, power outages lasting more than 24 hours are not allowed.

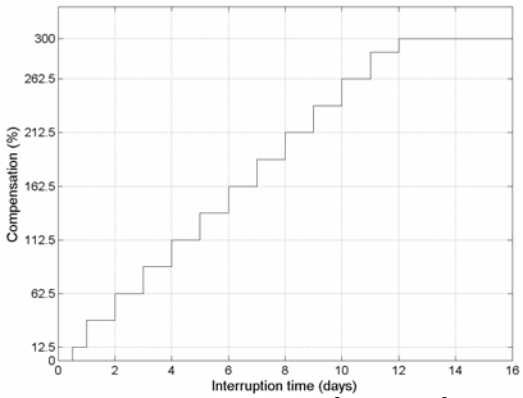


Figure 1.1. Compensation to customers as a function of interruption time. The compensation is expressed in percent of the estimated yearly network tariff.

The modification of the electricity law also includes two other important amendments. Firstly, all network companies must, on a yearly basis, establish a risk and vulnerability analysis regarding the security of supply and an action plan for how to improve the security of supply. Secondly, customers have a right to be informed by the network companies about their security of supply.

The use of the concept of risk and vulnerability is a rather well applied concept for many industries and sectors but not as much to the electrical power industry (with the exception of the nuclear power industry). Another motivation for the research behind this thesis is that the concept of risk and vulnerability can serve as a bridging common platform between people with differing background such as system owners, decision makers, and the public.

The title of the thesis is "*Risk and Vulnerability* Analysis of Large-Scale Technical Infrastructures". However, the focus is limited to *vulnerability* analysis. The reason for the somewhat misleading title is that it is a convention in the field to refer to *risk and vulnerability* analysis, with no general separation between the two. As it will be clarified in this thesis, vulnerability analysis can be used as the foundation for risk analysis. Since this is thoroughly discussed in the thesis, the title of the thesis is motivated.

1.2 Objectives and Delimitations

The initial objective of the thesis had a very broad perspective: to develop methods for risk and vulnerability analysis of interdependent large-scale technical infrastructures. The research area of risk and vulnerability analysis of technical infrastructures is relatively new, which has lead to a narrowing of the initial scope. The objectives of the thesis are in short:

- To develop methods for vulnerability analysis of a single technical infrastructure.
- To test the feasibility of these methods by empirical studies on electrical distribution systems.
- To discuss how vulnerability analysis can be utilized for risk analysis.
- To form an approach to how these methods can be used in order to analyse interdependent infrastructures.

The methods are aimed at vulnerability analysis of the fundamental part of technical infrastructures, i.e. the network that supports the transport of the desired goods. These goods could be electricity, communication, water, oil, gas, food etc. Vulnerabilities due to organizational and market factors are not explicitly addressed.

1.3 Contributions

The main contributions from the thesis are given below. Discussions and conclusions regarding this thesis are given in Chapter 8 and Chapter 9, respectively.

- A method for assessment of global vulnerability of technical infrastructures. Global vulnerability analysis is a way to assess the performance of the infrastructure when subjected to different types of threats and hazards.

- A method for identifying 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. The criticality of a component or set of components is regarded to be the vulnerability of the system to failures in these components.

- An approach to the analysis of interdependent infrastructures based on the developed methods. Interdependent infrastructures are several infrastructures that are interconnected.

- Illustrative examples of the methods applicability by assessing the vulnerability of real electrical distribution systems.

- The development of a tool in Matlab® to map infrastructures to the structure necessary for analysis. Tools for visualizing analysis results has also been developed. These could be made compatible with geographical information systems (GIS).

The methods, at present, can be regarded from the view of being a conceptual framework for the facilitation of vulnerability assessment of technical infrastructures. They are nevertheless, as presented in the thesis, applicable and valuable methods for vulnerability assessment.

1.4 Outline of the Thesis

Chapter 2 starts with a discussion and definition of the concepts of risk and vulnerability and how they relate to each other. This is followed by a discussion of technical infrastructures and interdependencies of technical infrastructures. The chapter ends with a brief introduction to the field of network theory. Network theory has served as a conceptual framework for the methods developed in this thesis.

Chapter 3 introduces the subject of electrical power systems in general and electrical distribution systems in particular. Readers well acquainted with this area may omit this chapter.

Chapter 4 presents the approach used in the thesis to model technical infrastructures. In particular, the modeling of electrical distribution systems is treated.

Chapters 5 and 6 present the proposed methods in order to assess the vulnerability of technical infrastructures. Chapter 5 introduces the approach of global vulnerability analysis. Chapter 6 discusses a method to find and rank critical components in technical infrastructures.

Chapter 7 present empirical studies of three different electrical distribution systems, applying the methods presented in the two previous chapters.

The outcome of this thesis is discussed in Chapter 8. The thesis ends with some conclusions and ideas for future work in Chapter 9.

1.5 Publications

The work and ideas presented in this thesis are largely based on articles that are published or accepted for publication. The developed methods presented in the thesis are not solely the work of the author. They are the result of a fruitful cooperation between the authors of the articles [1] and [3] below, and no general division of work between the authors can be made. The articles are:

[1] Johansson, J., Jönsson, H., Johansson, H., (2007). Analysing Societal Vulnerability of Electric Power Distribution Systems ', *Int. J. Emergency Management*, Vol. 4, No. 1, pp.4–17.

[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, September 25-27.

[3] Jönsson, H., Johansson, J., Johansson, H., (2007). Identifying Critical Components in Electric Power Systems: A Network Analytic Approach, Accepted for presentation at: *European Safety and Reliability Conference 2007* (ESREL2007), Stavanger, Norway, June 25-27.

Chapter 2

Concepts and Definitions

In the area of risk and vulnerability research, different definitions of many concepts and terms exist. This chapter begins with my viewpoints of some of these terms and how they are used in this thesis. A brief reference to research conducted in this area is given, to either support or discuss the choice of viewpoint. In the following section, a short discussion around technical infrastructures is given. The chapter ends with a summary of the fundamental aspects of network theory, which has influenced the approach used in this thesis to assessing vulnerability of technical infrastructures.

2.1 Risk and Vulnerability

The words risk and vulnerability are commonly used in everyday life. Humans think in risk terms daily in order to cope with the reality we live in. Sometimes risk is used as a term to describe the probability of an event, for example the phrase "there is a risk it might rain today". 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. A phrase like "the risk involved in buying that apartment is too great", exemplifies this. 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 loose money on the deal). The buyer has thus made a decision not to buy the apartment using a risk-based approach. The concept of vulnerability is not as clear. Most often vulnerability refers to how easily a system, organization, or human performance is degraded for some hazard or threat materializing. Sometimes vulnerability refers to a state in a system, such as a door left open making it easy for a burglar to access ones house. Vulnerabilities can be identified without quantifying the probability of something exploiting them; the open door can for example be identified as a vulnerability regarding burglary without quantifying the probability of a burglar breaking in. Formal definitions of the terms risk and vulnerability, and how they relate to each other, are given in the following sections.

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)

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. 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.

To perform 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 usually 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 risk analysis. It might be possible that the probability is not known, 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.

Vulnerability

There have been arguments against the traditional risk analysis approach since it tends to focus on the hazard, and not the ability of the system to withstand hazards, i.e. focus on mitigating the hazard, or 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 and Mars, 2000). Some define vulnerability analysis as taking a wider scope than traditional risk analysis (e.g. Einarsson and Rausand, 1998; Holmgren, 2004). I argue that the definition of risk, as put forward by Kaplan, does not exclude this wider scope of the traditional risk analysis. I further argue that vulnerability analysis is about taking a different point of view, rather than just 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 perturbation. 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 other (Hansson & Helgesson 2003). In addition, two identical (cloned) systems are viewed as always equally vulnerable to all possible hazard exposures, independent on 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 vulnerability is then regarded as a property that arises from the states of the system (e.g. Haimes, 2006). 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).

Vulnerability is seen to be the antonym of the two terms robustness and resilience. Robustness is a static property describing the ability for a system to withstand a strain. Resilience is a dynamic property describing a systems ability to recover from a disturbance.

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 deliberate events. In the field of power system analysis the term *disturbances* is normally used to describe hazards from within or from outside of the system. In Johansson et al. (2007a) we, as in Holmgren (2006), use the word *perturbation* to describe the combination of both hazards and threats. In the thesis, perturbations will be used to describe both hazards and threats that can be either endogenous or exogenous.

In order to assess the vulnerability, as put forward here, the consequences that arise given a certain perturbation must be estimated, i.e. in contrast to risk where the quantification of the probability of the perturbation is also of importance. The concept of vulnerability is defined as (Johansson et al., 2007b):

1. "What can happen, given the perturbation?"
2. "How likely is it that that will happen, given the perturbation?"
3. "If it does happen what are the 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 highly critical, by some notion, components. The perturbation 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 perturbation, i.e. one component failure. If the system is vulnerable, then combining the vulnerability with the probability of a perturbation exploiting the vulnerability yields the risk.

The Relation Between Risk and Vulnerability

The concepts of risk and vulnerability are rather tightly related to each other. The following section is meant to discuss and visualize the view of how they are related. For the discussion of risk, it is drawn on concepts put forward by Kaplan and Garrick (Kaplan et. al., 1981 and 2001). For the discussion of vulnerability, it is drawn on concepts put forward by Haimes (2006).

In Figure 2.1 the *normal state*, S_0, of a system is shown in a phase plane. The normal state can be viewed as an "as planned" state of the system. Initiating events, *IE*, can push this system into an end state, *ES*. The end state represents the state where the consequences are evaluated. This full trajectory,

from S_0 to an ES is defined as a *risk scenario*. Different initial events might lead to different or 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 that can be reached by different initial events (e.g. hard weather, technical malfunction, or a malicious attack) and can lead to different end states (e.g. the loss of a power line). These system states 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 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.

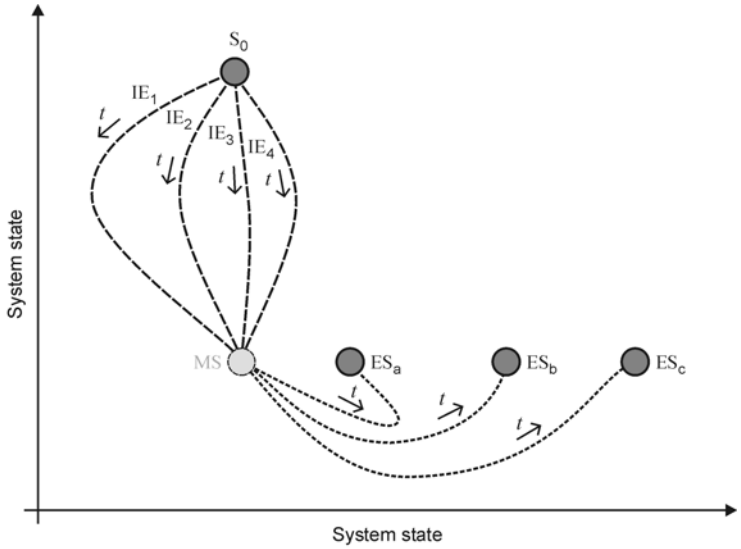


Figure 2.1. The concept of risk. S_0 = system as planned, IE = Initiating Event, MS = Middle State, ES = End State.

For the definition of vulnerability, this middle state is the focal point. In Figure 2.2 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. one component out of function or two components out of function) it is possible to evaluate what the possible end states can be, i.e. the

consequences. There might be several initiating events that lead to the same middle 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. Hansson and Helgesson (2003) define robustness as "the tendency of a system to remain unchanged, or nearly unchanged, when exposed to perturbations". For most systems, there will be a desire to return to the initial or a desired state after the system has been perturbed. 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 go back to a *desired state* (not illustrated in the figure). The trajectory and the efforts necessary to return the system to the initial or a desired state are viewed as the *resilience* of the system. Lately *resilience* has become a hot topic and the term has no single clear definition. 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, see Hollnagel et al. (2006) for a discussion of the concept. 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". The full trajectory from a middle state, through an end state, to the initial or desired state is defined as a *vulnerability scenario*.

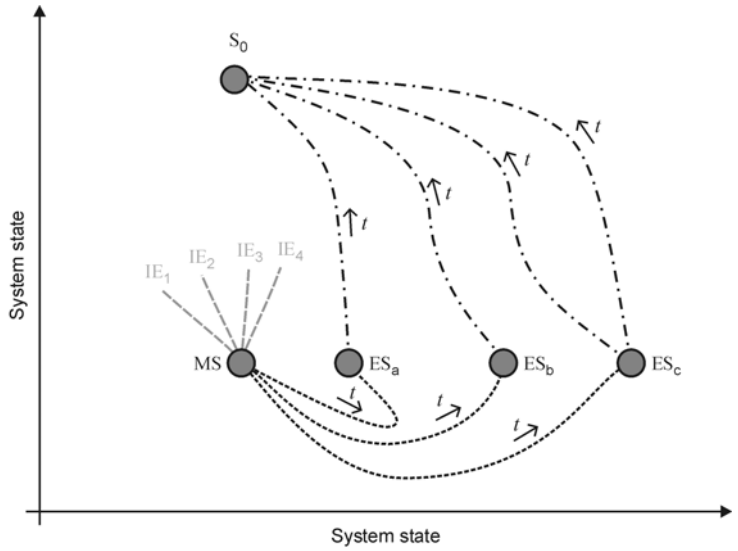


Figure 2.2. The concept of vulnerability. S_0 = system as planned, IE = Initiating Event, MS = Middle State, ES = End State.

For the system to go from the S_0 to the middle state it has to be exposed to a perturbation. For power systems, at transmission and sub transmission level, the well-known N-1 design criterion 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. This leads us into the aspect of vulnerability, answering the "risk triplets" conditioned on the perturbation. Identifying a system's vulnerability thus gives the answer to what consequences that arise given a specific perturbation without identifying the specific initial event that led to MS.

In Figure 2.3 the concepts of risk and vulnerability are brought together. The identification of all the middle states and the end states of the system can be seen as a partial vulnerability analysis. The methods presented in the thesis have the focus on identifying middle states and estimating the end states, i.e. the consequences. A vulnerability analysis also requires the identification of the recovery from these end states. A partial vulnerability analysis can be complemented by identifying and quantifying the probability of initial events, which can put the system into the middle states, to yield a traditional risk analysis.

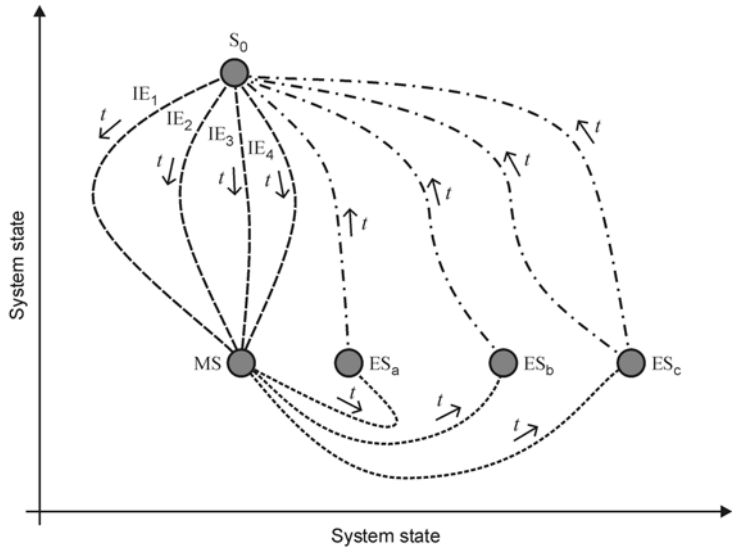


Figure 2.3. Bringing risk and vulnerability together. S_0 = system as planned, IE = Initiating Event, MS = Middle State, ES = End State.

The concept of vulnerability is different from the concept of risk in the aspect of not having to estimate (qualitatively or quantitatively) the likelihood or type of the initiating event. This leads to the prospect of a more thorough and more open-minded search for possible middle states of the system. A vulnerability analysis gives valuable information of the extent of the consequences when the system is perturbed. It also yields important information to what types of perturbations the system is vulnerable. If desired the vulnerability analysis can be complemented with an assessment of the likelihood of perturbations exploiting the vulnerability, i.e. approaching a risk analysis. This can for example be necessary in order to select between different alternative investments for vulnerability mitigation.

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 are actions 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 2.4 the different phases of crisis management are illustrated. The figure is based on a framework from FEMA (Federal Emergency Management Association) (FEMA, 1997) and a framework from CCMD (Canadian Center for Management Development) (CCMD, 2003).

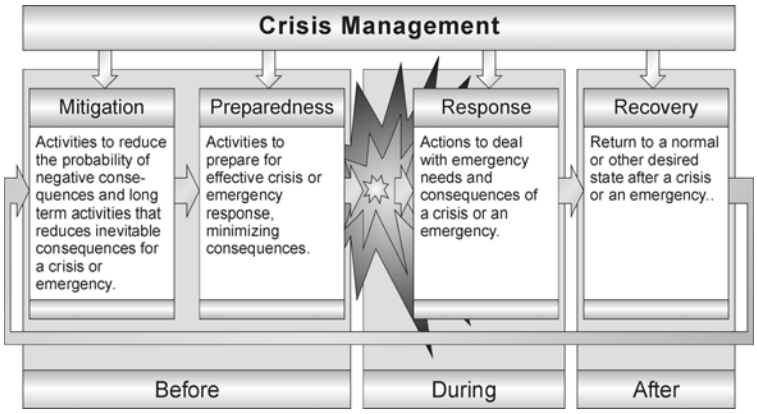


Figure 2.4. The different phases of crisis management in accordance with FEMA and CCMD.

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 this thesis is on proactive crisis management concerning mitigation and preparedness. Aspects of the research could also be used, with appropriate further research, in the recovery phase.

2.2 Large-Scale Technical Infrastructures

A proper definition of "large-scale technical infrastructures" is in place since the term is used throughout the thesis. The part "large-scale" indicates that the system is spatially widespread and that the system requires a vast number of components for its proper function. For the definition of "large-scale" I don't put any restrains on whether the system is to be regarded as being *complicated* or *complex*. 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 used to indicate that a system has properties such as non-linearity, adaptability, and emergence. For a more thorough – and very interesting – discussion of the terms complicated and complex, Axelrod et al. (2000). Ottino (2004), and Amaral et al. (2004a and 2004b) are recommended. My viewpoint is that the technical part of the system that constitutes the foundation for providence of intended services can be regarded as a complicated system, e.g. railroads, electrical networks, roads, and water pipes. The larger view of a technical system, including the impact of economical, legal, organizational, and other contextual factors, most certainly force the analyst to regard it as a complex system.

The term "Technical" is defined by Oxford English Dictionary (OED) as:

> *"**adjective 1** of or relating to a particular subject, art, or craft, or its techniques. **2** requiring specialized knowledge in order to be understood. **3** of or concerned with applied and industrial sciences. **4** according to a strict application or interpretation of the law or rules."*

"Infrastructure" is defined by OED as:

> *"**noun** the basic physical and organizational structures (e.g. buildings, roads, power supplies) needed for the operation of a society or enterprise."*

Thus, "large-scale technical infrastructures" corresponds to, from my point of view, a system that is serving a large spatial area, such as a country, municipality, or city, with many underlying components that interact in a way that requires specialized knowledge in the field of applied and industrial sciences to be understood.

Critical Infrastructures

Large-scale technical infrastructures are often identified as critical or as 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. In KBM (2005) examples of infrastructures defined as critical are given:

- Telecommunication
- Data communication
- Electrical power supply
- Provision of fuels
- Watersupply, 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). Electrical power

supply stands out as an especially critical infrastructure since many other infrastructures depend heavily on a reliable power supply.

Infrastructure Interdependencies

The critical infrastructures that support and form the basis of the society we live in are so complicated, and even complex, that modeling and simulating any one of them is not an easy task. In the hallmark of efficiency and economy, 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 network. Coincidentally, this same telecommunication network is necessary for an appropriate recovery of the power system. Mutually dependent infrastructures are called *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 shown the interdependency of critical infrastructures. 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 is estimated to 500 million SEK. The system went down because one nuclear reactor had internal problems and was disconnected from the grid and one bus bar malfunctioned, i.e. an N-2 contingency (could be seen as a 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 unserved energy. Business and industries had to close. Shops had to close since they could not charge their customers. The backup power generation in hospitals did not work properly, leading to cancelled operations. People at care in their homes had to be transported to hospitals since the medical equipment in their homes did not work. The communication system used by the police did not work. In some areas, the cell-phone system went down. Traffic lights and lattice barriers ceased to function, leading to severe traffic problems. 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 societies dependency on electricity. Fortunately, the communication systems necessary for the operation and control of the

power system functioned properly since it has back-up batteries that lasted long enough to handle the restoration of system operation. The incident has nevertheless lead to an increase of the battery capacities in transmission system substations.

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 their food properly since refrigerators and freezers stopped working, 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 pumping. Ventilation, elevators and automated doors stopped working. This lead to straining efforts for the local police and the social services to help 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. The local power company responsible for the grid and the local authorities had different opinions. In order to repair the faulty cables, specialized repairers had to be flown in from Australia. The economical consequences of the crisis were significant. The power outage highlights an important aspect of crisis management and 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 a storm by the name 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 650 000 persons were without power supply. The full restoration of the power supply took seven weeks. During the event, the telecommunication used for operation and control was lost to half of the substations in the area. The train service between Malmö and Stockholm was interrupted for about

two weeks. The incident has lead to a massive investment program in order to replace roughly 17 000 kilometers of bare overhead conductors with underground cables. The storm also rendered the road network unusable due to the sheer amount of trees scattered over the roads. This severely hampered the rebuilding of the network. The severe consequences of the incident led to modifications in the Swedish Electricity Law regarding compensation for customers.

The above examples illustrate the importance of a proper understanding of how infrastructures are coupled and the consequences that the malfunction of one infrastructure can have on other infrastructures. Interdependencies between technical infrastructures are not only a technical issue but also affect social and environmental systems that depend upon their services. 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 behavior, 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 candidates techniques for modeling and simulating interdependent infrastructures are described and discussed. The article point out the lack of analytical modeling and simulation tools for the study of interdependencies and the need of more comprehensive research in this area. Zimmerman gives in (Zimmerman, 2001) several good examples of infrastructure interdependencies. In (Zimmerman et al. 2006) the duration of an electric power outage, T(e), to the duration of a subsequent infrastructure outage, T(i), due to electric power outages, is given as a ratio T(i)/T(e). This measure is claimed to be a measure of the direction of a cascade. In (Restrepo et al., 2006) geographical interdependencies in electric power infrastructures are given.

There are several articles either giving an overview (e.g. Peerenboom et al., 2007; Brown et al. 2004) or describing certain modeling and simulation tools for analyzing infrastructure interdependencies (e.g. Gursesli et al., 2003; Benoît, 2004; Tolone et al., 2004; Balducelli et al., 2005). They all capture aspects of critical infrastructure interdependencies. Nevertheless, it is apparent that there is still a need for research and development in this area before they can be of practical use for full-scale risk and vulnerability analysis of critical infrastructures and the effect of interdependencies. In this thesis, the methods presented can be used as the foundation for interdependence analysis, see section 9.2, although the focus is on vulnerability analysis of single infrastructures.

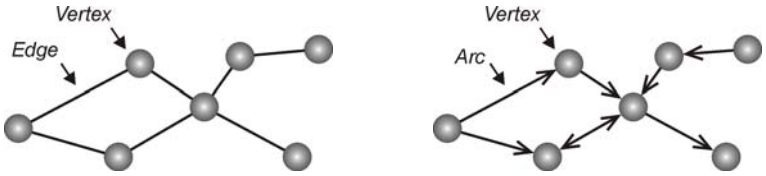
2.3 Network Theory

The research described in this thesis uses network theory as a conceptual framework. Network Theory derives from 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 introduction to network theory given here is based on Watts (2003), Newman (2003), Holme (2004), and Strogatz (2001). The first reference takes a popular science approach to the subject, while the latter three references give a good overview of the subject and has extensive references to related literature. The theory described in this chapter stems from these references if not explicitly stated otherwise. The aim is to give the reader a basic understanding of Network Theory.

The basic concept of Network Theory is to build a model of real-world networks and describe the form and function of the network by different measures. Network theory has been used to study a wide range of systems in the form of networks (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.

Graph Theory to Network Theory

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 2.5. 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.



a) b)

Figure 2.5 Example of a) an undirected graph with an edge and vertex indicated, and b) a directed graph with an arc and a vertex indicated.

The idea behind network theory is the notion that it is possible to draw relevant conclusion about a network (could be 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, 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 network can be found.

Describing the Network Structure

There are numerous terms and metrics in the field of network theory with the aim to describe the static structure of a network. In this section, a few of the most commonly used are briefly described. The section starts with terms and metrics that stem from graph theory, illustrated in Figure 2.6, and ends with some of the metrics commonly used in network theory, illustrated in Figure 2.7.

Path is 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 is a path that ends in the same vertex as it starts, i.e. $v_1 = v_n$. A circuit that consist 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. 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* is simply the length of a geodesic between v and w. The average distance of graph is referred to as the *characteristic path length*.

The *eccentricity* of *v* is the maximal distance from *v* to any other vertex in *G*. *Radius* is the minimal eccentricity among all vertices in G and *diameter* is the maximum eccentricity among all vertices in G.

The *degree* of *v* is 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. *Average node degree* is simply the arithmetic mean of the degree for all vertices belonging to *G*. *Neighbours* of *v* is the vertices at distance one from *v*, and the *neighborhood* of v is the set of vertices at distance one from *v*.

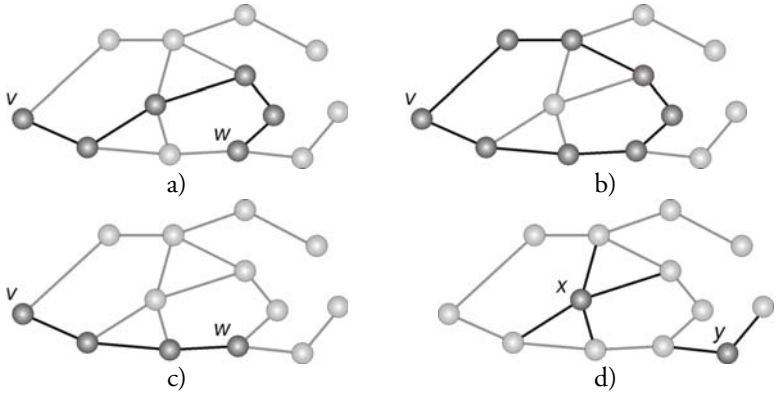


Figure 2.6 a) An elementary path between *v* and *w* with the length six. b) An elementary circuit between *v* and *w*. c) The distance (shortest possible path) between *v* and *w* is three. d) The degree of node x and y is four and two, respectively. For all the graphs the diameter is 7, the radius is 4, the characteristic path length (average diameter) is 5.15 and the average node degree is 2.46.

The structure of a network is the result, or the cast, of the forces and limitations that formed it. If one thinks of a road network, there will be very few nodes (street crossings) with more edges (roads) than four connected to it (except for some roundabouts and some older crossing sections in cities). This is a physical property, the limitation of physical space, which is reflected in the topology of the network. By measuring the structural properties for a network, one can classify and draw general conclusions from a network. It should be noted that to be able to draw any conclusion about the dynamics or properties of the physical system from the network representation, one has to have good knowledge and understanding of the physical system, e.g. a corresponding theory of behavior.

The *degree distribution*, *p(k)*, is the probabilistic density function of the node degree for a graph. Networks can be classified by which degree distribution function it approximates to. Real-world networks have shown to often have *power-law distributions*, i.e.:

$$p(k) = ak^{-\gamma} \tag{2.5}$$

where a and γ are constants and k is the degree. This function is quite different from what is expected from a purely random network formation process, implying that real-world networks (such as the www and the Internet) are not formed by a random process. A network that has the power-law distribution is sometimes called *scale-free networks*, since the function will look qualitatively the same even if rescaled. The power-law distribution function should be accompanied with cut-offs, addressing environmental constraints for the system (e.g. there is an upper limit on how many roads a junction can have due to physical constraints).

Betweenness, C_B, (more correctly referred to as *Betweenness Centrality*) is a measure that tries to capture the importance of a vertex, v, or edge, e, in a network, most often used for communication networks. It is a measure that describes how many shortest paths, geodesics, that goes through a specific vertex or edge. Node betweenness is defined as:

$$C_B(v) = \sum_{u \in V} \sum_{w \in V \setminus \{u\}} \frac{\sigma_{uw}(v)}{\sigma_{uw}} \tag{2.6}$$

where σ_{uw} is the number of geodesics between u and w, and $\sigma_{uw}(v)$ is the number of geodesics between u and w that passes v. Edge betweenness is defined as:

$$C_B(e) = \sum_{u \in V} \sum_{w \in V \setminus \{u\}} \frac{\sigma_{uw}(e)}{\sigma_{uw}} \tag{2.7}$$

where $\sigma_{uw}(e)$ is the number of geodesics between u and w containing the edge e. The betweenness measure thus assumes that all "flows" in the system take the shortest path, without any "flow" constraints. There are other measures that try to address this shortcoming, for example *flow betweenness* and *random walk betweenness*.

Clustering coefficient, C, describes, just as the name indicates, how clustered the network is in form of the density of triangles in the network (there are different definitions of the clustering coefficient, the chosen one is proposed by Watts and Strogatz (1998)):

$$C = \frac{1}{n}\sum_{i \in V} C_i = \frac{1}{n}\sum_{i \in V} \frac{M_i}{k_i(k_i - 1)/2} \tag{2.8}$$

where 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. The denominator $k_i(k_i - 1)/2$ is thus the maximum number of edges that can exist between the neighbours of vertex i. In a friendship network, a high clustering coefficient would mean that the friend of a friend of yours is likely to also be your friend. There are also other clustering coefficients dealing with loops of higher order than three.

Average geodesic length, l, describes how tightly coupled the network is, defined as (Latora et. al. 2001):

$$l = \frac{1}{N(N-1)}\sum_{w \neq v} d(v,w) \tag{2.9}$$

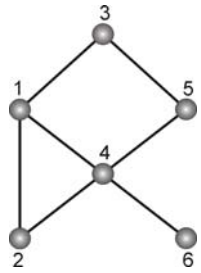
where $d(v,w)$ is the distance, length of the shortest path, between v and w. If the network is disconnected, i.e. consists of two or more subcomponents, $d(v,w)$ becomes infinite. Thus the *inverse geodesic length*, l^{-1}, is often preferred:

$$l^{-1} = \frac{1}{N(N-1)}\sum_{w \neq v} \frac{1}{d(v,w)} \tag{2.10}$$

It is also possible to calculate the average geodesic length for each component of the network to get around the problem of an infinitive l.

The average geodesic length thus describes how many steps in average it takes to go from a vertex to another. Let say that we are studying a network that is describing the railway network of a country, with the vertices being railway stations and the edges the rail connecting the stations. If $l = 8$ it thus mean that one in average have to pass seven stations before arriving at the destination. The most famous example of the "smallness" of a network is the phrase "six degrees of separation" (Watts, 2004). In 1967, the social

psychologist Stanley Milgram performed an experiment by sending out letters to a few hundred randomly selected people in Boston and Omaha (in Nebraska) with the instructions to send it to a specific person in Sharon, Massachusetts, who worked in Boston. The receivers of the letters, and the subsequent letter holders, were only allowed to send it to people they knew on first-name basis. The results from the experiment came out as a surprise; the average geodesic length of the network was only about six, i.e. it took on average only six steps for the letter to reach the recipient. The type of network that Milgram studied is known as a *small-world* network. Based on the average geodesic length and the clustering coefficient one can divide networks into *small-world* and *large-world* networks, where small-world networks are characterized by a small average geodesic length and a large clustering coefficient.



Vertex, v	C_B	C_i	$1/(N-1)\cdot\sum d(v,w)$
1	4	1/3	7/5
2	0	1	8/5
3	1	0	9/5
4	11	1/6	6/5
5	2	0	8/5
6	0	0	10/5
		$C = 0.25$	$l = 1.6$

Figure 2.7. Beetweenness, clustering coefficient and average geodesic length, calculated for a small example network.

In the field of network theory there is also numerous research addressing the issue of synthesizing networks. In brief, the aim is to develop a scheme that generates networks with certain properties, either by a minimal model to generate a specific network structure or by models that generates networks that have the same structural properties as real-world networks. In the present thesis real-world networks are mapped "one to one" in order to create the model. Discussions or reference to this field is thus deliberately omitted. Furthermore, the network itself is rather static although the process it supports is highly dynamic. Holme (2004) gives a good overview of network models.

Dynamics of Network Models

The dynamic of the network is the removal or addition of vertices and edges and simultaneously measuring some chosen property of the network. 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. Some global property of the network, e.g. average geodesic length, is measured while the network is being attacked in succinct steps. For an example, see Figure 2.8. 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.

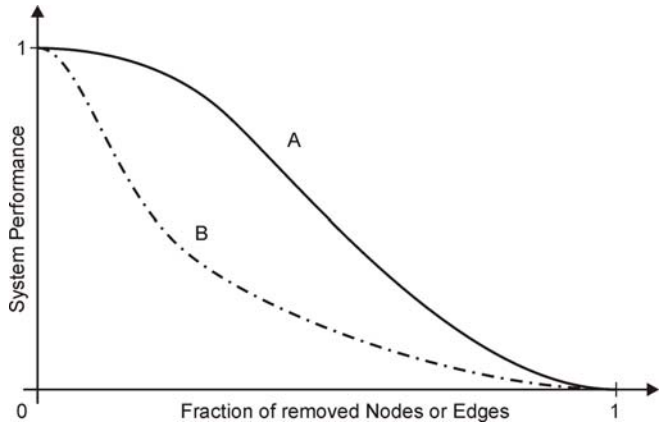


Figure 2.8. Measuring the system performance. On the vertical axis is the normalized performance of the network and on the horizontal axis the fraction of removed nodes or edges. Let the two curves, A and B, represent the system performance for two different attack strategies. Since the system performance drops faster for attack strategy B than for A, it can be stated that the system is more robust to attack strategy A than for attack strategy B.

Chapter 3

Electrical Power Systems

The aim of the research behind this thesis is to develop methods for risk and vulnerability analysis of technical infrastructure in general, and specifically for electric power supply. The focus has come to be on distribution systems rather than transmission. This is for several reasons. A key reason is that the major part of the outage time experienced by customers originates in the distribution system. This is also the reason that the new electricity law will have the largest impact on distribution network owners. Furthermore, distribution networks are often owned by municipalities, which have come to be in focus in most of the FRIVA-framework. The focus on distribution systems is however not a limitation, since the methods developed here can easily be implemented for higher system levels.

The chapter is intended for readers not well acquainted with electric power systems. It starts with a brief overview of the Swedish power supply, followed by an overview of electrical distribution systems. For further reading on electrical distribution systems, see Lakervi and Holmes (2003).

3.1 Brief Overview of the Swedish Power Supply

The Swedish power industry has gone through some rather radical changes during the last two decades, similar to the development in many other countries in Europe. Before the 1990s the generation, distribution, and marketing functions of the power system was tightly integrated in a few companies and with a rather high transparency between the companies. Since 1 January 1996, the electric power market has been deregulated in Sweden. This has lead to a slightly less transparent power industry and changes in legislative and regulatory mechanisms.

There are several actors in the Swedish power industry. At the national level, the main actors are Svenska Kraftnät (SvK), the Swedish Energy Agency (Energimyndigheten), and Swedish Energy (Svensk Energi). SvK, formed in

1992, is responsible for the national transmission grid and has the system responsibility of the Swedish electricity supply. The Swedish Energy Agency was formed in 1998 and is the regulatory body for the energy market and responsible for guiding state capital in research and development projects. Swedish Energy is a trade and interest organization for electric power companies in Sweden. At the regional level there are mainly three actors: E.ON, Vattenfall, and Fortum. These companies own and operate the regional networks and the major part of the generation capacity in Sweden. At the local level there are about 180 different distribution system companies owned mainly by corporations and local authorities. Regional and distribution network owners operate, since the deregulation of the market, in natural monopolies. Due to the monopoly situation, the Energy Market Inspectorate, sub department of the Swedish Energy Agency, therefore on a yearly basis evaluates the network tariffs against the actual performance of the network. At NordPool, the Nordic electricity market, electricity is traded in long and short term contracts by players on the Nordic market.

Electric power systems can be divided into three subcategories: generation, distribution, and consumption, similar to any other supply and demand chains in modern societies. Since it is difficult to store any greater amount of electric energy, there always has to be balance between generation and demand. SvK is responsible for this balancing. Electric power delivery networks are normally divided into three rather distinct levels of operation, depending on the power transfer capability and thus the voltage level the network is designed for:

- Transmission – National network
- Sub-transmission – Regional network
- Distribution – Local network

In Sweden the voltage level for the transmission system is 400kV - 220 kV. The transmission system in Sweden is interconnected to those of neighboring countries (Denmark, Norway, Finland, and Germany). The sub-transmission level has a voltage level of 130 kV - 40 kV. Distribution grids have roughly the size of a municipality and operate at a voltage level of 20 kV – 0.4 kV. The primary distribution grid operates at voltage level of 20 – 10 kV. All these networks are tightly interconnected which means that disturbances at higher voltage levels can easily traverse down to lower voltage levels. Disturbances on transmission system also easily traverse to the systems in the other Nordic countries. In Table 3.1 some key figures for the three levels of operation is seen.

Table 3.1. Key figures for the three levels of operation for the Swedish system.

Key Figures	Transmission	Sub-Transm.	Distribution
No. of companies	1	4	180
Tot. Revenue (kSEK)	3 283 000	6 920 000	20 670 000
Labour cost (kSEK)	---	123 000	2 280 000
Financial result (kSEK)	801 000	1 560 000	1 084 706
Overhead line (km)	15 000	31 480	222 270
Underground cable (km)	---	634	273 440
Interruption time (min)	2	20	140

* The figures for the transmission are from SvK yearly reports for the years 2005, 2004, 2003, and 2002 and are averaged for the years 2001-2005 (SvK, 2007). The figures for the sub-transmission and distribution are averaged for the years 2001-2005 (Swedish Energy Agency, 2007). The interruption time for the sub-transmission and distribution system is the average interruption time. The interruption time for the transmission system is based on energy not supplied. These figures should thus be seen as rough estimates of the interruption time.

A large portion of the Swedish power generation is connected to the transmission and sub-transmission system. The power is then transported in the transmission system to regional networks and further down to the consumers in the distribution systems. This top-down approach of power delivery systems is the prevailing design concept in Sweden. The main flow of power is from the north of Sweden, where hydropower generation is located, to southern Sweden where the bulk of the consumption is located. Denmark's production of electrical energy stems mainly from smaller generation sites connected to the sub-transmission or distribution system. This has lead to a new possible approach for the operation of the transmission system in Denmark. Sub-transmission systems with enough generation capacity to support the load in an area are seen as an autonomous cell. The Danish power delivery system can then be constructed by a numeral of these autonomous cells that is interconnected by the transmission system, i.e. a bottom-up approach.

The topology of the networks is different for the three levels of operation. Transmission and sub-transmission networks are built and operated in a meshed manner. In a meshed structure there is at all times several ways for electric power to go from a generation site to a customer or from an in-feed to the lower delivery networks. In these networks, one component malfunction *very rarely* leads to any consequences for customers. Distribution networks are to some extent built meshed, but are always operated radially. In a radial structure there is only one way for electric power to go from a generation site or an in-feed from higher levels to a customer. In these

networks, one component malfunction *always* leads to consequences for customers. The different use of structures is due to aspects of reliability, operational, and economical factors. Meshed networks are in general more reliable, more demanding to operate, and more expensive to build in contrast to radial networks.

Disturbances at the transmission level can lead to catastrophic consequences, as demonstrated by the national blackouts in Sweden in 1983 and 2003 (Kearsley, 1987; Larsson et al., 2004). Nevertheless does most of the interruption time for customers stem from the distribution network (see Table 3.1). In (Holmgren, 2001) the meantime between disturbances with unserved energy not caused by lightning is estimated to 58 days for the Swedish transmission system. For the distribution grid in Stockholm the meantime between disturbances with unserved energy is estimated to 109 hours.

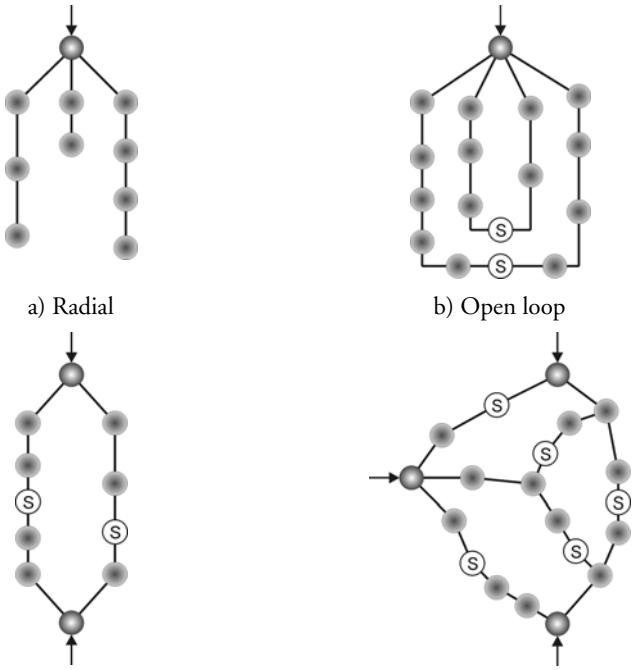
For power systems, it is often distinguished between system adequacy and system security. System adequacy is defined as the ability for the power system to supply demanded power and system security is defined as the ability of the system to operate normally in the event of disturbances (Chassin, 2005). The concept of system security in power systems can be seen, in some respect, as the antonym to system vulnerability.

3.2 Electrical Distribution Systems

Electrical distribution systems are spatially rather confined, typically the size of municipalities, and supply in average 50 000[2] people with electric power. In some distribution systems there are also smaller generating plants, based on: combined heat and power, hydro, and wind. These smaller generation plants are normally referred to as distributed generation, since they are spatially distributed at the lower voltage levels of the electrical delivery network. In recent years there has been a growing interest in using distributed generation as means for reducing the vulnerability of distribution networks to the loss of power from higher voltage levels. Operating a smaller distribution network or a part of a regional sub-transmission network disconnected from the transmission system is called island operation. A network with island operation capability and the possibility to prioritize power delivery to customers, e.g. to hospitals and local authority offices, would be less vulnerable to large-scale disturbances in the transmission system.

[2] 9 million people in Sweden and about 180 distribution system owners.

As stated earlier, distribution networks are operated in a radial manner although normally built with a meshed structure. These and other types of structure are shown in Figure 3.1. A distribution system is normally a mixture of several types.



a) Radial b) Open loop

c) Link arrangement d) Meshed

Figure 3.1. Examples of different distribution network structures. The nodes with arrows indicate in-feed points and the other nodes are substations where customers are connected. Nodes with an *S* indicate points where the network is normally sectionalized, i.e. normally open points.

Distribution networks in rural areas are mainly built with a radial structure, see Figure 3.1 a). A radial network is vulnerable to single component failures since it will render one or several downstream substations without power. If possible, distribution systems are therefore built with a meshed structure with open points, sectionalizers, at several locations in the network. At in-feed points and in larger substation there are also breakers installed for the outgoing feeders. The open-loop arrangement, see Figure 3.1 b), renders a more flexible and more reliable power supply to the substations. In case of a

component failure, sectionalizers can be opened in order to isolate the fault. By closing the normally open sectionalizer the substation will have power supply again. If the in-feed point malfunctions none of the substations will have power supply. The link arrangement in Figure 3.1 c) has the possibility to supply the substations from two different in-feed points. The most flexible arrangement is the meshed arrangement in Figure 3.1 d). This structure enables the rerouting of power supply from several in-feed points and through multiple ways.

The reason to operate distribution networks radially is due to both economical and operational factors. If the distribution system is situated in urban areas, the cost for a more meshed structure is feasible, due to the short distances and the amount of customers. In rural areas the distances is longer and there are less customers, requiring the less costly radial structure of the network. Faults in power system components can lead to up-stream components being destroyed and can be a hazard to humans and animals if the fault is not cleared in a reasonable time frame. In order to clear faulty components, distribution system must have protection equipment that complies with a certain protection scheme. The protection schemes are much less complicated for radial structures than for meshed structures, leading to a simpler operation of the system.

In the case of a single component failure, for example a short-circuit in a cable, the network is reconfigured if possible. This is done in order to shorten the interruption time for the customers. In distribution systems the reconfiguration is often made manually, and thus takes time. Still the reconfiguration time is generally much less than the time it takes to identify the fault location and to repair the fault, hence the benefit of having a more meshed structure.

When the storm Gudrun swept in over the southern parts of Sweden and, more or less, destroyed the distribution networks in some areas. The transmission grid was almost unaffected and the sub-transmission networks were slightly affected. During the first night roughly 650 000 customers were blacked out and it took about seven weeks before the last customer had power supply again (Johansson et. al. 2006). In January 2007, the storm Per swept in over Sweden, rendering about 170 000 customers without electricity. It took about two weeks before all the customers had power supply again. The storm Gudrun and the storm Per clearly show that distribution systems with overhead lines in forested areas are vulnerable to severe storms. A significant question arises: are there other vulnerabilities as easily exploitable?

Chapter 4

Modeling Technical Infrastructures

The modeling of any physical system 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 aim of the analysis. For network theoretical studies of technical infrastructures only the most fundamental part of the infrastructure is modeled, i.e. the system that facilitates the physical transportation of the services they provide. Supporting systems, such as legislative and financial, are omitted from the analysis since these mainly have impact on the infrastructure in longer time frames than the analysis aims for.

In order to give the reader a background of previous work in the field of network theory and electric power system, the chapter starts with a brief overview of recent research in this area. The subsequent sections present the approach of modeling technical infrastructures used for the research in the thesis.

4.1 Network Theory Applied to Electric Power Systems

There has been a wide interest in the application of network theory with the aim to analyze and understand complex systems such as the electrical power system. Studies of electrical power systems with use of network theory have mostly aimed at the transmission level. 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 in the area of electrical power systems and, recently, of urban street networks. Their overall approach regarding electrical power

systems is a model to study 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 be too generalized to straightforwardly be applicable to vulnerability analysis of electrical power systems. In later publications, the focus seems to have shifted towards spatial centrality measures of urban streets (Crucitti et al. 2005b, Porta et al. 2005, Porta et al. 2006) showing the applicability of network theory to differing technical infrastructures.

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. Chassin and Pose stress that analyses of electrical bulk power systems are computationally very complex when using standard power engineering methods. This will lead to the fact that only a small subset of all possible cases are examined, and even for these cases the topology of the system is simplified in many aspects. By using a network theoretical approach, it is more feasible to study much larger parts of possible subsets.

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. It is thus a measure that, in some sense, describes the loss for a substation to receive power from multiple generators. Seen from a substations point of view, the service is not affected as the possible connection to different generators decrease. The service is not degraded until the power delivery is cut off entirely. Assume for example that CL equals 50% for a power delivery network, which means that half of the possible paths between

generators and distribution substations are lost. What impact this has for the ability for a substation to receive power is not clear. In et al. (2007a) we propose a more appropriate measure called Customer Equivalent Connectivity Loss, simply describing whether a substation has power supply or not, see Chapter 5.

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 has shifted more towards game theory. The vulnerability of an infrastructure is defined as the probability of a system collapse that causes large negative societal consequences during a given time period. The framework for vulnerability analysis, as presented in the doctoral thesis, is essentially what is defined as a traditional risk analysis together with the concept of resilience in this thesis. He points out that: the relation between graph measures and vulnerability is not straightforward, important characteristics of electric power systems are lost when using a traditional network analytical approach thus not capturing the dynamical behavior of power grids, and actions taken to enhance the resilience of a network is not captured by traditional graph measures. His closing remarks in the licentiate thesis is an open questions whether graph modeling should be extended or if it is better to adapt existing power engineering simulation methods for vulnerability analysis. In the doctoral thesis, he declares that answer probably lies in between. He argues that vulnerability studies of power networks would benefit from cross-fertilization between electrical power engineering, risk and policy analysis and the mathematical modeling of complex systems.

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. He also discusses the possibilities to utilize network theory in order to study and understand cascading failures in power networks. He concludes that application of network theory in power systems is still on a theoretical level but believes 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.

4.2 System Modeling

In most network analytical approaches, the physical model of the system is seen as a part of the network model. For many network theoretical studies the nodes and edges are homogenous and only structural properties of the network is 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).

I argue for an approach of separating the network model and the physical model of the system. There are several advantages by separating the network model and the physical model. The tools and methods developed in this thesis can easily be applied to other technical infrastructures than the electrical power system. In order to do this, the only change is for the physical model, i.e. how the system reacts to perturbations and calculation of the consequences. The network model then serves as a common ground for the different technical systems and experts with domain-specific knowledge. The physical properties describing the system behavior are well researched for many technical infrastructures and should, where applicable, be used in the analysis. Furthermore, it will be easier to choose appropriate network and physical models depending on the aim of the analysis. Lastly, the separation gives a common platform, i.e. the network model, for all types of technical systems which possibly could be a fruitful approach to combine different technical infrastructures in the pursuit of understanding the effects of inter-dependencies, discussed further in section 9.2.

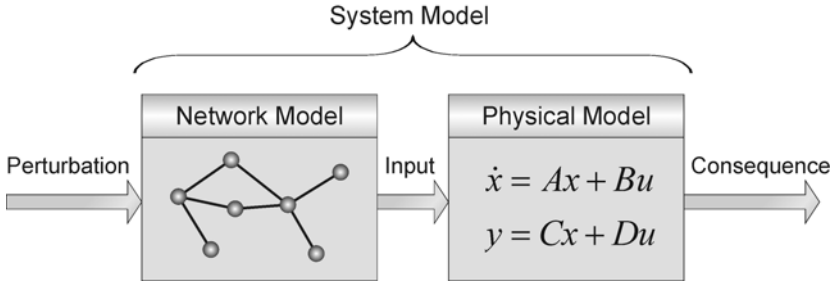


Figure 4.1. Schematic representation of the proposed division of the network model and the physical model for any given system representation.

4.3 Network Modeling of Distribution Systems

Distribution systems consist of various components with different functions, e.g. transformers, cables, overhead lines, breakers and sectionalizers. Network models only consist of two types of components, namely nodes and edges. In order to model an electrical distribution system as a network, several simplifications have to be made. The basis of the simplifications used in this thesis is to lump components that give rise to the same consequence into one network component. For example, a line and its line breaker will yield the same consequence when either one of them malfunction, that is loss of the possibility to transfer power, and are thus treated as one network component – an edge. This strategy is feasible also for components not operating as intended, since this will only move the fault to an adjoining component in the network model. For example, if a line breaker does not operate correctly, when the line has a fault, i.e. it does not open in order to clear the fault, the busbar protection has to operate in order to clear the fault. This corresponds to the malfunction of the node associated with the line. The resolution of the model can thus be adapted with regard to the aim of the analysis, rendering a flexible model. The drawback of oversimplifying the model is that it might be hard to assess where and what type of mitigating actions that are necessary to reduce the vulnerability of the physical system.

In this thesis, the structure of the distribution network is modeled as meshed in order to capture the built-in redundancy of the network, although it is radially operated. This approach leads to a slight underestimation of the vulnerability for the system, since the time it takes to reconfigure the network is not taken into account.

When mapping a real network into a network model one usually has to consider and deal with border effects that arise if a distribution system has possible in feed points outside the border of the studied network. In case of such in-feed points one can either disregard the possibility of alternative power routing, thus overestimating the vulnerability, or set them as in-feed point with limited capacity. The choice is depending of the detail of the system model utilized for the analysis, discussed in section 4.4.

By utilizing the network approach, it is more feasible to test the system for wider range of possible fault scenarios and thus a possibility to objectively assess the vulnerability of the system for a range of different perturbations.

4.4 Physical Modeling of Distribution Networks

In the thesis, it is differentiated between three different levels of detail of the physical modelling of the electrical distribution system. They range from a simplistic voltage model to a power flow model. All of the models are aimed at identifying which loads that are supplied with electricity when the network is perturbed, i.e. to asses if the service is available to the customer. Each step in the level of detail yields a better system performance model, and thus a more accurate description of the consequences that arise when the system is perturbed. The different models are referred to as: Voltage model, Capacity model, and Power flow model.

Voltage model

The simplest physical model of an electrical distribution network is to differentiate between node types, i.e. in-feed points, distribution nodes, and load nodes. The voltage model is a model that describes whether a load node, i.e. a substation with load, has connection to an in-feed node. In physical terms, it translates to if a substation has voltage. The power demand, power consumption, and capacity limits are all disregarded. One benefit of this model approach is that it only utilizes a simple search algorithm, and it is thus fast to calculate. Another benefit of the model is that it only requires a limited amount of input data. The downside is the obvious fact that by not regarding capacity limits in the electrical network, it might underestimate the consequences. This model is in essence what has been used in most network analytical studies of power systems. In the first paper by the author (Johansson et al., 2007a), this model was used.

Capacity model

The capacity model takes the basic physical limitations of an electrical network into account (e.g. Brown, 2002). The capacity model can be differentiated into two models depending on how accurately one wants to model the constraint of the physical system. The first one only considers the in-feed capacity (e.g. power ratings of in-feed transformers) and the power demanded by the substations (e.g. maximum power demand during a year). The second one also takes into account the capacity of edges (e.g. power ratings of cables and lines). In the third paper by the author (Jönsson et al., 2007), the former model was used for the analysis of an electrical distribution system. One benefit of the capacity model is that it takes into account basic physical limitations and is still quite fast since it is based on straightforward algebraic calculations. A drawback is that it requires more input data than the voltage model.

The algorithm used in the capacity model for the research in this thesis is based on a *breadth first* search algorithm. The capacity model takes the loads of the distribution substations and the capacities of the in-feed nodes into account. Two conditions have to be met in order for a specific distribution substation to have power supply. Firstly, there has to be a path between the substation and at least one in-feed node. Secondly, the in-feed nodes must have enough capacity to feed the distribution substations that are connected to them. Distribution of the capacities of the in-feed nodes is made by conducting a breadth first search, starting from the in-feed nodes. The power demands of the substations are subtracted from capacity of the in-feed node and the substations are flagged as supplied. When all the in-feed capacity has been consumed or when all substations with a path to the in-feed node are supplied, the next in-feed node, if any, is considered. The capacity of the next in-feed node is distributed using the same approach as above, except that the power demand of the substations that are flagged as supplied are not subtracted from the capacity of the in-feed node. The capacity distribution is continued until all substations that can be reached are supplied or until all available in-feed capacity is consumed.

Power flow model

The power flow model is widely used in the electrical power industry for analysis and design of electrical power systems. Power flow calculations constitutes of an iterative algorithm (usually Newton-Raphson) to calculate power flows and voltages across the network. The model requires full network data, such as: cable and line data, transformer data, and load data. The calculation time for a given network will be longer than compared to the capacity model. By using a power flow model the electrical properties of the network is accurately calculated and it is easy to identify if network constraints are violated. There are several books covering the subject of power flow calculations in electrical networks, see for example Glover and Sarma (1994). The power flow model has not been used in the research for this thesis, but is considered as a natural and valid direction for future research.

The three levels of physical models have different accuracy for describing how the system reacts to perturbations. Which model to use is decided by the aim of the analysis. It is nevertheless important that the physical model captures the essence of the consequences of interest when the system is perturbed. The descriptions of the three levels of detail also show how the implementation of physical models for other technical infrastructures can be carried out.

Chapter 5

Global Vulnerability Analysis

This chapter brings together concepts and theory described in the previous chapters to discuss an approach for analysing global vulnerability of technical infrastructures, with focus on electrical distribution systems. The aim of global vulnerability analysis is to describe the vulnerability of a network for different kinds of perturbations. It should be stressed that in order for the concept of vulnerability to make sense, it has to be related to a perturbation. An electrical distribution system in Sweden can, for example, be extremely vulnerable to earthquakes, tsunamis and antagonistic attacks while less vulnerable to technical failures, storms, and human mistakes. The likelihood of a perturbation exploiting the vulnerability or if the consequences are regarded as too high independent of the likelihood, determines whether or not mitigating efforts are necessary.

The approach for assessing global vulnerability of technical infrastructures is based on measuring the performance of the infrastructure model for different perturbations. The result of a study is presented in a plot with the performance of the network against the fraction of removed nodes or edges. By studying this plot, conclusions regarding the vulnerability can be drawn. A network is considered as vulnerable if the performance is highly degraded, e.g. there is a high degree of loss of function, due to small magnitudes of the perturbation. Since the vulnerability of the network is studied, the performance measure is initially zero and rises for higher magnitudes of perturbation. Figure 5.1 illustrates the basic concept of global vulnerability plots. The figure illustrates the system performance drop for three different kinds of perturbations, labelled A, B, and C. Since the performance drops more rapidly for perturbation A than for perturbation C, perturbation A is considered more harmful to the system than perturbation C. The system is thus more vulnerable for that type of perturbation.

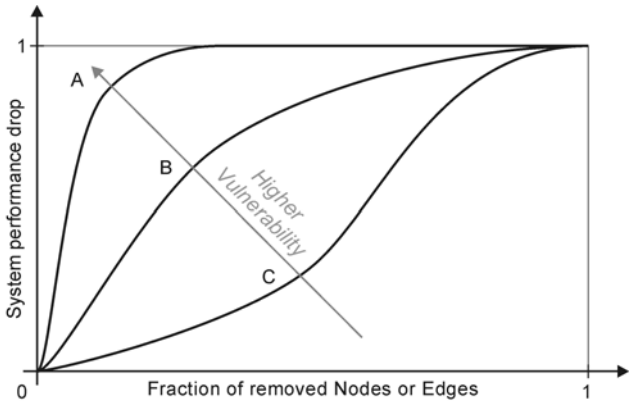


Figure 5.1. System performance drop for three different attack strategies: A, B, and C. The swifter the performance drops given the fraction of removed node or edges, the more vulnerable the system is for that perturbation.

5.1 Simulating Perturbations

The outcome of the vulnerability analysis critically depends on the how the perturbation is organized. In network theory, perturbations are achieved by removing nodes or edges, either randomly or in a targeted fashion. These are called *attack strategies*. Targeted attacks are the removal of network components in decreasing order of their criticality. The criticality of a node or an edge is usually described by a *centrality* measure, as presented in section 2.3. It is also possible to use non-topological criticality 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 power outtake or rate of loading. The attack strategies can be seen as a way to find middle states of the system. By assessing the corresponding consequences for these middle states, the vulnerability of the network is given, in analogy with section 2.1.

The attack strategies used in this thesis for global vulnerability analysis are random removal and targeted attacks based on centrality measures, yielding:

- Random removal of nodes or edges
- Removal of nodes in decreasing order of *initial degree*
- Removal of nodes or edges in decreasing order of *initial betweenness*
- Removal of nodes or edges in decreasing order of *recalculated betweenness*

To recapitulate from section 2.3; The degree for a node is equal to the number of edges connected to it and the betweenness for a node or an edge is given by the amount of shortest paths that passes through it.

In Figure 5.2 a simulation for an electrical distribution system with the attack strategy random removal of nodes is shown. 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 blue area contain 90% of the calculated consequences. The dotted blue lines illustrate maximum and minimum performance drop found in the simulations for the given fraction of removed nodes. The figure clearly shows the variability of consequences for a given fraction of removed nodes. If the number of simulations where infinite (or at least close to infinite), the most harmful way of removing nodes would be found.

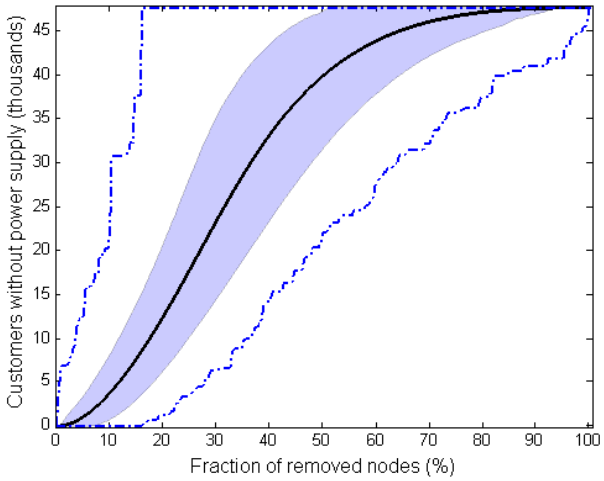


Figure 5.2. The results from a simulation with random removal of nodes for a electrical distribution system.

From one point of view, attack strategies can be seen as a way to estimate the range of possible performance drops with a limited amount of simulations, i.e. to assess the vulnerability of the system for different perturbations. From another point of view, they can be seen to simulate realistic perturbations. The attack strategies used in this thesis are quite coarse and describe possible types of perturbations rather than specific realistic perturbations. Random removal of nodes or edges can represent technical component failures.

Targeted attacks can represent antagonistic attacks or be seen as tests of how fast the system performance drops when components with decreasing order of centrality are removed. Since the perturbation models are quite simplistic, a natural development of the research in this thesis is to find models that are more realistic to their character, for example representing a storm. The use of more realistic perturbations would make it easier to draw conclusion regarding their probability to occur.

5.2 New Vulnerability Measures

Existing network analytic methods focus mainly on technical aspects of the electric system, i.e. the system's ability to withstand perturbations and recover from damages. I agree with the view proposed by Little (2002):

> *"… 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". (Little, 2002)*

It is thus necessary to have consequence measures that reflect the real consequences that arise when the service from an infrastructure is interrupted. In et al. (2007a) we proposed some new measures in an effort to come one step closer to capturing the societal consequences that arise when an electric distribution system is perturbed.

Customer Equivalent Connection Loss - CECL

CECL is a measure that describes the consequences of perturbations to a network. Customer Equivalent (CE) is a weighted measure that aims at capturing the societal consequences that the loss of service give rise to. In a power system, CE could for example be a linear combination of loss of power and the number of customers connected to a substation. It could also include a more general weighting in order to capture the importance of a customer, e.g. a hospital or a fire station yields a higher weight than a household. CECL is the fraction of CE that is without power when a network is perturbed, defined as:

$$CECL = \frac{CE_{loss}}{CE_{tot}} \tag{5.1}$$

It is always difficult to capture the consequence of interrupted services in a single measure. CE could nevertheless be a valuable tool in order to rank the value of the services to the customer in other terms than purely economical or technical. In Table 5.1, an example is given of such a ranking for a 10 kV electrical distribution system in a municipality. To achieve appropriate CE-factors, reflecting the societal consequences that arise due to interruption of supply, is a complicated and not easily achievable task. For the scope of this thesis the goal of providing a possible way of incorporating societal consequences is however considered fulfilled.

Table 5.1 Example of the use of customer equivalents (CE).

Type of customers connected to the substation.	Number of customers	CE-factor	Total CE for the substation
Fire Station	1	800	800
Hospital	1	1000	1000
Household – District heating	40	0,8	32
Household – Electric heating	10	1,2	12
Industry	1	200	200
Local authority building	2	200	400
Wastewater treatment plant	1	400	400

Societal Vulnerability Coefficient - SVC

Societal Vulnerability Coefficient (*SVC*) is a measure that facilitates the assessment of a networks vulnerability to perturbations. The SVC is the area under the performance curve shaped by the CECL-curve. If both the performance measure and the fraction of removed nodes or edges are normalized, then $0 \leq SVC \leq 1$. This measure can be used to compare the systems vulnerability for different perturbations or to compare the vulnerability of different systems given a specific attack strategy. A system with a low SVC is generally less vulnerable than a system with a high SVC. A system that is robust to small perturbations and vulnerable to large perturbation can have the same SVC as a system where the opposite is true. This should be kept in mind when using the SVC measure. Sometimes it may not be 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.

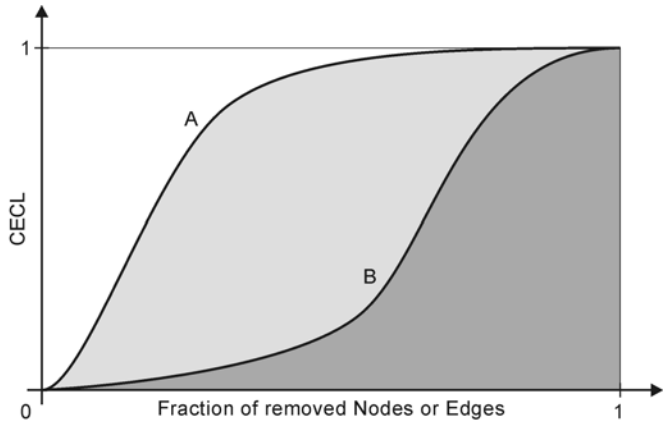


Figure 5.3 CECL as a function of the fraction of removed nodes or edges. The two curves, A and B, could represent either two different attack strategies on the same system or the same attack strategy applied to two different systems. Since $SVC_A > SVC_B$, attack strategy A is more harmful than attack strategy B or, in the case of two different systems, system A is more vulnerable than system B for the given attack strategy.

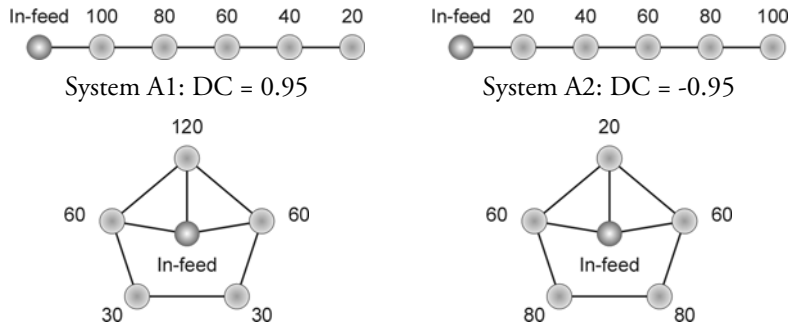
Design Coefficient - DC

The *design coefficient* is the correlation (more specifically the Pearson correlation) between the relative vulnerability for a node, v_j, and its importance, i_j. The relative vulnerability for a node is given by the fraction of nodes/edges that have been removed when it loses its function. Since the order for which a node loses its function might differ between simulations, it is necessary to consider the mean fraction of removed nodes/edges, $\overline{v}_j$. The importance of a node can be the number of customers equivalents that are serviced by that node. The DC measure is given by:

$$DC = r\left(\overline{v}_j, i_j\right) \tag{5.2}$$

For a distribution system the DC show, in a wider sense, whether the network 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 nodes supplying important nodes lose their function early when the network is perturbed. It should be noted that the DC-measure does not describe the robustness of the network. It only

describes the relation of how vulnerable a node is in relation to how important it is, as defined by the design of the network. The vulnerability of a node is given by the averaged order it loses its intended function when the network is perturbed. This means that an extremely meshed and redundant distribution network might have a lower DC than a radial network. The concept of the design coefficient is illustrated in Figure 5.4.



System A1: DC = 0.95 System A2: DC = -0.95

System B1: DC = 0.79 System B2: DC = -0.75

Figure 5.4 Example of DC values for four different systems. The figure above each node denotes the number of customers connected to that node, the importance measure. The vulnerability values are based on 1000 simulations with random node removal strategy. The only difference between system A1 – A2 and B1 – B2 is the placement of the customers, but it still makes DC go from a high positive value to a high negative value. That the DC value does not describe the overall robustness of the system is apparent when comparing system A and B.

5.3 Graphical Visualization

Technical infrastructures are of interest for a wide range of persons with differing background and knowledge, e.g. politicians, emergency personnel and decision-makers. To facilitate the discussion between persons working in different fields it is very important to present the vulnerability of an infrastructure in an easy understandable form. GIS (Geographical Information Systems) has become a central tool for many local, regional and national authorities due to this reason. The results from a vulnerability analysis can be presented as geographical vulnerability maps, and even incorporated in GIS-software. These maps can for example facilitate emergency response planning, since areas where emergency needs are likely to arise are easily identified These maps can be used with other GIS-data over

the population in order to see what type of population is most likely to be without power when the power system is severely disturbed. If vulnerability maps for different technical infrastructures (e.g. telecom, district heating, and roads) are available it will be possible to find areas where all of these infrastructures are weak and where emergency needs might arise.

The vulnerability map in Figure 5.5 is an interpolation based on the vulnerability of a node to the attack strategy random removal of nodes. The vulnerability for a node is given by the mean fraction of nodes/edges that have to be removed before it loses its function, based on several simulations. The figure shows, not surprisingly, that meshed areas close to in-feed points are less vulnerable than radial areas far from in-feed points for the given attack strategy.

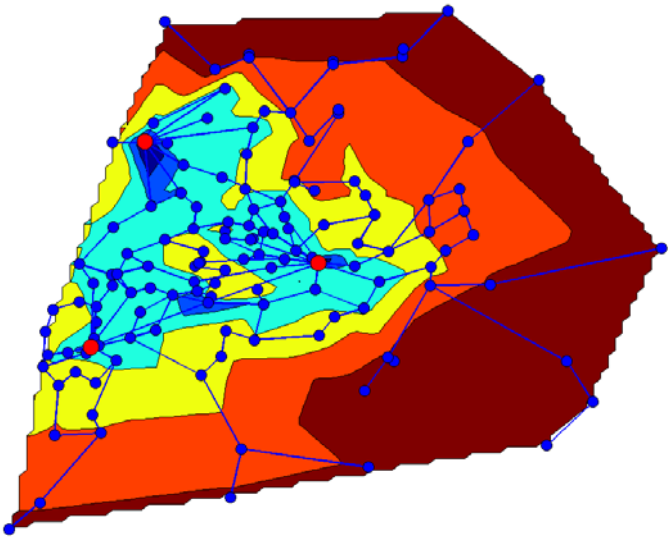


Figure 5.5. Vulnerability map of an electrical distribution system in a small city. The red and slightly larger nodes indicate in-feed nodes, the blue nodes indicate a substation. The blue lines indicate that there is a cable or an overhead line connecting the substations. The red areas are more vulnerable to the loss of electric power while the blue areas less vulnerable.

5.4 Risk and Global Vulnerability

The identification of a systems vulnerability to different perturbations is extremely important. The global vulnerability analysis gives a notion of the possible consequences that can arise when the system is perturbed. The analysis also gives important information regarding the type of perturbations the system is vulnerable to. In order to assess the risk of the system, the next step is to address the likelihood of threats or hazards exploiting the identified vulnerabilities. More realistic perturbation models would lead to a better estimation of the probability of occurrence. With the knowledge of both the consequences and the probability of the perturbation exploiting the vulnerability, it is straightforward to attain a risk analysis, in analogy with section 2.1.

Chapter 6

Critical Components

The global vulnerability analysis described in Chapter 5 yields important information about the overall vulnerability of the network. Another important aspect is to identify components that are critical for the system performance. These critical components point out where mitigating efforts should be focused in order to reduce the vulnerability or the possibility of a threat exploiting the vulnerability. The criticality of a component is described by the consequences that arise when it fails to perform its intended function. A component is represented by either a node or an edge. The node or edge might in turn represent one or several physical components. In this chapter, concepts and theory described in Chapter 2 and Chapter 3 are brought together to discuss how to assess what is here termed local vulnerability of technical infrastructures.

There are several issues regarding identification of critical components in large-scale technical infrastructures. Technical infrastructures are, in general, rather complicated systems in respect of the sheer number of components they consist of. It is thus important to employ a systematic approach for the identification, in order to cover the scenario space. The identified critical components or set of components also provides input regarding which components that should be studied in further detail regarding their probability to malfunction. The purpose of such a more detailed study is 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 vulnerability of a system can be described by sets of single or simultaneous component malfunctions. The malfunctioning of the components is regarded as a perturbation to the system. It is then straightforward to discuss the vulnerability of a system to single or multiple component malfunctions. Exhaustive consequence calculation for all possible combination of component malfunction will also yield the maximum

consequences for different orders of simultaneous component malfunction. The vulnerability of the system for one, two, three, or more simultaneous components malfunction is thus given. The systematic search and the calculation of the consequences for sets of single or simultaneous component malfunctions can be seen as a way to identify, for the given perturbation, all possible middle states of the system. The vulnerability of the network is thus given, in analogy with section 2.1.

6.1 Criticality

Components or sets of components are defined as critical if they give rise to large consequences when they fail to perform as intended. It is important to note that the probabilities of the components or sets of components to malfunction are *not* included in the criticality definition. The reason for excluding the probability is twofold. Firstly, it is due to the inherent problems of finding a true probability for each and every component in a technical infrastructure. Furthermore, it is impossible to find accurate probability measures for unlikely events. For example, what is the probability that a group of civilians actively sabotages a substation, rendering 25 000 customers without electricity?[3] Secondly, introducing technical probabilities too early in the analysis phase leads to the possibility that severe but less likely deficiencies are overlooked.

The criticality of a component can stem from the criticality of the component itself or from the fact that it is included in many failure sets with large consequences. 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, *N*, is equal to the failure set size, i.e. a third order failure set consists of three components that are out of function simultaneously. A component that is critical for certain set sizes is defined as a N:th order critical component.

6.2 Synergistic Consequences

When analyzing a network for higher order of criticality, the number of possible failure sets will grow rapidly with the order of the failure sets. In fact the number of possible fault scenarios will be:

[3] This incident happened in Malmö, Sweden, the 7 October 2006. A group of civilians threw in a floor lamp, short-circuiting the transformer station.

$$\frac{n!}{(n-k)!\cdot k!} \tag{6.1}$$

where n is the number of components in the network and k is the size of the failure set. For a network consisting of 800 components the number of failure sets will be: 800 for first order, about 314 000 for second order, and roughly 85 000 000 for third order failure sets.

To be able to more easily identify critical components and for what order they are critical, we introduced in Jönsson et al. (2007) the term *Synergistic consequences*. 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.

A failure set, F, of a size larger than one can be divided into subsets. Failure sets of a size larger than two can be divided in several ways; let F^i denote a specific division and S^i_m, where m = 1, 2, …, denote the subsets for that division. 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. A failure set has a synergistic consequence if and only if its total consequence, $C(F)$, is greater than the sum of the consequences for the subsets of F, i.e. $C(S^i_1)$ +…+ $C(S^i_m)$, *for all possible divisions* F^i:

$$\begin{aligned} &C(F) > \sum_{k=1}^{m} C(S_k^i)\ \forall F^i : \\ &S_1^i \cap \ldots \cap S_m^i = \varnothing,\ S_1^i \cup \ldots \cup S_m^i = F \end{aligned} \tag{6.2}$$

A failure set with a non-zero synergistic consequence is referred to as a *synergistic failure set*, F_{syn}, and a failure set without a synergistic consequence is referred to as a *non-synergistic failure set*, $F_{non\text{-}syn}$. The magnitude of the synergistic consequence of F_{syn}, is the difference between the total consequences of F_{syn} and the sum of the consequences of the subsets for the particular division with the largest sum:

$$C_{syn}(F_{syn}) = C(F_{syn}) - \max_{\forall F_s^i}\left(\sum_{k=1}^{m} C(S_k^i) \right) \tag{6.3}$$

The fraction of the synergistic consequences for a failure set can be calculated as:

$$f_{syn} = \frac{C_{syn}(F)}{C(F)} \tag{6.4}$$

What signifies a synergistic consequence is that it cannot be referred to the individual subsets of the failure set. Instead, synergistic consequences refer to the consequences arising due to the fact that all the failures in the set occur simultaneously, i.e. the consequences that arise in addition to the consequences due to the individual subsets. For example, synergistic consequences of third order failure sets cannot be referred to the consequences of its size 2 and 1 subsets. Synergistic failure sets is thus sets with consequences higher than what can be expected by looking at the consequences of the individual components in the set.

6.3 Ranking Critical Components and Failure Sets

In Jonsson et. al. (2007) a way of ranking the criticality of single components and combination of components is proposed. One way to rank the criticality of failure sets is to base the ranking solely on the consequences they give rise to. Alternatively, it can be done by utilizing the synergistic consequences in combination with the total consequences. The benefit of this method is that the top-ranked failure sets will be those that are not easily identified by the knowledge of the consequences that the individual components in the failure set give rise to. Furthermore, ranking failure sets according to the magnitude of their synergistic consequences implies screening out of some failure sets with high consequences, but whose consequences to a large extent stems from subsets that in themselves cause the large consequences. Such screening is plausible since these subsets have already been identified when systematically going through failure sets of smaller sizes. The identification of interesting failure sets can be simplified by using a plot with total consequences on the horizontal axis and the fraction of the synergistic consequences on the vertical axis.

Ranking the criticality for failure sets as described above is quite straightforward. However, it is also valuable to establish a criticality ranking of single components, which is not as straightforward. One possible way is to use the average consequences of all sets that contain a specific component. Consider two simultaneous component malfunctions. The criticality of a specific component is then seen as the vulnerability of the system to failures

in the specific component *and* one other component. There are generally many failure sets of size two that includes a specific component and each failure set is associated with a consequence. This metric can thus be interpreted as the average consequences due to the failures of a specific component *and* another component chosen at random.

Another possible way to rank the criticality of a component is to use the synergistic consequences, C_{syn}, for the failure sets the component is involved in. A metric that indicates which components that are the main contributors to the synergistic consequences for a certain failure set size is desirable. Such a metric is presented in equation 6.5.

$$Contribution_{size=k}(Comp_i) = \frac{\sum C_{syn}(F \mid Comp_i \in F)}{\sum C_{syn}} \qquad (6.5)$$

where $Comp_i$ is a specific component and k the size of the failure set. The metric expresses the contribution of a specific component's synergy 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 metric, indicating that this component deserves further attention.

Figure 6.1 is used to exemplify terms and methods described in this chapter. The network consists of six nodes, one in-feed node and five load nodes, and seven edges, i.e. thirteen components in total. To calculate the consequences, the voltage model as described in 4.4 is used as the physical model, i.e. a load node is supplied as long as there is a path between it and the in-feed node. Each load node has the value of one customer equivalent and the in-feed node has zero customer equivalents.

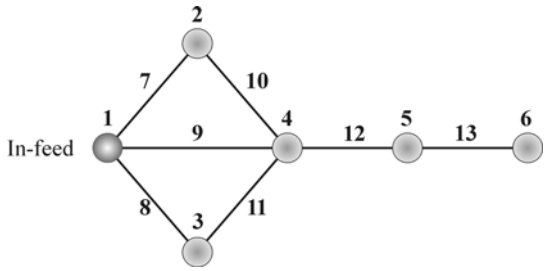


Figure 6.1. Example network of an distribution system. The numbers in the figure correspond to the component number of the specific node or edge.

Three sizes of failure sets are considered for the example network; 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 9 sets, respectively. In Figure 6.2 a scatter plot of all synergistic failure sets of size 2 and size 3 is presented. The figure shows that some failure sets give rise to large consequences but 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. This is evident when considering the [4 8] set in Figure 6.1. In this case, 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 5 and 6. Only the power loss to node 3 constitutes a synergistic effect. It is seen that the failure set [7 8 9] is critical (maximum consequence) with a 100% 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 lead to the same consequences but only has 20% synergistic consequences, because most of the consequences stems from the critical subsets [4 7] and [4 8], which in turn to a large extent derives from the critical component [4]. These scatter plots can thus be used to identify failure sets of special interest, i.e. sets with large consequences and with a large synergistic fraction.

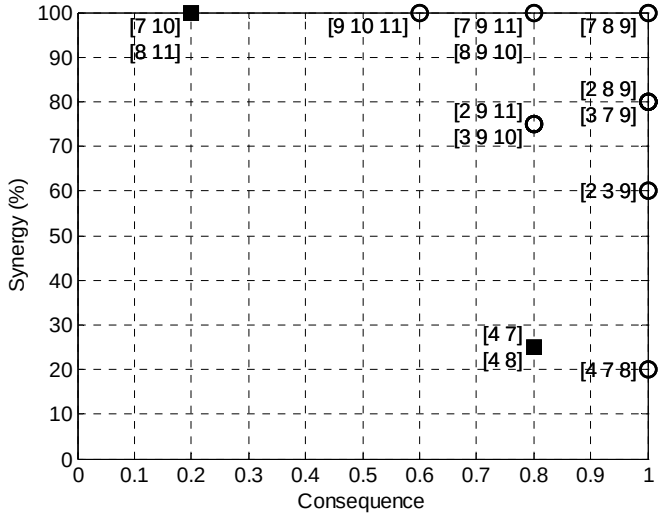


Figure 6.2. Consequence-synergistic scatter plot of synergistic failure sets of size 2 (filled squares) and size 3 (circles). The consequences of the failure sets, C(F) are presented on the horizontal axis and the fraction of synergistic consequences, f_{syn}, is presented on the vertical axis.

In Table 6.1 the information from the scatter plots are 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% are listed. The table shows that component 1 is the individually most critical component 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 set 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.

Table 6.1. Ranking of the criticality of failure sets.*

Size = 1		Size = 2			Size = 3		
F	C(F)	F	C(F)	fsyn (%)	F	C(F)	fsyn(%)
[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. Only the synergistic failure sets are presented for size 2 and 3 failure sets.

In Table 6.2 the criticality of individual components is presented. The average consequences are used as the criticality metric. The table shows that some components are very critical in themselves, such as component 1 and 4. Ensuring that such components are robust should be the primary concern in any vulnerability reduction activity. However, for this type of ranking it is hard to draw conclusions regarding for which failure set sizes a component becomes critical. Another drawback with this type of ranking is that the averaged consequences will converge for higher order criticality. This will have implications for deciding the importance of a component. For example, Component 7 and 8 are both more critical than component 9 for 2:nd order criticality. For 3:rd order criticality, component 9 is more critical than component 7 and 8. The differences of the average consequences is not significant and it is hard to tell for which order a component becomes critical

Table 6.2. Criticality of components in single and multiple failures.

Component	1:st order		2:nd order		3:rd order	
	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

In Table 6.3 it is easier to identify for which failure set sizes a component becomes critical. In this table the contribution of different components to the synergistic consequences is presented 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 smaller sizes. If three simultaneous failures are deemed possible the component deserves special attention. This type of ranking facilitates the identification of critical components for which robustness against perturbations are important.

Table 6.3. Component contribution to the synergistic consequences.

Component	2:nd order		3:rd order	
	Contribution (%)	Rank	Contribution (%)	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	---

6.4 Risk and Critical Components

The criticality of a component, or a set of components, has been defined as the vulnerability of the system to failures in these. It is important to note that only the consequences of failures are included in the notion of criticality. The identification of critical components and critical failure sets are important in order to assess the vulnerability of a system. The next step is to assess whether or not mitigating efforts are necessary to reduce the vulnerability. This step requires an estimation of the probability of perturbations exploiting the vulnerabilities. The criticality measure can be used to establish a priority ranking for which components that 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 for quantifying the probability of simultaneous failures, especially for common cause failures and malicious attacks. This is in addition to the apparent difficulty in finding a true probability for the failure of each and every component in a network. Instead of trying to identify the phenomena that lead to failures and try to derive which components that might be affected, it is argued for identification of component failures that cause severe consequences for the system as a whole and then consider whether these components can fail simultaneously, for example by a common cause.

It is not apparent that the likelihood of single or simultaneous component failures needs to bee addressed in a quantitative mathematical manner. The consequences that arise might not be acceptable to the society, leading to a decision of mitigating efforts although vague conception of the probability of occurrence. For most of the critical components, however, economical forces will lead the analyst into the need of a more thorough estimation of the probability of occurrence, thus embracing a risk-based approach of the analysis.

Chapter 7

Empirical Studies

The goal of the methods presented in this thesis is to facilitate vulnerability analysis of technical infrastructures. It is worth reflecting over the fact that the methods presented only cover a part of the efforts that are necessary for a full risk and vulnerability analysis of a technical infrastructure. The research has its focus on the most fundamental technical aspect of assessing the vulnerabilities of technical infrastructures, namely the vulnerability of the network. The electrical distribution system has served as the test case system to evaluate these methods.

In order to test the feasibility and applicability of the methods suggested in the thesis, they are applied to real electrical distribution networks in this chapter. First, the method to assess global vulnerability is demonstrated using the distribution system in two municipalities. Then critical components are identified for a distribution system in a different municipality.

Although the methods are demonstrated on the distribution system level, I argue that they are, with slight modification, just as valid for higher levels of the power distribution system hierarchy. The modification necessary is the use of a more detailed physical representation. The modification will render better consequence calculations and the ability to evaluate the possibility of cascading failures. The framework put forward for how to assess the vulnerability of technical infrastructure networks will still hold.

7.1 Global Vulnerability Analysis

The two electric distribution systems are referred to as system A and system B, like in Johansson et al. (2007a). The networks are located in two Swedish municipalities, both with a population of approximately 30.000. 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 the 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 the analysis, all breakers and sectionalizers in the normally radially operated network are treated as closed. This represents an ideal situation where the power can be rerouted instantaneously. In reality, however, such rerouting might be delayed since sectionalizers are manually operated. The system model used in the analysis is the voltage model as described in section 4.4.

The two distribution grids differ in that system B is only a part of a larger distribution system, i.e. it extends across the boundaries and connects to the distribution system in other municipalities as well. Sectionalizers are located in these boundaries, but in contrast to the other sectionalizers 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, since the voltage model is used. 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.

Network Characteristics

In Table 7.1, some basic network characteristics for the distribution system are presented. As a comparison, some network characteristics for three transmission systems are also given (Sun, 2005). The distribution grids have lower average node degree, lower clustering coefficient, and higher average geodesic length compared to the Western American Transmission system. This implies that the structure of the distribution systems have a more radial structure than the transmission system. The medium average node degree, high average geodesic length, and medium clustering coefficient suggest that the North Chinese transmission network has long radial feeders or is sparsely meshed. The Center Chinese transmission system seems, accordingly to its topology, be rather similar to a Swedish distribution system.

Table 7.1. Basic network characteristics of the two electric distribution systems and three transmission systems.

Network characteristics	System A	System B	Western America	North China	Center China
No. in-feed nodes	7	8	---	---	---
No. transmission nodes	191	442	---	---	---
No. distr. substations	568	830	---	---	---
Total no. nodes	766	1280	4941	8092	2379
Total no. edges	822	1342	6594	9018	2756
Average node degree	2.15	2.10	2.67	2.23*	2.32
Average geodesic length	22.1	22.9	18.7	32.0	21.08
Clustering coefficient	0.00218	0.00461	0.080	0.0017	0.0044

* This figure is 2023 in (Sun, 2005), which seems incorrect. Calculation of the average node degree yields 2.23.

Attack Strategies

Seven attack strategies for the removal of nodes and edges are used:

- Random removal of nodes
- Random removal of edges
- Removal of nodes in decreasing order of initial degree
- Removal of nodes in decreasing order of initial betweenness
- Removal of edges in decreasing order of initial betweenness
- Removal of nodes in decreasing order of recalculated betweenness
- Removal of edges in decreasing order of recalculated betweenness

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 presented in section 2.3. However, instead of calculating the shortest paths between all pairs of nodes, the shortest paths between any in-feed point or generator and all other nodes are calculated. 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 since it is the vulnerability of the distribution system that is of interest and not the systems vulnerability to the loss of in-feed. The results from the simulations are based on averaged values of 1000 simulations for random removal and 100 simulations for the other strategies. The random removal strategy is a

probabilistic attack strategy that requires a higher amount of simulations than the other attack strategies, which to a larger degree are deterministic.

Simulation Results

The most harmful removal strategy for system A is, as in correspondence with other network theoretical studies of power systems, the recalculated betweenness, see Figure 7.1. For this strategy, all customers have lost voltage supply after the removal of 5.3% of the nodes and 5.2% of the edges. The strategy based on initial betweenness is only slightly more detrimental than the random based removal. Initial node degree removal is more harmful than initial betweenness and random removal but less harmful than recalculated betweenness.

For system B the most harmful removal strategy is the same as for system A, recalculated betweenness, see Figure 7.2. For this removal strategy, all customers have lost voltage supply after the removal of 4.2% of the nodes or 4.2% of the edges. A removal strategy based on initial degree is more harmful than random and initial betweenness. In Figure 7.2, 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.

Initial betweenness turns out not to be a particularly harmful strategy, 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 that 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 all are critical. 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 node and edge based removal strategies are very similar for both systems A and B. The reason is that the systems are mainly radially fed with limited meshed structures. For the remaining of the analysis, the focus is on node-based removals. Much of the discussion is, nevertheless, equally applicable to edge-based removals.

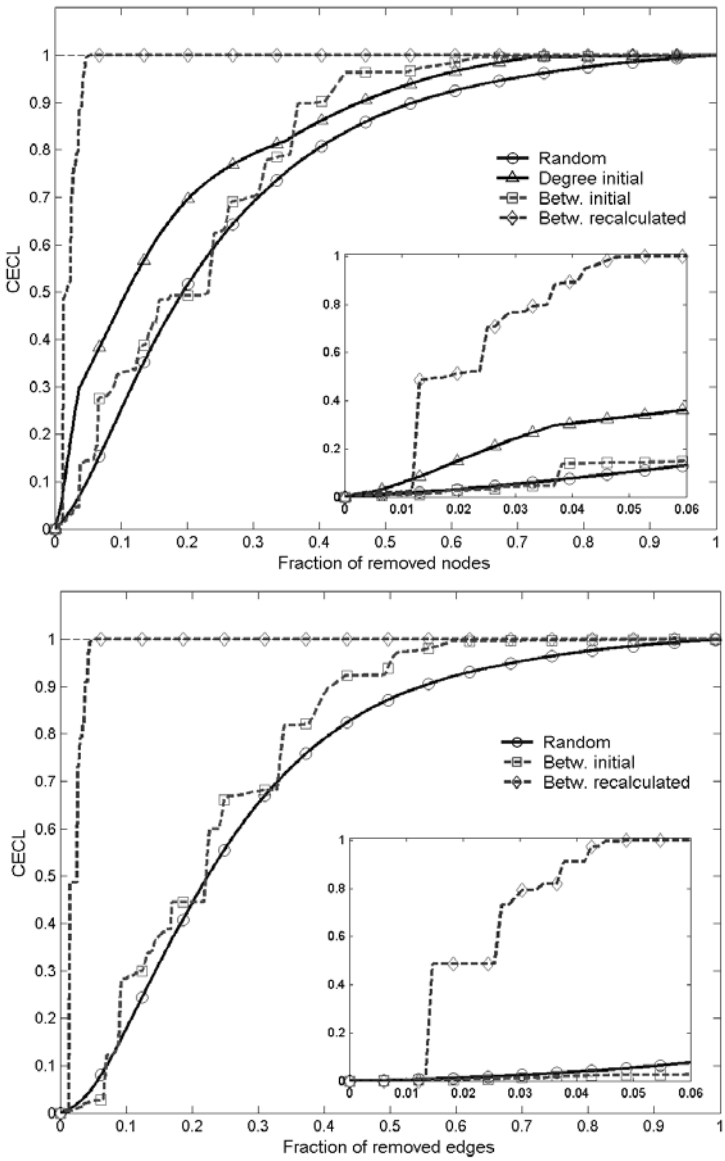


Figure 7.1. CECL, for different removal strategies, as a function of the fraction of removed nodes (upper) or edges (lower) for system A.

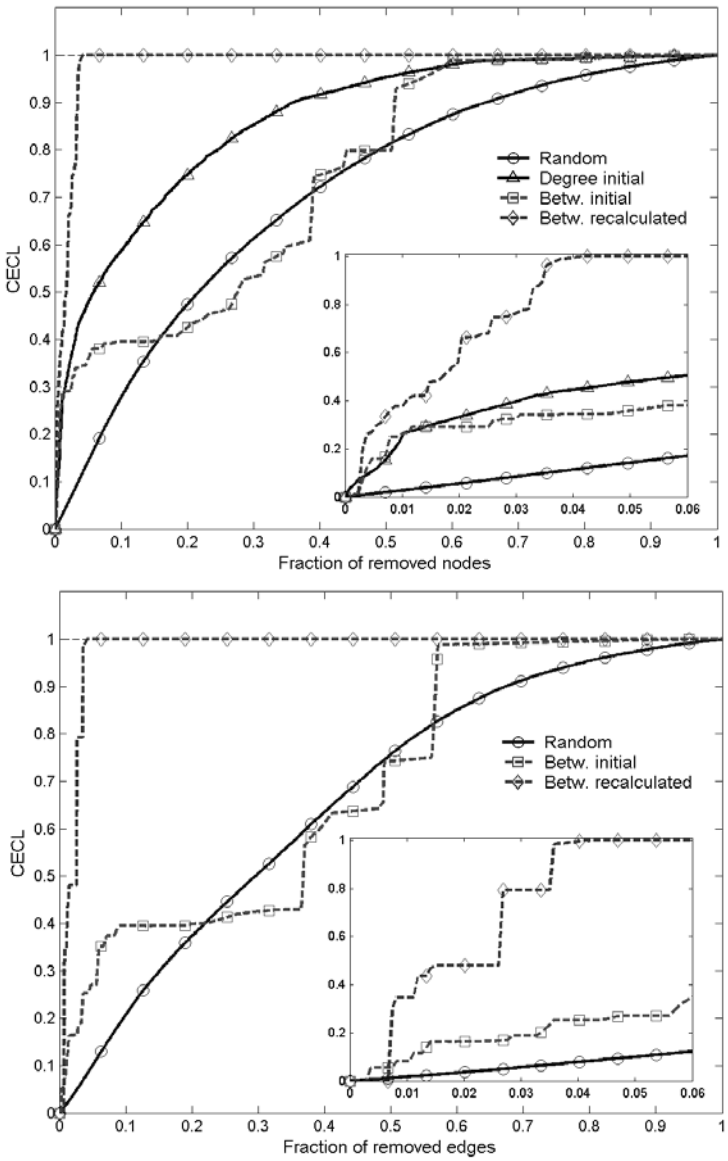


Figure 7.2. CECL for different removal strategies as a function of the fraction of removed nodes (upper) or edges (lower) for system B.

The vulnerability of the two systems for the different attack strategies is very similar in accordance with Figure 7.3. The main reason is that the general 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 initial degree, since the curve for system B is constantly above the curve of system A. Thus, system A is more robust to that type of perturbation, which is confirmed by comparing the SVC in Table 7.2. 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, except for recalculated node and edge betweenness. However, Figure 7.3 shows that system B is more vulnerable than system A for perturbations lesser than about 13% of removed nodes, but more robust to perturbations above 13%. Hence, it is important to note that the SVC measure cannot be used to draw conclusions about whether a system is vulnerable to small perturbations but robust to large, or vice versa. It is calculated for all magnitudes of the perturbations, i.e. from no perturbation to maximum perturbation, and it does not consider the fact that very large perturbations might not be realistic for some systems. If very large perturbations are not realistic, the SVC measure can be calculated for a smaller fraction of the CECL-curve.

As can be seen in Table 7.2 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 voltage supply to substations to 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 7.2 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.

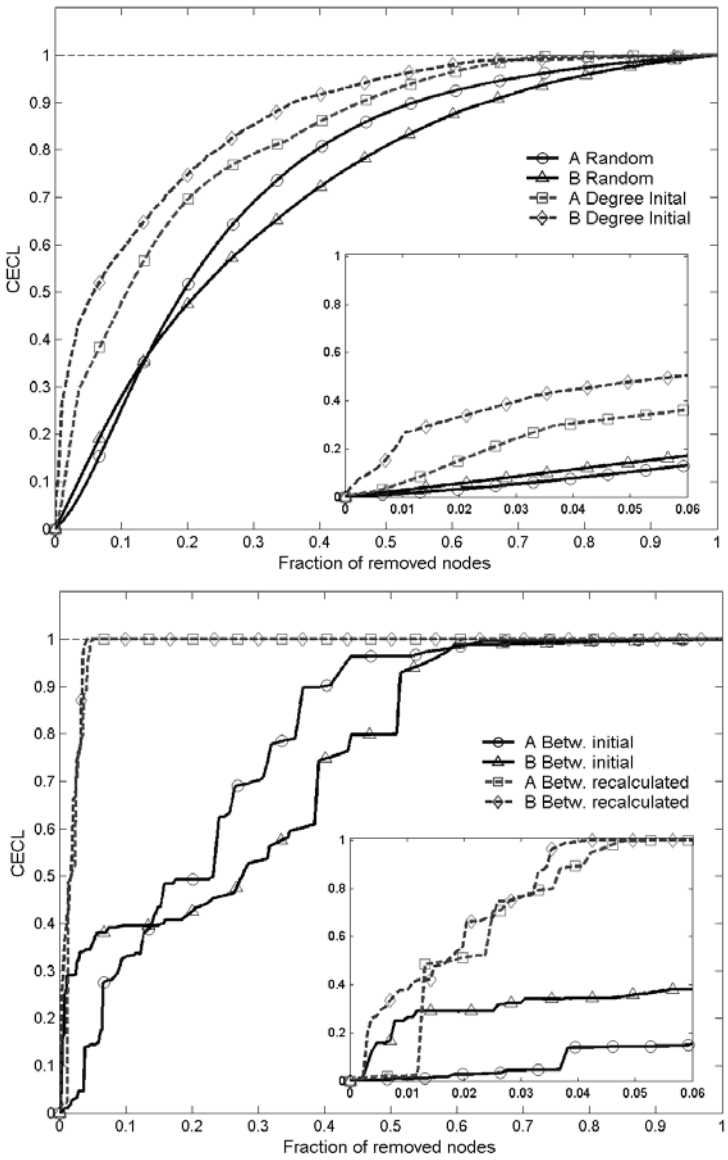


Figure 7.3. Comparison of system A and system B for different removal strategies. Random and initial degree removal of nodes (upper). Initial and recalculated betweenness removal of nodes (lower).

Table 7.2. SVC and DC presented for the different attack strategies.

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

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

Conclusions

The study has shown the applicability of the method to assess the global vulnerability of a system to different perturbations. The CECL-plots for the different types of perturbations clearly show that the systems might be robust to some perturbations but highly vulnerable to others. It is thus important that the vulnerability is specified for certain perturbation for the concept to make any sense. The perturbation models used in the analysis are rather coarse and more realistic perturbations (such as hard weather and ice storms) would be of interest, especially if it is desired to differentiate between different vulnerability mitigating investments. The study further showed that system B is in general less vulnerable to the applied perturbations and has a more robust design compared to system A. These conclusions corresponds well with the fact that system A can be characterized as a rural network while system B consists of both rural and urban networks.

7.2 Critical Components

To test the applicability of the method for identification of critical components described in Chapter 6, a study was carried out on a 11 kV electric distribution system in a Swedish municipality. The system is composed of 352 nodes and 451 edges, i.e. 803 components in total. The system is located in an urban area with underground cables only. 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 substations are modelled as nodes and the bus bar breakers are modelled as edges. The MV/LV 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 on 47 523 customers. An overview of the distribution system is given in Figure 7.4.

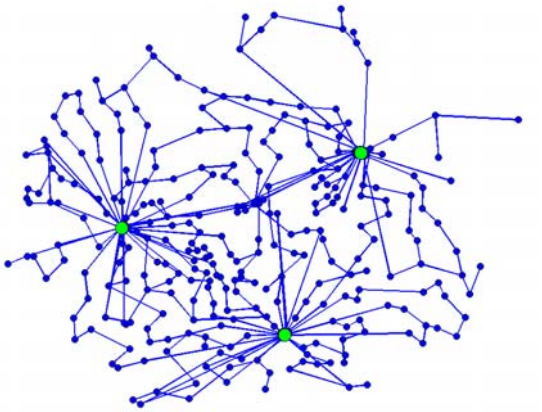


Figure 7.4. Overview of the electric distribution system. The larger green circles indicate in-feed nodes and the smaller blue circles indicate load nodes and transmission nodes.

System representation

The physical model used for the analysis is the capacity model, as described in section 4.4. The distribution system is radially operated but built meshed, which allows reconfigurations to take place in case of failures. In this analysis, any normally open sectionalizers are modelled as closed. This assumption leads to an idealised system representation since it assumes that reconfigurations are instantaneous. The calculated consequences are in some sense permanent until components are operational again, since no further rerouting is possible.

At each load node (i.e. MV/LV substations) the aggregated number of customers and the power demand are 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. A simple mean of these variables are used to estimate the CE of each load node, since both these parameters are important indicators of the consequences that arise when the power supply is interrupted. Thus, for load node *i* the CE is calculated as:

$$CE_i = \frac{\left(\frac{N_i}{\overline{N}} + \frac{P_i}{\overline{P}} \right)}{2} \tag{7.1}$$

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 normalised 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. In Figure 7.5 the power demand, the number of customers, and the calculated CE for the substations carrying load are shown. It is apparent that the CE-measure reflects both the customers and the power demand.

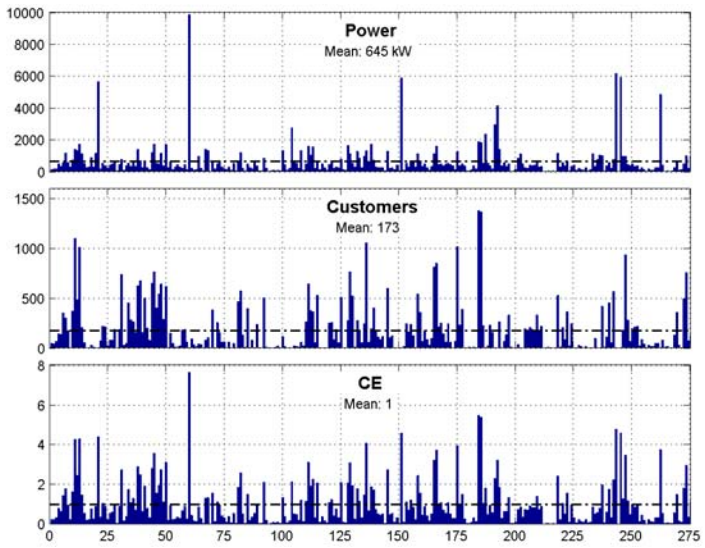


Figure 7.5. Power, customers, and CE is shown for the load nodes of the electrical distribution system. The black dotted line corresponds to the mean value of respective metric.

Results

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, 3 116 and 16 408 sets have synergistic consequences, respectively. In Figure 7.6, 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 consequence 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, i.e. giving a notion of the systems vulnerability to failures.

Even though 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 this analysis failure sets of size 2 with consequences larger than 0.0488 and synergy fraction larger than 79% are studied. For failure sets of size 3 it is chosen to study sets with consequences larger than 0.1020 and synergy fraction larger than 36%. These failure sets are presented in Table 7.3.

Table 7.3. 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} (%)
[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.

All of the selected failure sets in Table 7.3 contains at least one 11 kV 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 HV/MV transformers are listed as highly critical components, since the in-feed capacity is roughly twice as high as the peak power demand and rerouting of power is possible. In Figure 7.7 and Figure 7.8 the most critical failure set for each set size is displayed.

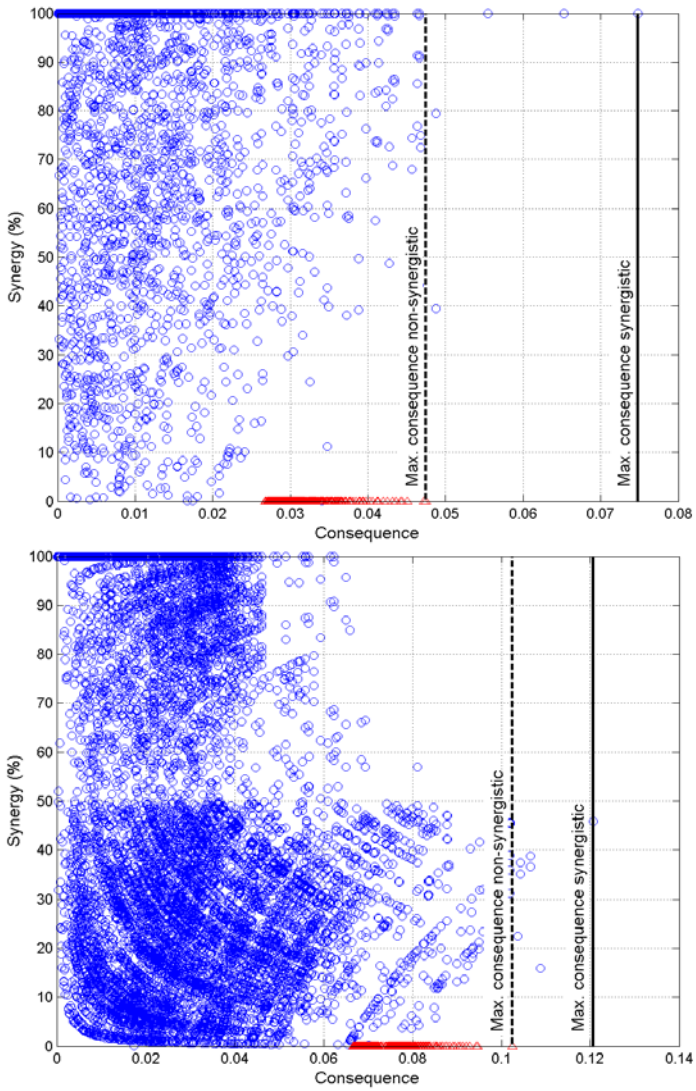


Figure 7.6. Consequence-synergistic scatter plot of synergistic failure sets of size 2 (upper) and size 3 (lower). The consequences of the failure sets, C(F) are presented on the horizontal axis and the fraction of synergistic consequences, f_{syn}, is presented on the vertical axis. Synergistic failure sets are represented with circles and the 1000 highest non-synergistic failure sets are represented with triangles.

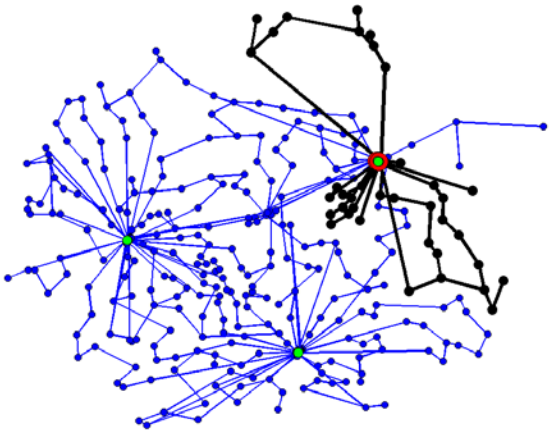


Figure 7.7. Display of the most critical failure set of size two. The blue areas are in service and black areas are out of service. Green indicates in-feed nodes and red indicates the components in the failure set. Totally 53 substations are without power and 15 MW is undelivered, affecting 3078 customers. The failure set consists of two 11 kV bus bars in the same receiving station.

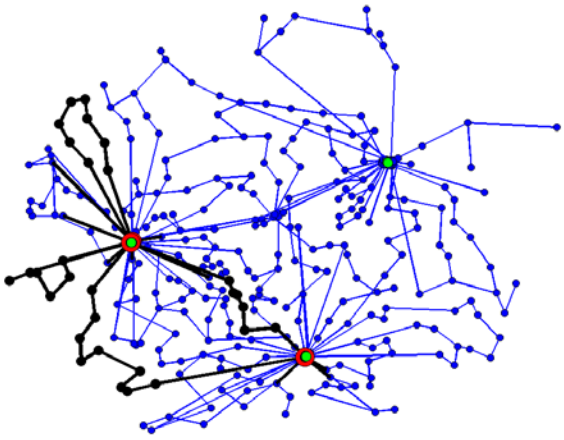


Figure 7.8. Displaying the most critical failure set of size three. The blue areas are in service and black areas are out of service. Green indicates in-feed nodes and red indicates the components in the failure set. Totally 32 substations are without power and 17.5 MW is undelivered, affecting 6775 customers. The failure set consists of three 11 kV bus bars in two different receiving stations.

If the bus bars and the transformers at the HV/MV substations are regarded highly reliable and screened out, other interesting failure sets can be identified. For example, failure set [53 198] with two substations. The failure of which leads to the consequence 0.048 because they, when malfunctioning, render substations with many customers without power supply. Another example is failure set [478 779], which contain two cables that render 9 substations without power when malfunctioning, with 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.

In Table 7.4, the five most critical components are presented for the three different set sizes. As in the previous example, the average consequences are used as a criticality metric. In the table, it is easily seen that the components that are critical in single failures are also critical when considering multiple failures. The reason is that it is 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 7.4 consists of nodes with a high CE.

In Table 7.5, the five components that contribute the most to the synergistic consequences are presented. This list can be utilized to determine which components that are interesting to study further, since they are involved in many failure sets that give rise to large synergistic consequences. Component 337 seems to be a component that is very critical, since it is ranked first for both second order and third order failure sets.

Table 7.4. Criticality of components in single and multiple failures.

Rank	1 failure		2 failures		3 failures	
	Comp.	C	Comp.	C	Comp.	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 7.5. 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

Conclusions

The case study has shown the application of the method to an electrical distribution system. It has proven to be efficient in identifying critical failure sets and critical components. Furthermore, the identification of the worst possible consequences a failure set can give rise to is in itself valuable information, and gives a notion of the systems vulnerability. For the results from the study to be of even more value, they should be discussed in detail with the company owning the network. This discussion would lead to the identification of vulnerabilities where mitigating efforts is of interest.

The method is very suitable for a systematic testing if a power delivery network complies with the N-1 design criteria. It can also be used for the systematic testing of N-k faults in order to assess the vulnerability to these kinds of contingencies. The need for systematic testing for N-k faults in power systems is pointed out in (Mili et al., 2004).

Chapter 8

Discussion

The thesis has presented an approach and some concrete methods for vulnerability analysis of technical infrastructures. With appropriate discussions of threats and hazards that could exploit the identified vulnerabilities, a risk analysis is obtained.

Three different electrical distribution systems were analysed using the developed methods. In order to establish a better notion of the vulnerability of distribution systems, more empirical studies are necessary. These studies should be performed for different types of distribution systems, i.e. rural or urban. The studies would give a better notion of the vulnerability of specific networks and a possibility to develop protocols for benchmarking different distribution systems. Furthermore, it would also be of interest to study the vulnerability of electrical networks at transmission and sub-transmission level. The proposed SVC and DC measures would prove useful for the comparison. In addition, the methods can be applied to other technical infrastructures, such as water distribution and telecommunication systems, by using different physical models. The physical models should capture the essentials of the behaviour of the system to component failures.

In order for the global vulnerability analysis to be a valuable tool to mitigate vulnerabilities, it should be complemented with an exposure analyses, aiming to establish how plausible different types of hazards and threats, i.e. perturbations, and their magnitude are in the area of concern. The perturbations used in the thesis are generic and would benefit from a refinement towards more realistic perturbations.

In addition to being useful as tools for vulnerability analysis, the methods in the thesis can also constitute a valuable tool 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. Properties, such as the fraction of

customers affected by power outages in a municipality 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 or families with children) and critical facilities (e.g. hospitals or fire stations) are affected.

The method for identifying and ranking critical components systematically evaluates component failures in order to determine their criticality. The method was used to analyse an electric distribution system. The proposed method can be used with a more detailed physical model (e.g. power flow model). This means that the applied method also will be even more valuable for the analysis of N-k faults of transmission or sub-transmission levels of the power system. The method will also be valuable for the identification of critical components for other technical infrastructures.

The criticality of a component, or a set of components, was defined as the vulnerability of the system to failures in these. It is important to note that only the consequences of failures are included in the notion of criticality. When making decision regarding vulnerability reductions the likelihood of failures need to be taken into account. The criticality measure can be used to establish a priority ranking for which components that 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 to realistically 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 try to derive which components that might be affected, it is argued for the identification of component failures that cause severe consequences for the system as a whole, and then consider whether these components can fail simultaneously, for example by a common cause.

I believe that the risk and vulnerability assessment of technical infrastructures should take a bottom up approach, starting from where the needs arise if a technical infrastructure fails to deliver its intended services. This would typically mean that municipalities should address the vulnerabilities in their area of responsibility. Counties should address the identified vulnerabilities in their area of responsibility. Finally, when reaching the national level a detailed map of the vulnerability of the infrastructure is yielded. This could for example lead to a different approach of how to mitigate the effects of underproduction in the Swedish power system, where the prevailing strategy

in handling this kind of crisis is rotating power cuts in larger regions. Seen from the functions necessary in municipalities, a better strategy would be to utilize local production, if available, to prioritized loads such as hospital and local authority offices. Unprioritized loads would be subject to rotating power cuts. There are efforts going on in this area in some Swedish municipalities.

The aim of the methods presented in the thesis is to find system states that lead to severe consequences, the extremes. Vulnerability analysis is argued to be the tool to find these system states. The manifestation of these system states might happen rarely which means that statistical data is not necessarily accessible, leading to the benefits of a vulnerability analysis in contrast to a traditional risk analysis. The discussion ends with a guide of how vulnerability assessments of technical infrastructure could be carried out in practice.

8.1 Vulnerability Assessment in Practice

In order to exemplify how the methods presented in the thesis can be used in practice for vulnerability analysis of technical infrastructures a systematic guide is presented in here, see Figure 8.1. Step 1-4 constitutes the vulnerability analysis and step 5-7 how the analysis can serve as a basis for discussion and implementation of vulnerability mitigating efforts. Steps 5 can be seen as going from the vulnerability analysis towards a risk analysis, although the threats and hazards do not have to be exactly quantifiable.

Step 1: System definition, delimitations, and consequences of interest

The first step in a vulnerability analysis is to define the system of interest. It is important to have a clear perception of what the aim of the analysis is, what should be included, and defining the delimitations. The efforts in this step will affect the validity of the vulnerability analysis regarding simplifications and assumptions. It is important that the choices and considerations made in this step are documented properly since they are necessary to understand the results of the analysis and the choices made during the process. An important part of this step is to decide the measures of consequence that will be used. The consequence measure can for example reflect societal losses or be seen from the system owner perspective and reflect technical consequences.

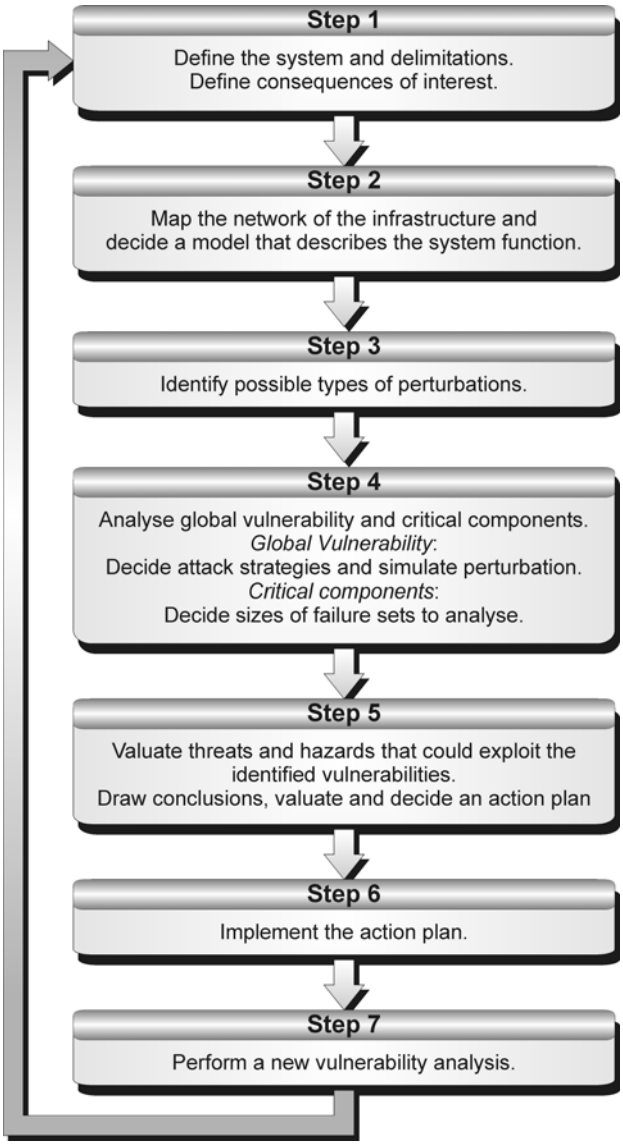


Figure 8.1. The different steps of a vulnerability analysis for technical infrastructures.

Step 2: Mapping and modelling of the system

In step two the focus is on mapping the system of interest and to create a network model of it. In many cases, several components can be aggregated to one node or edge. The basic rule is that they all lead to the same consequences when they malfunction. For an electrical distribution system, a line with an associated breaker or sectionalizer can be modelled as one edge. A model for the physical properties of the system must also be developed in order to correctly assess the consequences. This model should describe how the system functionality is changed when the system is perturbed. If the infrastructure is a road network, the model must describe how the traffic is affected when an edge (road) is put out of function. If it is an electrical distribution system there must be a model that describes the amount of customers that loses power supply when a node (substation or transformer) or an edge (overhead line or cable) is put out of function. The physical model of the system must of course be able to calculate the consequence measure that was defined in step 1. Those that perform the analysis have several important decisions to make regarding the level of detail and the description of the physical model for the calculation of the consequences. The aim is to specify a model with high enough fidelity so that it feasibly describes the consequences with respect to the aim of the analysis and the means available.

Step 3: Identify possible types of perturbations

The third step is about identifying what types of perturbations that the system could be expose to. It is important to declare if the aim of the analysis is to cover the entire scenario space or to evaluate the vulnerability for a specific perturbation. For analysis that tries to cover the whole scenario space, a screening for feasible perturbations has to be carried out in order for the analysis to be possible in practice, i.e. screening out perturbations that are deemed *extremely* unlikely. For the global vulnerability analysis there should be a discussion of the relationship between perturbations and real hazards and threats. For the identification of critical components, it must be decided on how many simultaneous component failures that are of interest.

Step 4: Analyze global vulnerability and identify critical components

This step consists of two parts: global vulnerability analysis and the identification of critical components. In the global analysis, simulation for each type of perturbation has to be carried out. Probabilistic perturbations (e.g. random removal of nodes or edges) must be simulated several times since every simulation will differ in respect to the consequences that arise. There will thus be a distribution of the consequences that can be used to calculate

mean and spread around the mean, see Figure 8.2 for an example. Deterministic perturbations (e.g. removing edges in a predetermined order) only have to be calculated once.

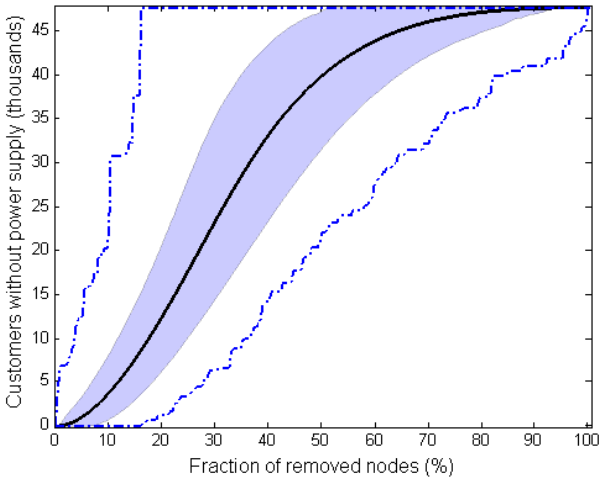


Figure 8.2. The results from a simulation with random removal of nodes for a electrical distribution system As consequence measure the number of customers without power supply is used. The black line shows the mean consequences for 50 000 simulations. The light blue area contain 90% of the calculated consequences. The dotted blue lines illustrate maximum and minimum consequences found in the simulations for the given fraction of removed nodes.

For the identification of critical components, the consequences for all possible combinations of component malfunctions for a given failure set size are calculated. For a network consisting of 800 components this means that 800 consequence calculations have to be performed for one component out of function, about 320 000 for two simultaneous components out of function, and about 85 000 000 for three components out of function. In order to find failure sets of interest a screening methodology is necessary. This methodology could be based on synergistic consequences and/or on consequences and the type of components out of function.

Step 5: Valuate the vulnerability and decide an action plan

In step five the identified vulnerabilities have to be classified as either acceptable or unacceptable. With the global analysis it is possible to determine what type of perturbation the network is vulnerable to. With the analysis of critical components it is possible to determine the worst consequences that could occur for a certain failure set size and to find vulnerable areas of the network. In order to valuate if the identified vulnerabilities are acceptable, a discussion of the likelihood of possible threats and hazards is in place. For the vulnerabilities that are deemed unacceptable, an action plan for vulnerability mitigation has to be drafted. Different alternatives can reduce the vulnerability with higher or lower degree of success. The cost of the alternatives is also an important factor. Both these factors are of course important when drafting the action plan. In this step decisions regarding more detailed analysis can be made, for example by refining the models or by more detailed investment plans.

Step 6: Implement the action plan

In this step, the actions decided upon in the previous step should be implemented. This step is of course extremely important since it is not until the mitigating actions are in place that the vulnerability is actually reduced.

Step 7: Update the vulnerability analysis

It is important to regularly update the vulnerability analysis, especially if the system or the environment it operates in has changed. To perform new analysis is also a way to improve the quality of those that have already been done, for example by doing analysis that is more detailed.

Chapter 9

Conclusions

In this last chapter, conclusions regarding the research presented in the thesis are presented. It starts with a short summary of the methods and results presented in the thesis. It ends with an approach to model interdependent infrastructures, based on the methods and concept put forward in the thesis, and other suggestions of future work.

9.1 Summary of Thesis

In the thesis a definition and general discussions of the concepts of vulnerability and risk, and how they are related, has been given. I argue that, in contrast to risk, the vulnerability is about taking a different point of view. The vulnerability of a system is manifested through its inherent states. Finding these states and the corresponding consequences is the aim of a partial vulnerability analysis. Quantifying threats and hazards that could exploit the vulnerability yields a risk analysis. The vulnerability of a system is also described by its resilience to perturbations, not addressed in the thesis.

In order to assess the vulnerability of a technical infrastructure two methods have been presented: global vulnerability analysis and critical components. Both these methods can be seen as methods to find the states of a system and assess the corresponding consequences, i.e. appraising the vulnerability. The methods require that the technical system can be modeled as a network and that a physical model can estimate the consequences of perturbations.

The empirical studies of electrical distribution systems showed the applicability of the proposed methods. The global vulnerability analysis clearly showed that the electric distribution system is vulnerable to certain perturbations while robust to others. The analysis of critical components showed the methods applicability to systematically identify failure sets that give rise to large consequences, thus assessing the vulnerability.

9.2 Future Work

There are several areas for further research in connection to the work presented in this thesis. The following subsections give short introductions to several interesting directions for future research. It starts with an approach to how infrastructure interdependencies can be modeled, based on the methods and concepts presented in the thesis. The subsequent areas for future research treats improvements of the presented methods and it ends with some areas where the presented concepts in the thesis could be of use. Regardless in which of these research areas future work will be carried out, there still is plenty to be done in this highly interesting and important area of research. The demand for tools and methods in this area will not be easily satisfied.

Analysis of Interdependencies

The research in the thesis has described risk and vulnerability analysis of single technical infrastructures. The underlying ambition for the presented methods has nevertheless been to study interdependent infrastructures. Omitting interdependencies of infrastructures will most likely lead to an underestimation of the vulnerability. In order to take interdependencies into account, a theoretical framework has been drafted. The methods presented in the thesis are the building foundation and takes a large step towards the analysis of interdependent infrastructures. In Figure 9.1, the concept of the modeling approach is presented.

Most technical infrastructures can be modeled as networks. The common denominator for all components in large-scale technical infrastructures is the geographical place they occupy. These two assumptions form the basis for the modeling of infrastructure interdependencies. The dependence of an infrastructure upon another is represented by a directed edge. If a node in one infrastructure has both an incoming and an outgoing directed edge from and to another infrastructure it is thus interdependent. A substation in a power system can be dependent on communication in order to remotely control breakers. The communication system is in turn dependent on power supply for its function, which leads to interdependency. These directed edges in the network model only describes a connection, i.e. not holding any information on the strength of the interdependence (e.g. tight or weak).

The response to perturbations to the network model and the effects of interdependencies are represented in the physical model for each infrastructure. For a cell phone system, the cells are dependent upon the power delivery system. These cells usually have battery backup capabilities for

some hours, important cells even have diesel generators. These types of time characteristics of the dependencies must be integral to the physical model.

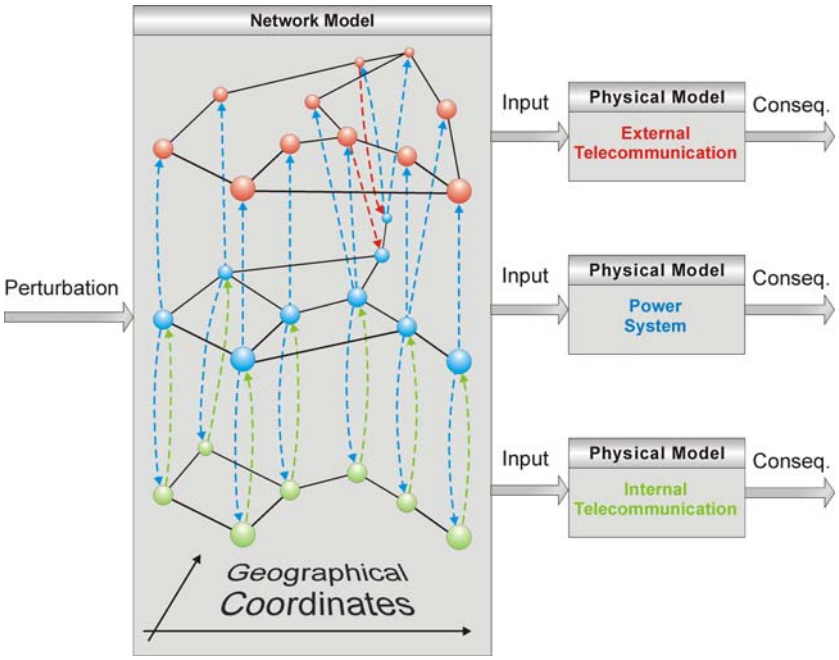


Figure 9.1. Theoretical framework for modeling interdependencies of technical infrastructures. The dashed lines represent dependencies. If a node of the external telecommunication network has a blue line, it symbolises that the node is dependent on power supply for its proper function.

The time resolution of the simulations is intended to be from minutes up to a week in order to capture the effects of time limited buffer zones (e.g. battery backup). The geographical representation of nodes and edges means that common cause failures, such as bad weather affecting several infrastructures simultaneously, can be simulated and analyzed. Perturbations could also be applied to one infrastructure in order to evaluate the consequences in dependent infrastructures. Several research questions arise. Is the suggested approach of modeling a suitable one? Are there structural properties of interdependencies that are unsuitable or even beneficial? Is it possible to find unexpected feed forward loops that enhance the vulnerability of interconnected infrastructures? How vulnerable are interdependent infrastructures?

The constant strive towards efficiency of technical infrastructures have resulted in these dependencies and interdependencies. They have thus historically been regarded as positive. The couplings between infrastructures have a backside since disturbance in one infrastructure can easily spread to other infrastructure. A significant question for future research is the valuing of positive aspects versus the negative aspects, in form of vulnerability, due to interdependencies.

Realistic Attack Strategies

More sophisticated strategies for removing nodes and edges should be developed for the global vulnerability analysis. In the thesis, some generic strategies are used, providing general information of the vulnerability of the electric distribution system. There is often 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 neither are random (which is assumed in random removal) nor deterministic (which is assumed in targeted attacks). If the probability of different attack strategies, i.e. storm, antagonistic threats and so on, can be assessed it would be possible to go from the vulnerability analysis towards a risk analysis. For some perturbations and systems, time aspects will be of importance. This should also be addressed in future research.

Resilience

In order to appreciate the full impact of perturbations to infrastructures, resilience is of importance. The concept of vulnerability includes both the robustness to perturbations and the resilience, i.e. the path back to normal operating conditions. The research presented in the thesis emphasizes on robustness, i.e. the consequences that arise when the infrastructure is perturbed. A significant part of resilience is time. Incorporating resilience to the vulnerability analysis is a challenge for future research. The incorporation would mean that mitigating possibilities, other than strictly structural, could be analyzed.

The research in the thesis could be modified in order to simulate *rebuilding strategies* for perturbed networks. The rebuilding strategies could be based on normal practice or on theoretical optimized strategies. These rebuilding strategies would address one resilience aspect of vulnerability analysis.

Physical Modeling

A comparison between the feasibility of results obtained for the different levels of physical modeling of electric distribution systems (i.e. voltage, capacity, and power flow) should be carried out. Furthermore, the development of physical models for other technical infrastructures than the power system should be addressed.

Search Algorithms for Critical Components

The approach of identifying critical components in networks, as presented in the thesis, could be approved. The algorithm always calculates the consequences for all possible failure sets for the given set size. If the number of components in the network is large and the failure set size of interest is larger than about three, the sheer number of possible failure sets will be insurmountable regarding the time required for the calculations. In Table 9.1 examples of the number of failure sets with respect to the failure set size and the number of components in the network is given. Therefore, ways of reducing the scenario space, without losing important information about the system's vulnerability to failures, have to be developed. A solution could be to use genetic algorithms in order to feasibly limit the search space. The science of search algorithms is a large research area in itself. The advances in this field should be utilized to solve the described problem.

Table 9.1. The number failure sets as a function of failure set size and components.

Failure set size	100 components	500 components	1000 components
1	100	500	1000
2	4 950	124 750	499 500
3	161 700	20 705 500	166 167 000
4	3 921 225	$2.573 \cdot 10^{9}$	$41.14 \cdot 10^{9}$
5	85 287 520	$255.2 \cdot 10^{9}$	$8.250 \cdot 10^{12}$

Power System Islands

The approach presented in the thesis could be used to assess where, in electrical distribution systems with distributed generation, electrical islands could be formed if the network is disturbed. This information could be of great value to other infrastructures and functions that are heavily dependent on electrical power. Such information could be used for planning the placement of telecommunication cells.

Synthetic Networks

The communication system and breakers in a 130 kV / 50 kV sub-transmission substation are fed by low voltage, either coming from a separate secondary winding of the 130/50 kV transformer or from the local distribution system. Telecommunication stations are often feed by the local 10 kV or 0,4 kV distribution system. The signaling system for railways is fed by local 0,4 kV distribution systems. Interdependency analyses of a region would thus need to include all lower voltage distribution systems in the region. To map these distribution systems into networks might be an insurmountable task. A possible approach would be to synthetically generate approximately correct distribution networks, which to all significant aspects have the same behavior as the real distributions system. The networks would be based on population data and in-feed points from the sub-transmission system. In Figure 9.2 a synthetic network can be seen. The research for more feasible algorithms for synthetically generated networks is another area that should be addressed.

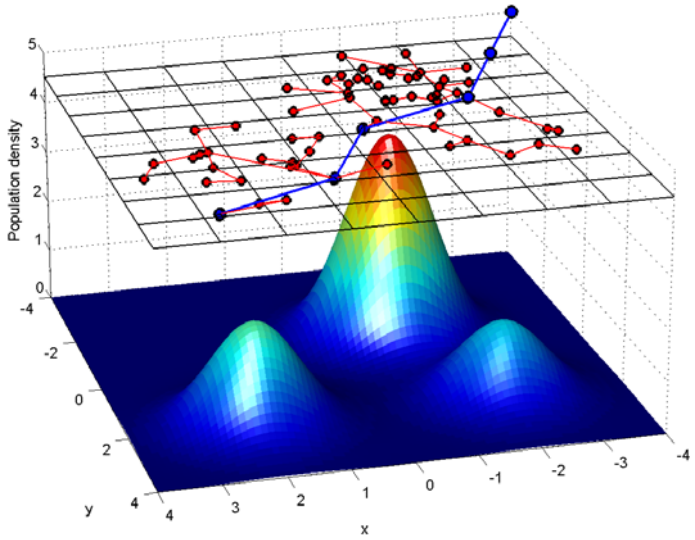


Figure 9.2. A synthetic distribution network (red). The algorithm for generating the network uses only population data (3D-plot) and in-feed points from the sub-transmission system (blue).

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 oppurtunities 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.

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 interdependencies of critical infrastructures using agent discrete event simulations, *Int. J. Emergency ManegemntI*, Vol. 2, No. 4, pp. 306-318.

Bengtsson, A., Nilsson, C., (2007). Extreme value modelling of storm damage in Swedish forests, Submitted to: *Natural Hazards and Earth System Sciences (NHESS).*

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

Brown, R.E., (2002). Electric Power Distribution Reliability, Marcel Dekker Inc, 2002, New York, USA.

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, 2003, Canada.

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.

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* 5(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.

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.

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.

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

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

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

Hollnagel, E., Woods, D.D, Leveson, N., (2006). Resilience engineering concepts and precepts, Ashby Publishing Limited, 2006, Aldershot, England.

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.

Holmgren, Å., (2004). Quantitative Vulnerability Analysis of Electric Power Networks, Doctoral thesis, Department of Transport and Economics, Royal Institute of Technology, Stockholm, Sweden.

Johansson, J., Jönsson, H., Johansson, H., (2007a). Analysing Societal Vulnerability of Electric Power Distribution Systems, *Int. J. Emergency Management*, Vol. 4, No. 1, pp.4–17.

Johansson, H., Jönsson, H., (2007b). Metoder för risk och sårbarhetsanalys ur ett systemperspektiv, To be published in: *LUCRAM rapport 1010,* Lund University, Lund, Sweden.

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, September 25-27.

Jönsson, H., Johansson, J., Johansson, H., (2007). Identifying Critical Components in Electric Power Systems: A Network Analytic Approach, Accepted for presentation at: *European Safety and Reliability Conference 2007* (ESREL2007), Stavanger, Norway, June 25-27.

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.

Kearsley, R., (1987). Restoration in Sweden and experience gained from the blackout of 1983, *IEEE Trans. Power Syst.*, Vol. 2., No. 2, pp. 422-428.

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.

Lakervi, E., Holmes, E.J., (2003). Electricity distribution network design, 2nd edition, Peter Peregrinus Ltd, 2003, London, United Kingdom.

Larsson, S. and 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.

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.

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.

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, pp. 399.

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

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.

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

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

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.

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, in *IEEE/PES Transmission and Distribution Conference & Exhibition: Asia and Pacific Dalian*.

SvK, (2007). Årsredovisningar för åren 2002 till 2005, Available: http://www.svk.se/web/Page.aspx?id=6114, [2007-05-03].

Swedish Energy Agency, (2007). Sammanställning av årsrapporter elnät 2001-2005. Available: http://www.energimarknadsinspektionen.se/For-Energiforetag/El/Inrapportering-for-elnatsforetag/Arsrapporter/Sammanstallning-av-arsrapporter-elnat-2001-2005/, [2007-05-03].

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.

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.

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.