Vulnerability Analysis of Electric Power Delivery Networks

Åke Holmgren

March 2004
TRITA-LWR LIC 2020
ISSN 1650-8629
ISRN KTH/LWR/LIC 2029-SE

Akademisk avhandling för avläggande av teknologi licentiatexamen som med tillstånd av Kungliga Tekniska Högskolan (KTH) i Stockholm framlägges vid ett offentligt seminarium onsdagen den 28 april 2004 kl. 13:30 i sal V1, Kungliga Tekniska Högskolan, Teknikringen 76, Stockholm

©Åke Holmgren 2004
Abstract

Disturbances in the services provided by the infrastructure systems – e.g. electric power supplies and communications – can have serious implications for everyday life, economic prosperity and national security. The disturbances can be initiated by natural disasters, adverse weather, technical failures, human errors, sabotage, terrorism or acts of war. The aim of this thesis is to study methods for proactive vulnerability analysis of electric power delivery networks (i.e. to analyze their sensitivity to threats and hazards), and to formalize vulnerability as a theoretical concept.

The thesis consists of three papers. In the first paper, we discuss concepts and perspectives for developing a methodology for vulnerability studies with the help of the following themes: The properties of the infrastructure systems, threats and hazards, vulnerability and consequence analysis, and measures for creating robust and resilient systems.

In the second paper we discuss how to assess vulnerability of power delivery systems with the help of standard power system performance indices. In two case studies, Swedish power delivery disturbance data is analyzed with statistical methods. We demonstrate that the disturbance size of large disturbances follows a power law distribution, and that the time between disturbances is exponentially distributed.

In third paper, we model electrical power networks as graphs, and conduct empirical studies of two power transmission grids. We calculate values of topological characteristics of the networks and compare their error and attack tolerance, i.e. their performance when vertices are disabled, with two frequently used model networks. Further, we perform a graph influenced vulnerability analysis of a fictitious power network, and evaluate different strategies to decrease the vulnerability of the system.
Preface

This thesis is based on my research performed during 2001–2004 at the safety research group (formerly Center for Safety Research) at the department of Land and Water Resources Engineering, Royal Institute of Technology (KTH), and the division of Defence Analysis at the Swedish Defence Research Agency (FOI).

The thesis consists of two parts; an introductory essay and three papers that form the basis of the thesis:


Acknowledgements

I wish to sincerely thank my supervisor Professor Torbjörn Thedéen for introducing me to the field of risk analysis, initiating this research project and always giving me constructive criticism. I much appreciate our discussions on politics, economics, statistics and life in general.

My special thanks are due to my assistant supervisors, Professor Lars-Göran Mattsson (KTH) and Dr. Stefan Arnborg (SvK), for many valuable comments and stimulating discussions. It has been a great privilege to work with Staffan Molin (FOI and KTH), fellow doctoral candidate, co-author of two papers, friend and “chief” at FOI. Many thanks also go to M.Sc. candidate Erik Jenelius, who contributed with several good ideas in the third paper on graphs, and worked hard implementing algorithms in MATLAB™.

I had an instructive time working with the undergraduate course “Risk in technical systems” together with Per Näsman (KTH) and has also benefited from his statistical assistance. I have enjoyed sharing office and taking coffee breaks with doctoral candidates Torgny Källstam and Tomas Jelinek. Britt Chow has given me all the necessary administrative help, and Lars-Erik Svahn and Jerzy Buczak have provided computer assistance.

I have spent much time in the creative work atmosphere at the department of Defence Analysis (FOI), and enjoyed coffee breaks, interesting discussions, study circles and Friday pubs together with Henrik Christiansson, Svante Barck-Holst, Georg Fischer, Riitta Räty, Daniel Torstensson, Anna Marklund, Fredrik Berefelt and Christian Carling.

Finally, I would like to thank my friends and family, especially my mother and father, for their continuous support in every way during these years.

Financial support from the Swedish Emergency Management Agency (SEMA), formerly the Swedish Agency for Civil Emergency Planning (ÖCB), under contract numbers KBM 0054/2002 and ÖCB 5-909/00, is gratefully acknowledged.
Contents

1 Introduction 1
  1.1 Protecting the critical infrastructure .................. 1
  1.2 A short introduction to power delivery .................. 2
  1.3 Power outages ........................................ 4
  1.4 Objectives and limitations ............................ 7

2 Research approach and important concepts 9
  2.1 Research approach ...................................... 9
  2.2 The infrastructure as complex systems ................. 10
  2.3 Vulnerability and related concepts ..................... 12

3 Proactive vulnerability analysis 17
  3.1 Principal foundations of vulnerability analysis ........ 17
  3.2 Practical vulnerability analysis approaches ............ 19

4 Discussions of the main contributions of the thesis 23
  4.1 On the vulnerability of infrastructure systems – a framework for discussion and analysis ............ 23
  4.2 Using disturbance data to assess vulnerability of power delivery .............. 24
  4.3 Graph modeling and vulnerability analysis of power delivery networks .............................. 25

5 References 29
Chapter 1

Introduction

1.1 Protecting the critical infrastructure

The infrastructure of a society consists of facilities for e.g. power and water supplies, communications, transportation and also the stock of buildings. In a broad definition of infrastructure, basic societal functions like education, national defense and financial and judicial systems can also be included. The notion critical infrastructure can be used to refer to the large technical systems – e.g. electric power grids, water supply systems, transportation and communications – that form the basis for most activities in society. These systems, all artifacts with a highly engineered nature, can be characterized as networks. In this thesis we will direct our interest towards the vulnerability of networks, especially power delivery systems. However, much what is being said is also valid for the other large-scale technical systems. With vulnerability, we shall initially mean a system’s sensitivity to threats and hazards.

The critical infrastructure is utilized to distribute energy, information, water, goods and people and is arguably of the utmost importance for business, government and society in general. Consequently, the services provided by these networks are essential for the quality of everyday life. As an economic engine, these structures are fundamental for a nation’s economic prosperity. A major collapse in these technical systems, resulting in a disturbance in the flow of services they provide, can constitute a severe strain on the society. Hence, the vulnerability of the critical infrastructure has implications on the national security. The technical systems might also enable, or facilitate, the recovery after a major catastrophe in society. For example, it has been shown that communications are critical in the restorations after a
natural disaster such as an earthquake or flooding. Regarding power system restoration, it is likely that a modern control system facilitates the recovery of a damaged power grid.

Disturbances in the services provided by the large-scale technical systems can be initiated by natural disasters, adverse weather, technical failures, human errors, sabotage, terrorism or acts of war. Since the systems of the critical infrastructure are increasingly interdependent, due to the rapid proliferation and integration of telecommunications and computer systems, disturbances can spread between the various technical systems. Even though the military threats still are the focal point of national security policies, the civil dimension – e.g. crisis management capabilities, information operations (IT-related threats) and the transnational terrorism – is increasingly emphasized. The armed forces of Sweden, and many other western countries, are currently undergoing a transformation towards network-oriented principles. In Sweden, the so-called network-based defense will rely on the advances made in the civil infrastructure, e.g. commercial computer systems and the telecommunication systems.

At the policy level, the issue of national security and the vulnerability of the critical infrastructure have been subject to numerous initiatives in the western countries, where USA so far has launched the most extensive initiatives. In 1997 the President’s Commission on Critical Infrastructure Protection (PCCIP) proposed a national strategy for the protection and assurance of the critical infrastructure, and in 2003 the Department of Homeland Security was founded. In Sweden, this subject has a long tradition within the civil defense. Lately, the Swedish Commission on Vulnerability and Security presented a “strategy for increased robustness in the technical infrastructure” in the official report “Vulnerability and Security in a New Era” (SOU, 2001).

1.2 A short introduction to power delivery

Construction of the electric power grids went hand in hand with the development and industrialization that lead to a prosperous western world. In the classical study ”Networks of Power; Electrification in Western Society”, Hughes (1983) emphasizes the importance of the electrification of society:

"Of the great construction projects of the last century, none has been more impressive in its technical, economical, and scientific aspects, none has been more influential in its social effects, and none has engaged more thoroughly our constructive instincts
and capabilities than the electric power system. A great network of power lines which will forever order the way in which we live is now superimposed on the industrial world. Inventors, engineers, managers, and entrepreneurs have ordered the man made world with this energy network. The half-century from 1880 to 1930 constituted the formative years of the history of electric supply systems, and from a study of these years one can perceive the ordering, integrating, coordinating, and systematizing nature of modern human societies."

A power system can schematically be divided into power generation, transmission and distribution, and consumption. The Swedish power delivery system is embraced in the following:

- The **transmission grid** (voltage level 400–220 kV) is a meshed network, connecting the large generating stations (mainly hydropower and nuclear power plants) and the very large consumers. The national transmission grid, a part of the Nordic Interconnected Grid, links together the northern parts of Sweden (where the majority of the generation is located) with the bulk of the power subscribers in the south. The transmission grid enables power trading with other countries and facilitates the optimization of generation within the country.

- The **sub transmission grid**, or regional grid (voltage level 130–40 kV), is a radial or locally meshed network connected to the national transmission grid via infeed points. Smaller generating plants, e.g. gas turbines, and relatively large consumers are connected to this grid.

- The **distribution grid** carries the electric power from the higher voltage levels to the final consumer (voltage level 40–10 kV for the primary distribution grid). The number of levels in the distribution grid depends upon the density and magnitude of demand and the terrain.

Electrical energy cannot be stored to any larger extent, and there always has to be a balance in an electrical system between what is being generated and what is being consumed. The load on the system varies over day and season, and so does the available production. These conditions put special requirements on the operation and control of the electricity generation and delivery process; the different actors in this widespread network have to communicate in real time. The delivery of electricity from power plant to consumer is coordinated and optimized with the support of e.g. SCADA-systems (Supervisory, Control And Data Acquisition) and EMS (Energy
Managements Systems). The various information and communication systems that link the power system together – enabling e.g. monitoring and control of the network, power trading, operational planning and development – utilize computer and telecommunication networks.

Since the electricity market reform in the early 1990s, the electricity markets in the Nordic countries have undergone major changes. The functions of power generation, delivery and marketing, traditionally integrated within the utilities, are now separated. Competition, ageing proprietary systems and reductions in staff and operating margins leading utilities to rapidly expand their use of information systems and to interconnect previously isolated networks.

1.3 Power outages

The technical conditions that may lead to a lesser or greater power system failure will include: Overloads, voltage or frequency outside limits, instability, disconnection of a substation or generating plant and, system splitting. Knight (2001) lists a number of factors contributing to the likelihood of a severe power disturbance:

- Exceptionally severe weather.
- Unexpected and sudden bad weather (causing a rapid increase in demand and increased plant failures).
- Sudden and large loss of generation or excessive non-availability of generating plant.
- Failure of anti-disturbance or protection equipment.
- Sudden changes in ambient conditions (e.g. thaw after a long period of freezing weather leading to insulator flashovers).
- Errors by control staff, planning staff or field staff.

A power disturbance with duration of only a few seconds can have a serious impact for e.g. the process industry, air-traffic control, and intensive care at hospitals. The societal effects of a shortage in power supply can be both direct and indirect. A major power outage affects all functions in society and economical life stops in a region without electricity. People in large cities are more easily affected than those living in rural areas. Indirect effects of a major blackout can range from an increase in crimes in larger
cities to interruptions in communications and low indoor temperatures. Especially critical is the state of dependence between telecommunications and power systems. In less than six hours there will be interruptions in the mobile communication stations with battery backup. After 10–24 hours there will be a shortage of food in the cities, and after some days there will be a shortage of fuel, affecting the reserve supply of electricity through generators. In short we can conclude that the impacts of a major power outage will be determined by the nature of the area affected (e.g. economic activities and types of industry), the duration of the disturbance, the time of day, the time of year and the weather conditions.

Most power disturbances in Sweden are weather related and occur in wintertime. They mainly affect local distribution grids in rural areas. Two widespread blackouts have occurred in Sweden during the last 30 years. The voltage collapse in the winter 1983 resulted in large loss of generation (approximate 65 %) and duration of six hours (70 % of all power delivery was in service within two hours). The outage in September 2003 was caused by two simultaneous faults; a full shutdown in one of the reactors in Oskarshamn Nuclear Power plant and a fault in a 400 kV substation. Southern Sweden and eastern Denmark (including the capital city Copenhagen), were blacked-out. The restoration of the transmission grid (400 kV) was completed in less than one hour, and after seven hours almost all supplies were resumed (SvK, 2003). Approximately five million people were affected by this outage.

In the following, we summarize a few recent major power outages that have received international attention.

**Canada, January 4, 1998:** Between the 4th and 10th of January, eastern Canada was hit by the worst ice storm in modern time. Due to extreme ice formation on power lines and other components, the power grids in Québec and Ontario were severely damaged. At the most, 1.6 million customers were without electricity, and a large part of the 5.5 million inhabitants in the region suffered from power outages. In some areas, the restorations took nearly four weeks, but of the affected consumers 90 % had received power within two weeks. Residual repairs of the power grid continued into early summer. During the ice storm, social and economical activities ceased to function. This put enormous pressure on the crisis management organization, e.g. emergency lodging for 100 000 people had to be arranged. The ice storm also caused disturbances in northwest USA (Fischer & Molin, 2000).
New Zealand (Auckland), February 20, 1998: A series of power disturbances caused severe stress on the city of Auckland. After four power cable failures, the power retailer and distributor announced that they no longer could supply power to the central business district. The power crisis that followed lasted for more than five weeks and the power was unstable several months later. The number of people affected of this outage was small, but the severe economical effects of the disturbance clearly showed the significance of the business district for the country’s economy (Molin & Fischer, 2001).

USA (New York City), July 6, 1999: A distribution network in northern Manhattan lost eight of its 14 feeder cables due to heat related failures in connections, cables and transformers. The network had to be de-energized to protect it from massive damage, which interrupted power to 68 000 customers (200 000 people) in 19 hours (POST, 2000).

France, December 26, 1999: Severe storms crossed France for some seven hours, causing heavily damage on the national transmission grid. The maximum number of transmission lines out of operation was 38 and 5 000 MW of demand was unsupplied. A second storm hit France on the 28th of December, resulting in large power outages (Knight, 2001). Power was interrupted to nearly 3.5 million households.

USA and Canada, August 14, 2003: The outage was caused by a combination of electrical, computer and human failures. Uncorrected problems in northern Ohio developed into a cascading blackout; this included an ineffective system monitoring tool, loss of generation, no efforts to reduce load, lines tripping because of contact with overgrown trees and finally, overloads. The blackout affected 50 million people (61 800 MW of electric load) in the Midwest and Northeast United States and Ontario in Canada. Power was not restored for two days in some parts of the United States, and parts of Ontario suffered from rolling blackouts for more than one week (U.S.-Canada Task Force, 2003).

Great Britain (London), August 28, 2003: A transformer in distress needed to be disconnected from the grid. During this operation, automatic protection equipment operated incorrectly. The switching was interpreted as fault by the automatic system and several substations were disconnected. Approximately 20 % of London’s total supplies
were lost and 476,000 consumers affected. Power supplies from the National Grid were restored after 40 minutes (Ofgem, 2003).

**Italy, September 28, 2003:** A trip in a Swiss transmission line, caused by a tree flashover, was the starting point in a sequence of events leading to the major blackout in Italy. The trip in the first line caused overloads on other lines, and after some 20 minutes a second important line was lost (the reason was probably a flashover caused by the sag in the line due to overheating of the conductors). The overloads that followed lead to the isolation of the Italian system from the European network (UCTE). Instability phenomena resulted in a very low system voltage in northern Italy, and accordingly the trip of several generation plants. Automatic countermeasures (e.g. load shedding) were implemented to manage the loss of imported power. However, the large loss of generation plants made it impossible for the Italian system to operate separated from the UCTE-network (UCTE, 2003). Power was interrupted to possibly as many as 55 million people. The power supplies was resumed in the capital Roma after nine hours, and in some parts of southern Italy restoration took up to 18 hours.

### 1.4 Objectives and limitations

This thesis is a result of a joint research project on critical infrastructure protection, involving researchers from the Royal Institute of Technology (KTH) and the Swedish Defence Research Agency (FOI). A fundamental idea in the project is that in order to manage the vulnerability of power delivery systems, an understanding of the whole *disruption process* is required: From the preventive work – i.e. proactive analyses and measures undertaken to avoid disturbances – to the management of the (acute) crisis – i.e. mitigation, recovery and restart.

Here, we are mainly concerned with the proactive phase, especially the vulnerability analysis, i.e. the analysis of the systems sensitivity to threats and hazards. Technical and organizational crisis management of power systems in emergencies will be treated in a future thesis. Thus, the aim of this thesis is to study methods for *vulnerability analysis of electric power delivery systems* (networks). An important objective is to formalize vulnerability as a theoretical concept, to use in studies of network’s sensitivity to threats and hazards. This will include investigating how the concept can be operationalized, i.e. practically useful when studying the vulnerability of power delivery systems, and to conduct case studies of power outage data.
We set the focus on large catastrophes that can cause severe strain on the whole society, i.e. we apply a *national security perspective*. For power delivery systems this means disturbances with long duration, large power loss, and a great number of people affected.

Our aim is to generate information and knowledge that will improve the basis for decision- and policymaker’s judgments, i.e. we adopt a *decision-making perspective*. This foremost concerns methodology on how to assess the vulnerability of systems, e.g. when choosing between various system solutions. To some extent, the emergency decision-making perspective, e.g. what strategies and operations that should be performed to recover a damaged system, can also be included in such assessment. The decision-making perspective has implications on how we look-upon the power delivery systems. In spite of their highly engineered nature, we principally treat these systems as somewhat abstract networks. Taken together with the national security perspective, the result is that we do not explicitly treat power-engineering methods for analysis, simulation and control of power systems under normal operating conditions. Finally, we defuse those critical infrastructure issues that relate to everyday life, e.g. financial and market risks.
Chapter 2

Research approach and important concepts

2.1 Research approach

To study the vulnerability of the infrastructure from a national security perspective, we believe, knowledge from many areas has to be integrated through what is commonly known as systems analysis. In systems analysis, analytical tools, e.g. mathematical and statistical models, play an important role. To be able to properly use these means, a good overview of theories and methods, their applicability and limitations, is needed. Further, mobilizing and combining knowledge from different areas is a craftsmanship, requiring creativity and an understanding of the problems at hand, and the situations where the results are to be used. Miser & Quade (1985) state the following:

“Systems analysis is not a method or a technique, nor is it a fixed set of techniques; rather it is an approach, a way of looking at a problem and bringing scientific knowledge and thought to bear on it. That is, it is a way to investigate how to best aid a decision or policymaker faced with complex problems of choice under uncertainty, a practical philosophy for carrying out decision-oriented multidisciplinary research, and a perspective on the use of available tools.”

The problems that systems analysis deals with often involves one or more of the following difficulties: Inadequate knowledge and data, many disciplines involved, inadequate existing approaches, unclear goals and shifting
objectives, pluralistic responsibilities, resistance to change in social systems and complexity (Miser & Quade, 1985).

2.2 The infrastructure as complex systems

Henceforth in this thesis we will use the notion *infrastructure systems* to refer to the large technical systems, e.g. power delivery systems, which form the basis for most activities in society. A general definition of the concept of a system can be found in IEC (1995):

**Definition 1** “A *system* is a composite entity, at any level of complexity, of personnel, procedures, material, tools, equipment, facilities and software. The elements of this composite entity are used together in the intended operational or support environment to perform a given task or achieve a specific objective.”

The term system is used in many situations, and several appropriate definitions can be found in the literature. However, common themes are: elements (or components), an interaction between the elements, a systems environment (and hence boundaries of the system), and the notion that the parts of the system perform to accomplish a given task.

A well-established approach when studying large technical systems is to use the perspectives proposed by Linstone (1984): a technical perspective, an organizational perspective and a personal perspective. Kaijser (1994) proposes another set of perspectives appropriate for studies of the infrastructure: a technical perspective, a geographical perspective, an economical perspective and an institutional perspective. Beside the technical components and structures we need to take into account the organizations and persons that develop, run, and use the systems together with the economical, institutional, cultural and legal conditions that form a frame for supplying the service in question. The technical and the social dimensions of technology are intertwined, i.e. “the technical is inherently social” (Summerton, 1994). Hence, the concept *sociotechnical system* is often used.

Rinaldi et al. (2001) claim that all “infrastructures” have one property in common, i.e. “they are complex adaptive systems”. There has been a remarkable growth in academic research focused on complexity in recent years, with contributions from mathematics, physics, biology, and many other areas. Regarding the origin of complexity, it is a well-known principle that simple rules commonly produce random and complex looking behavior. With the help of simple programs (cellular automata) it is possible to
show that complexity can arise from local interactions and simple decision rules. This does not, however, prove that simple rules are the source of such behavior in nature or in technical systems.

When we say that a system is complex, it is a way of describing the nature of the system (classifying the system), but it can also be a metaphor or analogy. The term complex can be used to make an arbitrary distinction between something perceived as simple, and something perceived as complicated – the simple/complex dichotomy.

Complexity, used as a metaphor, usually implies a critique against the traditional reductionist approaches and the predominant systems theory (Karlqvist, 1999). Thus, it is a conception that synergies emerge when we are bringing together large sets of entities. Labeling a system complex can be a way of swiftly capturing a number of properties, such as non-linearity, adaptability, self-organization, emergence etc. Ottino (2004) means that complex systems can be identified by “what they do (display organization without a central organizing authority – emergence), and also by how they may or may not be analyzed (as decomposing the system and analyzing sub-parts do not necessary give a clue as to the behavior of the whole)”. Ottino agree on that the infrastructure systems fall within the scope of complex systems, and points out that “although engineers developed the components, they did not plan their connection”, further many engineering systems “are already formed, one has to interpret and explain”, there is “no such luxury as starting de novo”. Thus, an important question is how to stay connected with, and guide, the development of systems that self-organize and adapt.

Gell-Mann (1997) argues that a variety of different measures would be required to capture all our intuitive ideas about what is meant by complexity, and that complexity, however defined, is not entirely an intrinsic property of the entity described; it also depends to some extent on who or what is doing the describing. Here we shall not undertake a formal definition of complex systems, instead we agree with Simon (1962):

“Roughly, by a complex system I mean one made up of a large number of parts that interact in a nonsimple way. In such system, the whole is more than the sum of the parts, not in an ultimate, metaphysical sense, but in the important pragmatic sense that, given the properties of the parts and the laws of their interaction, it is not a trivial matter to infer the properties of the whole. In the face of complexity an in-principle reductionist may be at the same time a pragmatic holist.”

11
2.3 Vulnerability and related concepts

In this thesis we use concepts from a number of different scientific cultures – e.g. systems safety and reliability analysis, risk management and economics, computer security, policy analysis, and the power engineering discipline. For several of the concepts there exist many appropriate definitions.

In dictionary definitions of “vulnerable”, a common denominator is references to deliberate actions (threats), e.g. “susceptible to attack”, (WordNet, 2004), “exposed to danger or attack; unprotected” (OAD, 1989), or “open to attack or assault by armed forces” (Webster, 1975). There are also somewhat more general phrases such as “capable of being wounded or hurt” (WordNet, 2004).

For technical applications there are no generally accepted definitions of the concept vulnerability. In the information security profession vulnerability has been defined as “a condition of a missing or ineffectively administered safeguard or control that allows a threat to occur with a greater impact or frequency, or both” (Peltier et al., 2003). Berdica (2002) defines vulnerability in the road transportation system as “a susceptibility to incidents that can result in considerable reductions in road network serviceability”. In the military area, the concept has been used to describe how vulnerable for example a ship’s hull or an aircraft is with respect to physical impacts. In recent years the concept has also been used in connection with human and societal systems, biological systems or ecosystems, engineering structures and complex industrial systems (Einarsson & Rausand, 1998).

Einarsson & Rausand (1998) define the vulnerability of an industrial system as “the properties of an industrial system; its premises, facilities, and production equipment, including its human resources, human organization and all its software, hardware, and net-ware, that may weaken or limit its ability to endure threats and survive accidental events that originate both within and outside the system boundaries”. We have used this definition as a starting-point, and successively modified it during the course of the project. In the first paper of the thesis, Holmgren (2003), vulnerability is defined as follows:

Definition 2 Vulnerability is the collection of properties of an infrastructure system that may weaken or limit its ability to maintain its intended function, or provide its intended services, when exposed to threats and hazards that originate both within and outside of the system’s boundaries.
Thus, vulnerability in a system is a susceptibility (sensitivity) to threats and hazards that substantially reduce its ability to maintain its intended function. We use the vulnerability concept to characterize a system’s lack of robustness and resilience with respect to various threats and hazards. In this situation, robustness signifies that the system will retain its system structure (function) intact (remains unchanged or nearly unchanged) when exposed to perturbations, and resilience implicates that the system can adapt to regain a new stable position (recover or return to, or close to, its original state) after perturbations. Robustness and resilience taken together are a complement to vulnerability in the same way as safety is to risk.

Other attempts have been made to integrate several similar qualities into one abstract concept. Dependability has been proposed as a generic term combining concepts such as availability, reliability, safety and security. Dependability could in this case be defined as “task accomplishment” and “provision of expected service” (IEC, 1992; Jonsson, 1998). It is likely that a system that is both robust and resilient can provide the services we expect and therefore accomplish its tasks.

In the first paper of the thesis we choose, for practical reasons, to include the qualities of resilience in robustness. The concept robustness has been used as an opposite to vulnerability in several official Swedish documents, e.g. SOU (2001).

However, Hansson & Helgesson (2003) use the recovery time, i.e. the time it takes for the system to recover after a perturbation, and show in a formal analysis that robustness can in fact be treated as a special case of resilience (namely when the recovery time equals zero). It should be noted that concepts such as vulnerable and robust have become value-laden words with political dimensions. For example, the expression “the vulnerability of the modern society” can implicate a distrust of technological progress and an idea that society was more capable before the large-scale technical systems came into place.

The monadic concept “vulnerability”, divides systems into two categories: vulnerable and not vulnerable. The comparative notion “at least as vulnerable as” compares systems according to their degrees of vulnerability. According to Hansson & Helgesson (2003), a monadic concept is more fundamental than the comparative one. However, the monadic concept can, in theory, be obtained from the comparative one through the addition of precise limit somewhere on the scale of degrees of vulnerability.

A monadic notion of vulnerability is not useful in real life – all systems are sensitive to some threats and hence vulnerable in some respect. However, using the comparative notion is not always straightforward. A system may
be vulnerable with respect to some threats (perturbations) but not to others. If two systems are vulnerable in relation to different kinds of threats, there may be no evident answer to the question which of them is more vulnerable. They may very well be incomparable in terms of vulnerability.

In the literature it is possible to find precise mathematical meanings of concepts such as risk and reliability. A precise measure of vulnerability can be helpful for decision- and policymakers. In theory, it is possible to obtain an absolute measure of risk or, as in this case, vulnerability. Nevertheless, for technical systems it is often preferable to make relative comparisons between different system solutions.

The definition of vulnerability presented above (Definition 2) is not sufficiently explicit for neither empirical, nor theoretical studies. In the second paper, Holmgren & Molin (2003), we have approached this problem by using several operational variables (indicators) to measure the vulnerability of a system. Thus, we propose the following measure of the vulnerability of an infrastructure system:

**Definition 3** The vulnerability of an infrastructure system is the probability that the negative societal consequences of a disturbance $X$ is larger than some value $x$, i.e. $P(X > x)$ during a given period of time and for large $x$.

Hence, the vulnerability of an infrastructure system is the probability of a system collapse that causes large negative societal consequences. We do not attempt to exactly specify what constitute large negative consequences (large $x$). However, the term “severe strain on society” (frequently used in Swedish official policy documents) can be used to vaguely characterize what represents a major disturbance. Further, selecting one operational variable that captures the consequences of a power outage is not straightforward. The consequences of a disturbance can be described by e.g. the cost of the disturbance, the number of affected power subscribers, the number of injured or dead people, the size of the affected area, the power loss, the unserved energy, or the duration. It should also be noted that we disregard the time aspect in Definition 3, i.e. how often the catastrophes occur.

From probability theory, we know that $P(X > x) = 1 - F(x) = R(x)$, where $F(x)$ is denoted the probability distribution function and $R(x)$ is the survivability function. For a continuous random variable, $F(x)$ is obtained by integrating the probability density function $f(x)$, i.e. $F(x) = P(X \leq x) = \int_{-\infty}^{x} f(t)dt$, and for a discrete random variable $F(x) = \sum_{t \leq x} f(t)$. In some situations it is possible to talk about the probability that a hazard or threat is realized, however, in other cases, e.g. a terrorist attack, a conditional approach can be used, i.e. $P(X > x \mid$ a specific negative event is realized).
There are obvious similarities to the risk concept in the definition above. However, the risk concept is both a bit more restricted and a bit broader. As with the risk concept, we have two components: the probability or likelihood of a negative event and the resulting negative consequences. Risk is often reserved for random/uncertain events with negative consequences for human life and health and the environment. Regarding the vulnerability of the infrastructure systems, planned attacks play an important role. Further, it is principally a focus on the system’s survivability. Finally, we do not use the concept of vulnerability in relation to minor disturbances.
Chapter 3

Proactive vulnerability analysis

3.1 Principal foundations of vulnerability analysis

The following three questions capture the essential elements of the risk analysis (IEC, 1995):

i) What can go wrong (by hazard or threat identification)?

ii) How likely is it to happen (by frequency analysis)?

iii) What are the consequences (by consequence analysis)?

The traditional risk analysis of technical systems focuses mainly on technical failures and failures resulting from extreme natural conditions, e.g. extreme weather. Further, the analysis of the consequences of the accidental events mainly concerns the negative consequences for human life and health and the environment. As we have stated above, the focal point of the vulnerability analysis is the survivability of the system. Infrastructure systems can break down due to many reasons – from extreme natural events such as snowstorms, failure in technical components up to terrorist attacks and war. Consequently, we include both threats from planned attacks (antagonistic attacks) and unintentional threats and hazards in the vulnerability analysis.

Societal crisis management consists of a number of phases, for example: prevent, mitigate, response, recover, and learn (Rosenthal et al., 1989). Managing the vulnerability of infrastructure systems demands an understanding of the whole disruption process – from the time when the accident
or disruption takes place until mitigation and restoration actions have been completed. In some cases it can be more suitable to concentrate on resources to abort an ongoing disruption, rather than using the resources to prevent that the disruption takes place. Hence, the major difference between the risk and the vulnerability analysis is that the latter focuses on the whole disruption period until a new stable situation is obtained. Consequently, we add a fourth question, which involves analysis of resources and strategies for mitigation, recovery and restart:

iv) How can the system function be recovered after a disruption?

A typical situation when analyzing risk in technical systems is that we have few data of accidents or disturbances with severe consequences. Hence, it is seldom possible to use ordinary statistical methods to estimate the risk. Sometimes, useful information can be obtained from incidents (or precursors). However, in many situations, especially when we are dealing with new technologies or new systems, no severe accidents have yet occurred. We therefore have to use theoretical (logical) models and/or experts’ opinions. Thus, we can discern three principal ways to estimate the probability, or likelihood, that a certain event (disturbance) will occur (Holmgren & Thedéen, 2003):

- **Ordinary statistical analysis** of empirical accident or incident data, e.g. analysis of traffic or workplace accidents.

- **Theoretical (mathematical) modeling** of the technical systems *in combination with empirical data* for components, e.g. probabilistic safety analysis (PSA) in the nuclear and process industries.

- **Expert judgments**, e.g. within the qualitative engineering risk analysis methods. Expert judgments can be collected through more or less formalized methods, e.g. through interviews or surveys. Empirical data can also be combined with expert judgments with Bayesian statistical tools.

Regarding the negative consequences of a disruption or accident, a similar division can be made. Within the engineering disciplines, analytical and numerical models play an important role in *consequence analysis*, e.g. for evaluating the consequences of fire or explosions. There are also lessons to be learned from *case studies* of major disturbances.
Two principal ways of obtaining knowledge can be identified in theory of science – *empiricism* and *rationalism*. That is, knowledge through empirical observations or through rational reasoning. Modern science usually combines these two traditions. We can compare with the three principal ways of estimating the probability in the vulnerability analysis given above. In the first approach, statistical analysis of accident data, we use available empirical observations and draw conclusions from these. An ideal situation would of course be to perform controlled experiments. However, this is seldom possible at a higher system level, and very unethical if people, as a result, could be hurt. In the second approach, we use a combination of theoretical modeling and empirical observations. Here, it can be possible to perform controlled experiment, e.g. so-called life tests of technical components to obtain information about their failure rate. If humans are part of the system, e.g. operators in control room, data can sometimes be obtained through experiments or games. Concerning the third approach, expert’s opinions are based on rational reasoning (enhanced by, or derived from, practical knowledge), but also influenced by the experts own values and beliefs.

### 3.2 Practical vulnerability analysis approaches

In the previous section we have outlined some principal foundations of vulnerability analysis. In practice, there are a variety of methods; adapted to different levels of detail and for different objectives of the analysis. The aim of the analysis can be to identify critical (or weak) entities in the system and to advance the understanding of the system, e.g. evaluate an existing system (check its status or follow up changes). A vulnerability analysis can facilitate the development of responses to possible crisis situations, and found the basis for prioritization between different alternatives to improve system performance. Conducting an analysis helps create an awareness of risk and vulnerability management in the organization and thus increases the motivation to work with these issues. Hopefully, the analysis will help to develop the internal expertise and skills in the organizations, which further can promote action.

Here, we give a short account of five different methods; ranging from a policy oriented vulnerability assessment method of the “electric power infrastructure” to a quite technical model for analyzing the vulnerabilities introduced in overall power systems by communication systems.
DOE’s vulnerability assessment methodology: This policy-oriented methodology is developed and validated by the Office of Energy Assurance (OEA) at the U.S. Department of Energy (DOE). The methodology is divided in three phases: pre-assessment, assessment, and post assessment, where each phase consists of a series of tasks. The pre-assessment phase involves the following elements: Define the scope of the assessment, establish appropriate information protection procedures, and identify and rank critical assets. The assessment methodology involves 10 different study areas: Network architecture, threat environment, penetration testing, physical security, physical asset analysis, operations security, policies and procedures, impact analysis, infrastructure interdependencies, and risk characterization. Mainly qualitative analysis techniques, e.g. interviews, checklist, tours and physical inspections, are used in the vulnerability survey. Finally, the post-assessment phase includes prioritizing assessment recommendations, developing an action plan, capturing lessons learned and best practices, and conducting training (DOE, 2002).

A semi-quantitative vulnerability analysis methodology: In Einarsson & Rausand (1998) a two-step semi quantitative approach to vulnerability analysis of production systems (complex industrial systems) is presented. The objective of the first part of the analysis is to find and describe “scenarios of relevance” (threat scenarios that have negative consequences above a certain level), and to study how the system is prepared to handle these scenarios. The final task of this part is a ranking of the scenarios according to their criticality. The result of the first phase of the analysis is list of critical scenarios. The second part is an analysis of likelihood and consequences. First, the potential cause chain, from the root causes to the accidental events, is analyzed to establish how actions can be made to reduce the likelihood of the initiating event (accident). Second, the consequences of the accidental events are analyzed in order to understand how they can be reduced by e.g. addressing design, operational or contingency aspects. The analysis is supported by three work sheets, and has been used in several studies of production systems: consumer gods industries, electro mechanical industries and car parts manufacturing.
A probabilistic infrastructure risk analysis framework: A very brief framework of a probabilistic infrastructure risk analysis model, initially developed for a small community’s water supply and treatment system, is described in Ezell et al. (2000). In the first phase of the work, decomposing the system and subjectively rank order threats and vulnerabilities identifies the risks to the infrastructure. The next phase – “Modeling Risks to the Infrastructure” – begins by developing scenarios to model. Here, well-known tools from the risk analysis discipline (event and fault trees, i.e. logical tree diagrams) are used. The goal of phase two is to construct a probabilistic model to assess risks associated with a given scenario. Phase three is the assessment phase, where the following quantities are to be calculated: the system performance under unusual load, the extreme loss and the expected loss. The final phase – “Manage the Risk to the Infrastructure” – includes generating alternatives with the goal of improving system performance, and a tradeoff analysis of the alternatives.

Structural vulnerability analysis of networks: Albert et al. (2004) study the North American power grid from a “network perspective”, and the grid is represented as a graph (sets of vertices and edges). The actual flow of electrical energy is not considered; only the grid’s topology is modeled. This paper has several similarities with our study of the vulnerability of power delivery networks presented in the third paper, see Holmgren (2004); consequently we will not describe the results in detail here. In short, Albert et al. calculate some topological characteristics of this vast power network and investigate the connectivity loss in the grid due to the removal of vertices corresponding to transmission substations.

A Communication Agent model: Liu et al. (2001) proposes a Communication Agent model to study the vulnerability induced in the power system by interactions with the communication system. The model uses a framework called SPID (Strategic Power Infrastructure Defense system). For this system, an agent model, MAS (Multi-Agent System), is developed to describe interactions between major functional blocks in a power system. There are different levels of agents in an MAS system, and each agent on the different layers is independent of other agents and tries to achieve its individual goal. The agents can communicate with each other (with a standardized computer language), and there is also resource sharing so the agents can cooperate to achieve a

21
global objective. The Communication Agent handles the communication subsystem issues, and provides a handful of functions. The agent can for example “keep track of the states of communication (aliveness, congestion, redundancy) links”, “detect communication link failure”, and “perform Communication System Vulnerability Index (CSVI) calculations”. A loss of a communication link means that control signals or measures cannot be sent through that link. Liu et al., uses two different definitions of CSVI, and the objective of this index is to help the agents to “learn the network status and to adjust their plans according to this Vulnerability Index”. The model is quite technical, and only a very limited example is given in the paper. Liu et al. implements an agent that monitors the throughput of a network (given as a value of a CSVI). The system administrator can, for example, be notified when the value of the CSVI reaches a predefined threshold.
Chapter 4

Discussions of the main contributions of the thesis

4.1 On the vulnerability of infrastructure systems – a framework for discussion and analysis

In the first paper, four (not mutually exclusive) themes are used to structure the discussion on infrastructure vulnerability and to review literature: The nature of the infrastructure systems, threats and hazards, vulnerability and consequence analysis, and measures for infrastructure system protection.

Societal crisis management of large-scale power outages has been shown to demand coordinated actions between public and private organizations across the national boarders, and the issue is therefore a matter of both national and international security.

A classification of threats and hazards can be based on i) the possible consequences of the threat, ii) which methods or resources that are needed to manage, or prevent, the potential outcomes from the threats, or iii) the cause of the threats, i.e. what, or who, is causing the threat. In this paper, we present a cause related classification of threats and hazards. Even though the antagonistic threats, e.g. IT-related threats and transnational terrorism, are alarming and have attracted a lot of attention, recent blackouts show that adverse weather and technical failures still needs consideration.

We recommend a vulnerability analysis methodology based on multiple perspectives since both technical and non-technical factors are of great importance. Risk analysis methods from the systems safety and reliability disciplines can be used to some extent.
However, the recent advances in modeling and simulation of complex networks and game theoretical approaches should also be taken into account. Proactive actions are required in order to assure the continuous supply of services from the infrastructure systems. We believe that the general principle should be to prevent the systems from degenerating into alert and emergency states, but if this does occur, it is important to minimize the disturbances and restore normal conditions as quickly as possible. Thus, strategies and resources for crisis management are imperative to reduce the vulnerability of the infrastructure systems. Successively taking decisions (using adaptive strategies) and developing the ability to act on unexpected situations as they emerge, e.g. through the use of games and scenario analysis, helps managing the uncertainties present in all long-range planning.

4.2 Using disturbance data to assess vulnerability of power delivery

In the second paper, we show how standard power performance indicators – i.e. unserved energy, restoration time and the number of disturbances with energy unserved – can be used to assess if the vulnerability of a power delivery system has changed. That is, we use available empirical observations to draw conclusions on the abilities of the systems. An underlying assumption in this thesis is that the aspect of reality we try to capture, i.e. the vulnerability of a system, is possible to operationalize and measure. Compressing all information about a power outage in a few quantitative indicators is indeed a great simplification of reality. However, by using a few, standard indicators we obtain a high transparency, decrease the need for value judgments, and make it possible to use statistical methods to study the indicators more objectively over time.

In two case studies, statistical analyses of disturbance data from Swedish power transmission and distribution are presented and discussed. Under normal operating conditions lightning strikes are the main cause of disturbances in the Swedish national transmission grid. Further, there are only a few disturbances per year that lead to unserved energy. Also, the unserved energy in relation to the total amount of transmitted energy is extremely small. In the distribution grid of Stockholm, cable failures are the dominant cause of disturbance. For the two studied time series of disturbance data, the value of unserved energy and the number of disturbances appear to be of the same order of magnitude during the studied period.
Analysis of output data can give a good understanding of everyday disturbances and the power systems ability to endure them. The available data set does not give us enough information to make more profound statements about disturbances with long duration, large power loss, and a great number of people affected. However, we demonstrate that the disturbance size follows a power law distribution. The density function \( f(x) \sim k \cdot x^{-\gamma}, k > 0 \) and \( \gamma > 1 \), for large disturbances (\( x \to \infty \)). That is, \( \log[P(X > x)] \sim (1 - \gamma) \cdot \log x + \log[k/(\gamma - 1)] \) when \( x \to \infty \). This observation is also supported by studies of disturbance data from one U.S. power grid.

Further, the analysis shows that the time \( T \) between the disturbances is exponentially distributed, \( T \in \text{Exp}(m) \). If we consider disturbances resulting in unserved energy not caused by lightning strikes, \( N(t) \) in \((0, t]\), they can be described by a Poisson process, \( \{N(t); t > 0\} \), \( N(t) \in \text{Po}(\lambda t) \). The estimate \( \lambda^* = 1/m^* \approx 0.017 \) (disturbances per day) for the national Swedish transmission grid.

Searching for Swedish power disturbance data, we have been in contact with a number of organizations (several utilities, public organizations and authorities, and other organizations) through their representatives and through their publications. An important finding from the work with this study is that knowledge of statistical methods and the practice of handling data in general is relatively low. Discussions on quality of the data are sparse, and existing data material is seldom analyzed with statistical methods. Here one can compare with how data on occupational accidents and road traffic accidents are collected and analyzed.

### 4.3 Graph modeling and vulnerability analysis of power delivery networks

In the third paper, we model networks as graphs \( G = (V, E) \), i.e. sets of vertices \( V \) (nodes) and edges \( E \) (links). The objective of our analysis is to advance the understanding of the nature of the infrastructure systems, especially electrical power delivery networks, and to study how the structure of a network affects its vulnerability.

Many complex networks exhibit a tendency to cluster; in social networks this represents circles of friends in which every member knows each other. Further, the “small world”-property appears to characterize complex networks, i.e. despite their often-large size there is a relatively short path between any two vertices. Finally, several complex networks have a het-
erogeneous topology, i.e. some vertices have a very large number of edges connecting to them, and other vertices only have few edges. Hence, we calculate three quantities to describe the network’s topology: the clustering coefficient $C$ (a local property that captures the density of triangles in the graph), the average path length $\ell$ (the number of edges between every pair of vertices in the graph, a measure of how scattered the graph is) and the degree distribution $P(k)$ (the probability that a randomly selected vertex has exactly $k$ edges).

Empirical studies of the Nordic power transmission grid and the Western States transmission grid in the United States show that they are more scattered, and have a more tree-like structure, than the two most frequently used model networks in graph theory, i.e. the Erdös-Réyni random graph and the so-called Barabási-Albert scale-free network. The Nordic grid is more scattered than the Western States network, i.e. $\ell$ is larger and $C$ is lower. For both power grids $C$ is significantly larger than the equivalent random graph, and $\ell$ is more than twice as large. However, we point out that $C$ is not an ideal measure for meshed networks such as power grids. For small networks, we propose using the number of cycles in the graph instead of $C$, which only captures the cycles with three edges. Further, we demonstrate that $P(k)$ of the Nordic network decays exponentially (compared with scale-free networks, e.g. the Internet, where $P(k) \sim k^{-\alpha}$). This characteristic feature of power transmission grids is supported by earlier studies of the Western States transmission network.

Next we study how the networks disintegrate when vertices are disabled. Two kinds of threats are considered: the removal of randomly chosen vertices (error tolerance) and the removal of deliberately chosen vertices (attack tolerance). Deliberate attacks are realized through the removal of vertices in decreasing degree order. The empirical networks exhibit similar disintegration patterns. All four networks disintegrate considerably faster when the vertices are removed deliberately than randomly, i.e. they have a lower attack tolerance than error tolerance. We can clearly show that the scale-free network and the power grids are more sensitive to attacks than the random graph, and thus the behavior of the two model networks is in accordance with earlier studies.

In the second part of the paper we present a graph influenced vulnerability analysis of a fictitious power delivery network. We illustrate how a wide spectrum of threats can be represented as the removal of vertices and edges, and evaluate different strategies to decrease the vulnerability. For the given example, a combination of measures to enhance the robustness and the resilience of the system yields the largest decrease in vulnerability.
The measures we use to classify graphs mainly give an idea of the average topological properties of the network. Only large changes of the networks topology will be visible by studying these quantities (indicators). The relation between the vulnerability of a network and the values of the graph measures is not straightforward. We show that the generic topological analysis of error and attack tolerance is too imprecise to enable a realistic study of an upgrading of the Nordic transmission grid. Consequently, a graph analysis requires detailed topological data if the benefits of an upgrading of a real-life network is to be evaluated. Actions taken to enhance the resilience of the network are not captured at all by the graph measures.

Several important characteristics of electric power networks are abstracted away in the graph modeling. An important challenge lies in capturing the dynamical behavior of power grids, e.g. analysis of cascading failures as a result of instability. Attempts have, however, been made to analyze cascading failures, and include capacity constraints, in graph models.

There are various simulation packages used in planning, management, and daily operation of power systems. However, the “power engineering aspects” dominates in the simulation models, and the author does not know of suitable simulation packages for studying vulnerability (planned attacks and large-scale disturbances) and operational and technical crisis management at a societal level. Graph modeling gives a conceptual picture of the studied network, and graphs can serve as simple reference models to compare with. Presently, it is an open question weather we shall continue to extend the graph models further or if it is possible to adapt existing power engineering simulation models. Irrespective of which, we believe that further studies of the vulnerability of power networks would benefit from a cross-fertilization between electric power engineering, risk and policy analysis and the mathematical modeling of complex systems.
Chapter 5

References


