# Critical Infrastructures as Socio-Technical Systems

## Applications to electricity distribution systems

**Finn Landegren**

LUND UNIVERSITY

**Licentiate Thesis**

**Department of Industrial Electrical Engineering and Automation**

**2014**

Department of Industrial Electrical Engineering and Automation

Faculty of Engineering

Lund University

Box 118

221 00 LUND

SWEDEN

http://www.iea.lth.se

ISBN 78-91-88934-65-9

CODEN:LUTEDX/(TEIE-1073)/1-135/(2014)



Printed in Sweden by Tryckeriet i E-huset, Lund University

Lund 2014

“Scientists, philosophers, writers, engineers, doctors, astronauts, and ordinary people are working tirelessly on world-changing projects, assuming that one day our lives can be saved on a massive scale. As their work comes to fruition, our world becomes a very different, more liveable place.”

Annalee Newitz from *Scatter, Adapt, and Remember –*

*How Humans will Survive a Mass Extinction (p. 11)*

# Abstract

Our society has come to depend to an increasing degree on a set of critical infrastructures examples of which are the power, transport, water and telecommunication systems. Several past events, e.g. the hurricane Gudrun in Southern Sweden in 2005 and the volcanic eruption of Eyjafjallajökull in Iceland in 2010, high-light the vulnerability of these systems as well as the immense societal consequences that system failures can bring about.

Several researchers argue that in order to make progress concerning risk and vulnerability analysis of critical infrastructures a broader scope is needed that takes into account not only the technical network which is at the heart of most of these systems but also organizational and societal system aspects. The suggestion that critical infrastructures should be viewed as socio-technical systems is guiding the present research. The research work has been focused at the electricity distribution system, which is a crucial part of one critical infrastructure.

The thesis consists of three main research tasks. The first of these is a review of approaches that have been used for simulating socio-technical systems. The suitability of the presented modeling approaches for performing vulnerability analyses of CIs is investigated. It is concluded that a hybrid model, combining network theory modeling and agent based modeling, should be useful for treating three issues that are of interest in risk and vulnerability analysis of critical infrastructures.

The second research task concerns analysis of societal consequences from disruptions in electrical distribution systems. A case study is performed on a municipal electricity distribution system. Two Swedish electricity regulations, outage compensation and Styrel, are used to obtain measures of societal consequence from power outages. (Styrel is a system used at a national level in Sweden for prioritizing power consumers based on their importance to society. In order to achieve this all Swedish electricity consumers are grouped into nine predefined priority classes.) It is found that results given by the two measures are not, overall, well correlated and it is concluded that this indicates that the present system for outage

compensation does not capture the consequences from power outages of high priority customers, as measured with Styrel.

The third research task concerns analysis of restoration processes following disruptions in electrical distribution systems. A socio-technical model is developed that describes the infrastructure network as well as the repair teams responsible for restoring the system in case of failure. A method is suggested that makes it possible to analyse resilience of critical infrastructures through simulation of restoration processes. The method is demonstrated in a case study on the municipal electricity distribution system that is mentioned above. It is analysed for six levels of strain on the network how the resilience of the system depends on amount of available repair teams as well as on six different kinds of material resources used by the teams. It is found that, when back-up power is not considered, electricity will be restored to some customers after much more than 24 hours in some of the simulated scenarios. This is the case for all levels of strain as well as for all analysed levels of resources. Back-up power, which is not considered in the analysis, will therefore be necessary in order to abide by the Swedish law requirement of restoration of all customers within 24 hours.

It is concluded that the developed methods, by focusing on vulnerability and resilience rather than risk and hazard, could be useful when preparing for a wide range of foreseeable as well as unforeseeable hazard events.

# Acknowledgements

Having studied the critical infrastructures of our society I've also come to learn quite a bit about the critical role of friends and colleagues. Therefore thanks are in place.

First and foremost, Jonas and Olof, thanks for coming up with a thrilling research topic. Thanks also for acting as the supervisors you are by not letting me go astray but instead consistently pointing to the goal I should aim for. I'm looking forward to continued work together with you.

Thanks also goes to the employees at the electricity distribution company for offering me the material without which the research presented here could never have been done. I especially appreciate the hands-on experience you gave me through the afternoon round trip that we did.

Thanks IEA colleagues for an enjoyable work environment and for much warmth. Thanks for the good conversations we have had going in the lunch restaurant as well as at fika and the occasional afterwork.

Thanks also to the project partners in PRIVAD, fellow PhD-students as well as more senior researchers. I really appreciate the great breadth of competencies that we have within this project and I hope that we will be able to intermingle these competencies in our future work.

Thanks MSB for funding my research. I'm inspired by the thought of being able to contribute to your vision of a functioning society in a changing world.

Thanks friends in Uppsala and elsewhere for enriching my life. Thanks mum, dad, Nils, Kalle and Elisabeth, grandma Birgit and grandma Ingrid for all your support and care.

Last but definitely not least: thanks Taravat, azizam, for being my life partner.

**Thanks!!**

# Contents

# Chapter 1

# Introduction

This chapter first provides a background to the field of risk and vulnerability analysis of critical infrastructures, and briefly introduces the challenges that are posed here. The objectives and delimitations of the thesis are then described. This is followed by a presentation of the contributions of the research underlying the thesis. Then an outline of the thesis as well as a list of publications on which the thesis is based is provided. It is also clarified how the publications relate to the overall purpose of the thesis.

Our society today depends on technological systems of a complexity vastly surpassing what could be conceived of only a hundred years ago. Among these systems so called critical infrastructures have a primary importance. While critical infrastructures have undeniably provided us with great benefits they have also become unprecedented sources of vulnerability (Winner, 2004). Spending a day without access to electrical power, transportation systems, telecommunication systems, banking services, etc., proves increasingly difficult for the majority of the population in modern societies. However, it is not easy to predict what threatening events will in fact exploit the vulnerabilities of these complex systems. Before the new millennium there were widespread beliefs that the energy grid, airline, transportation, banking, and other systems would be disrupted by computer malfunctions set off by the millennium bug, and that society would thereby be plunged into chaos (Winner). While this prediction did not come true, other events that few foresaw instead came to pass, notable among these is the 9/11 terror bombing. This, as pointed out by Lewis "was an attack on banking and finance, using the transportation sector" (Lewis, 2006, p. 6). However water systems as well as ground based transport systems were indirectly affected. Following the disaster 210 million liters of water were each day flowing through broken water mains. The combined effect of falling debris and flooding also impacted the telecommunication system as well as the transportation system (O'Rourke, 2007). The collapse of the World Trade Center towers also caused major damage to the slurry wall that surrounded the building's basement. If this wall had failed it could have lead to flooding of the underground rail system of New York (Little, 2004). It was hard to predict the World Trade Center bombing prior to the actual event, and most likely today it is equally hard to predict the next major catastrophic event. It might, as some have predicted, come in the shape of an "electronic Pearl Harbor" set about by a concerted action by hackers (Bendrath, 2001), or as a nuclear attack launched by terrorists (Allison, 2004). Indeed, as Perrow argues, there is no need to smuggle weapons of mass destruction through our borders. "They already litter our landscape [often in the form of large industrial facilities] and they are more likely to be triggered by natural and industrial disasters than terrorists" (Perrow, 2011, p. 2). A wide array of natural disasters including storms and floods, possibly fuelled by man-made climate change, as well as solar storms, volcano's and earth-quakes also threaten to disrupt the systems upon which we depend. Considering the poor condition of large parts of the global economy in recent times, the threat may also come in the form of major economic set-backs. After all, what would happen to the critical infrastructures if money for their maintenance dwindled? Indeed as has been argued by Rees (2013) many of the risks that can be foreseen today are so great as to threaten the very existence of the human population. Using the terminology of former US secretary of defense, Donald Rumsfelds (Pawson et al., 2011), we can conclude that several of the hazard events that the future has in store for us are known knowns, meaning that we are aware of their possibility as well as the consequences that they could have. However, a second, more worrisome category is the known unknowns, comprising the scenarios that we know could be realised but whose consequences cannot as yet be foretold with any certainty. Even more troublesome, finally, is the unknown unknowns, comprising the hazard scenarios that the future might bring with it but that we, at our present state of knowledge, have as yet no awareness about. All of these issues makes it a high priority to find new and better ways of securing our critical infrastructures.

In this thesis critical infrastructures (from now on referred to as CIs) is the main subject. Edwards argues that the most noticeable feature of these systems is how little we notice them, they are as much taken for granted as the air we breathe (and as necessary for our survival one might add). Yet, as he further points out, these systems define our very existence, "to be modern is to live within and by means of infrastructures". They are one of our principal means of dealing with the world around us and make it conform to our needs (Edwards, 2003, p. 2). Several researchers point out that new methods are needed in order to grapple with CIs and their vulnerabilities (Rasmussen, 1997; Leveson, 2004; Hansman et al., 2006; Qureshi, 2007; Johansson et al., 2013). One characteristic that sets CIs apart, and that makes new approaches called for, is that they are not, like computers, cars or skyscrapers, entirely made up of technological component parts. Instead they are hybrids, encompassing technological components as well as individual human operators and entire organizations. It is this characteristic that makes it possible to view them as so called socio-technical systems (STSs). Qureshi reviews accident modelling, a field that is closely related to that of risk analysis since accident models are used for analysing the risk of coming accident events as well as for analysing the causes of past accidents. He argues that traditional models within this field do not take into account the kind of accident causation that is typical for STSs, namely those where the cause cannot be attributed to a single component failure or human error, but rather to the interaction of technical, human and organizational factors (Qureshi, 2007). Rasmussen similarly questions the adequacy of traditionally used accident models, since they tend to disregard all except the lowest levels of the hierarchy that most STSs constitute. While the levels of a STS in fact range from politicians and legislators, over managers and work planners to system operators and the physical process, the focus of traditional accident models is on the last two levels, i.e. the operator level and the physical level. Due to this blind spot we oftentimes cannot see that the stage for an accident is set already at the legislative or the management level (Rasmussen, 1997). The methods presented in this thesis are in fact not covering this wide range of system levels. The method presented in Chapter 6 is only taking the two last levels into account, while the method presented in Chapter 5 is only taking the last level into account. This weakness is discussed further in Chapter 7. Hansman et al. (2006) suggests that in order to handle CIs and the system of systems that they together constitute, integrated socio-technical models are needed that usefully describe the interactions between the technical infrastructure and its social context. Little, similarly, proposes that the challenges of CIs could be met if a holistic strategy is used where technology, people and institutions are included, and he argues that this would lead to far greater long-term security (Little, 2004).

In this thesis the electricity distribution system, which is part of a CI of special importance in today’s society, is simulated as a STS. The hypothesis behind this research is that systems that involve not only technical aspects, or social/organisational aspects, but rather are characterized by the interplay of these two system aspects can be better understood if such a simulation approach is used. Two issues where a socio-technical interplay is involved and on which this thesis can hopefully shed some light is that of restoration processes in the electricity distribution system and societal consequences from disruptions of the electricity distribution system. Concerning the work on restoration processes the time duration required to bring all customers back, after failures occur in an electricity distribution network is studied. The possibility of using back-up power is however disregarded in this work. It is also analysed in what way the outage time depends on system parameters of the repair system, e.g. number of spare parts and number of repair teams. Based on the method that is developed it is possible for network operators to see what their margin is to safety boundaries as well as the way that outage times will increase as they approach the boundary. In the work that has been done concerning assessment of societal consequences from CI disruptions failure scenarios in a CI network are simulated and ranked in accordance with two methods for assessing societal consequence from outages. The method makes it possible to compare the results from the two ways of assessing societal consequences to see to what extent they are in agreement.

As has been indicated the field of risk and vulnerability of CIs is broad and poses several great challenges to the research community. In this thesis, by necessity, the focus is narrowed down. As was previously mentioned only the lower levels of the STS that the electricity distribution system constitutes is explicitly simulated, i.e. the technical and operator levels. Furthermore concerning the variety of hazard scenarios that was referred to previously none is explicitly analysed. Instead a vulnerability and resilience analysis approach is chosen, meaning that perturbations of the electricity distribution network and the resulting customer outage times are analysed regardless of what particular hazard event could actually give rise to the perturbations in question. The choice to focus on vulnerability and resilience rather than risk and hazard (see section 2.3 for a clarification of these concepts) is made for the reason that has been hinted at above, namely that the number of hazard events that is known to be possible is great and that, along with these are known unknowns as well as unknown unknowns that might outnumber the known hazard events by far. This being the case it becomes problematic to attend to each individual hazard individually and build one specific defence for each one of them. Instead of doing this an approach based on vulnerability analysis and resilience engineering is here advocated for as a complement to hazard and risk analysis. Regardless of what hazard event that is in fact realised the ability of our CIs to either withstand system strain, due to robust design, or quickly recover, thanks to an efficient repair system, will be of crucial importance. These two issues are in focus in the research presented below.

## 1.1 Objectives and delimitations

The overarching objectives of the research work presented in this thesis is to develop methods that can be used to :

1. Analyse societal consequences from disruptions of CI networks;

2. Analyse safety boundaries for CIs based on simulation of CI restoration processes.

The developed methods have been applied to an electric distribution system and their applicability can only be guaranteed within this domain of application. The motive for choosing to focus on one particular CI is that the methods can then be more quickly tried out and tested as the complexity of modelling several different systems is avoided. In a later stage the methods can hopefully be applied to a wider range of CIs and then perhaps also account for CI interdependencies (see Chapter 8). There are several reasons why an electric distribution system has been chosen for testing the methods. Firstly data on network topology is relatively easy to obtain for electric distribution systems. Furthermore, the electric distribution system is a crucial part of an especially important CI. While society is dependent on all its CIs, the CIs themselves are all dependent on the power system as is indicated by Figure 1.1. The matrix shown in Figure 1.1 is based on answers by representatives of CIs (one representative per CI sector) in southern Sweden. It was presented at a seminar arranged by the Scania county board. The figure shows the answers from the participants, the results are however only preliminary. While it is unlikely that actors will falsely believe themselves to be dependent on CI services of some kind the opposite is likely to be the case, i.e. actors can falsely believe themselves to not be dependent on CI services. Notably the dependency matrix presented here seems to suffer from such flaws. Several actors, for instance the representatives of the electricity and fuels CIs, seem to have underestimated their level of dependence on CI services. The crucial importance of the power system is also indicated by disasters in the past. As pointed out by Mili et al., "The prolonged disruption of the electric infrastructure throughout the region after Hurricane Isabel led to a domino-like failure of nearly every regional infrastructure system within a matter of hours or days" (Mili et al., 2004, p. 5).

| | Electricity | Heating | Fuel | El. communication | Emmergency com. | Financial services | Mail services | Water and sewer | Food | Road transport | Rail transport | Air transport | Sea transport |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Electricity | ■ | | ● | | | | | | | | | | |
| Heating | ● | ■ | ● | | | | | | | ● | ● | ● | ● |
| Fuel | ● | | ■ | | | | | | | | | | |
| El. communication | ● | | ● | ■ | | | | | | ● | ● | ● | ● |
| Emmergency com. | ● | | ● | | ■ | | | | | | | | |
| Financial services | ● | | | ● | | ■ | | | | | | | |
| Mail services | ● | | | ● | | | ■ | | | | ● | ● | |
| Water and sewer | ● | | ● | ● | | | | ■ | | ● | | | |
| Food | ● | | ● | | | | | ● | ■ | | | | |
| Road transport | ● | | ● | | | | | | | ■ | | | |
| Rail transport | ● | | ● | | | | | | | | ■ | | |
| Air transport | ● | | ● | ● | | | | | | | | ■ | |
| Sea transport | ● | | ● | ● | | | | | | | | | ■ |

Figure 1.1: Dependency matrix based on answers from representatives of CIs in southern Sweden. A point on row m and column n indicates that actor m depends on actor n.

In order to reach the overarching objective a number of subordinate tasks have to be carried out. As argued by Shinozuka et al. (2003, p. 66): in order to model "the impacts of electric power disruption […] one must:

1) Assess how damage to individual pieces of electric power equipment affects power flow across the network;

2) Model how a damaged network would be repaired and how electric power would be restored over space and time;

3) Capture how the loss of electric power would affect households, businesses, and other units of society, not only directly but also

> indirectly through the cascading failure of other utilities, typically water systems."

A model will be developed that encompasses the three domains identified by Shinozuka et al. (See Figure 1.2). So far this model, spanning the three system domains has not been realised. Instead parts of the chain have been addressed separately in two different modelling methodologies.

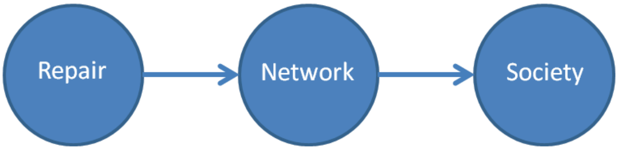


Figure 1.2: Domains covered in this thesis.

The reason why it is of interest to include these domains within one modeling context is the following: the network model is needed for identifying possible failure scenarios and their overall implications for the functionality of the network. The model of the repair system is needed for determining the time duration of the functionality loss in the network. Finally the societal model is needed to determine what the societal consequences will be in terms of money, losses in life and health or other for a functionality loss of a certain size and duration. Each domain in the model therefore is essential for enabling the analysis of how failures in the network give rise to societal consequences. Since, in the two methods presented in this thesis only parts of the chain have been covered, the methods cannot achieve the above mentioned results. In the method for analysing restoration times societal consequences are not addressed in detail, but only takes into account the number of customers that are not supplied with power. Similarly the method for analysing societal consequences of power outages is not explicitly taking repair into account but instead assumes a static restoration time. Concerning 1), a simplification has been done which deviates from what Shinozuka et al. proposes. Power flow is not explicitly modelled; instead a purely topological model is used for reasons of computational efficiency (see discussion about model validity in section 5.4). Concerning 3) indirect effects of power outages are not explicitly modeled. Instead assessments have been used that have been done as a part of the Styrel system (Energimyndigheten, 2012) (more details about Styrel are given in section

3.2). The purpose of the Styrel assessments is to permit practical prioritization of customers regarding societal consequences from power outages. The explicit aim of the Styrel system (Energimyndigheten, 2011, p. 18) is also that interdependencies and indirect effects should be taken into account in the assessments. This important aspect of societal consequences from CI disruption which Shinozuka et al. mentions can therefore be assumed to be taken into account by the Styrel assessments.

## 1.2 Contributions

The main scientific contributions of the research underlying this thesis are the following:

1) A case study in which a comparison is made between results obtained with two different power outage consequence measures (see Chapter 5);

2) A method that enables analysis of four issues that are crucial for assessing resilience of electrical distribution networks (see Chapter 6).

## 1.3 Outline of thesis

Chapter 2 discusses concepts that are of crucial importance in the thesis. In the first section the critical infrastructure concept is introduced. Next an introduction is given to the concept of socio-technical systems. Then the concepts risk, vulnerability and resilience are discussed. Finally network theory is presented as it is used in the research to represent the physical infrastructure network.

Chapter 3 provides background information about the electric distribution system. The chapter starts off by describing the structure of the entire power system. Then the issue of power system regulations is discussed and an overview of Swedish regulations is given. Finally power distribution restoration is discussed. This concept here denotes the process by which electricity is brought back to customers following upon disruptions in the distribution system.

Chapter 4 reviews approaches for performing computer simulations of STSs. The suitability of the presented modelling approaches for performing vulnerability analyses of CIs is investigated.

Chapter 5 presents the method proposed for analysing societal consequences from disruptions in the electrical distribution system. Two different electricity regulations are used to obtain measures of societal consequence and the results given by the two measures are compared.

Chapter 6 presents the method proposed for assessing resilience of electrical distribution systems. It is investigated how outage time depends on the availability of repair personnel and materiel.

Chapter 7 contains a discussion of the results presented in Chapters 4-6. In Chapter 8 conclusions are given and possibilities for future research are mentioned. Finally, after the reference list the abbreviations that are used most frequently in the thesis are listed.

## 1.4 Publications

The thesis is based on the following two publications as well as a paper on which work is ongoing.

1. Landegren, F., Johansson, J., & Samuelsson, O. (2013). Review of Computer Based Methods for Modelling and Simulating Critical infrastructures as Socio-Technical Systems. In *European Safety and Reliability Association Conference (ESREL2013)*, *Amsterdam, Netherlands, September 29, 2013*.

2. Landegren, F., Johansson, J., & Samuelsson, O. (2014). Comparing Societal Consequence Measures of Outages in Electrical Distribution Systems. In *European Safety and Reliability Association Conference (ESREL2014), Wroclaw, Poland, September 14, 2014.*

3. Landegren, F., Johansson, J., & Samuelsson, O. Mapping the Space of Safe Operation for Socio-Technical Systems, To be submitted.

The relation between the papers and the three system domains of interest in the research project is illustrated in Figure 1.3. Paper 1, presented in Chapter 4, reviews methods for modeling STSs and the intention when doing this paper was to find ways of modeling the three system domains simultaneously. In other words this paper can be said to cover all three system domains. Paper 2, presented in Chapter 5, concerns assessment of societal consequences from power outages. A network model is here used to simulate failure scenarios and two Swedish electricity regulations are used to assess the consequences of the failure scenarios. In this way the network and society system domains are covered by this paper. Finally in paper 3, presented in Chapter 6, restoration processes are simulated[1]. In order to do this failure scenarios are once again simulated by means of a network model and a model of a electricity network repair system is used to assess the time required to bring electricity back to all customers. In other words the repair system as well as the network domains are covered by paper 3.

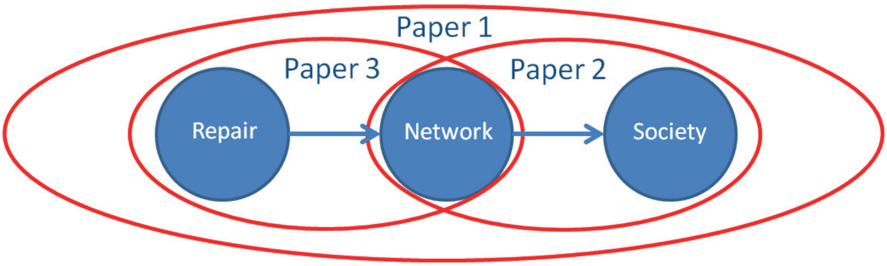


Figure 1.3: Picture explaining the relevance of the papers to the three domains of interest.

[1] Back-up power is not considered in the simulation of restoration.

# Chapter 2

# Concepts and definitions

In the previous chapter the CI research field was introduced and it was proposed that progress could be made in this field if CIs are analysed as STSs. It was also said that this thesis is intended to apply the STS perspective to electrical distribution systems, which is a part of one CI, in order to treat two particular issues: restoration processes in electricity distribution systems and societal consequences from disruptions in electricity distribution systems. In this chapter concepts that are of fundamental importance in the thesis are presented and it is clarified what is meant by these terms. First the CI concept is treated, since the electricity distribution system, which is studied in this thesis, constitutes a part of a CI. Then follows an introduction to the socio-technical system concept. The reason for giving this introduction is that the STS perspective constitutes the lens through which electricity distribution systems are looked at in this thesis. This is then followed by a presentation of the three closely related concepts risk, vulnerability and resilience. The reason for presenting these issues is that the developed methods are intended to be of use primarily in the context of vulnerability analysis and resilience engineering. Finally network theory is described, this is motivated by the fact that this modeling approach is at the center of the methods presented in this thesis.

## 2.1 Critical infrastructures

The aim of the research presented in this thesis is to develop a method for analysing the vulnerability of society with respect to disturbances in CIs. The CI concept is therefore of crucial importance in this thesis. Edwards proposes that the concept "'infrastructure' is best defined negatively, as those systems without which contemporary societies cannot function"

(Edwards, 2002, p. 3). Finger et al. (2005) on the other hand give a more explicit definition of infrastructures arguing that they have three generic features in common. Firstly they are based on physical networks, secondly they pose challenges to institutional governance since traditional market oriented solutions are often not possible since severe forms of market failure are involved. Therefore supporting regulation is needed to ensure proper functioning of these sectors. Thirdly, infrastructures serve major social needs and are of significant economic and political importance.

CIs are a subset of infrastructures. They have been given the following definition in the first version of the US National Plan for Critical Infrastructure: “those systems and assets – both physical and cyber – so vital to the Nation that their incapacity or destruction would have a debilitating impact on national security, national economic security and/or national public health and safety” (Moteff & Parfomak, 2004, p. 5). Yusta et al. (2011) provide a similar definition stating that “there is broad consensus in defining the critical infrastructure as the ones whose sudden unavailability may cause loss of life, serious or severe impact on health, safety or economy of citizens” (Yusta et al., 2011, p. 6102). Thus, while all infrastructures enable major societal functions, the subset of infrastructures referred to as critical enable societal functions that are fundamental for national security, national economic security and/or national public health and safety.

While the CI concept is rather new, having been used since the 1980s (Moteff & Parfomak, 2004, p. 4), the phenomenon which it describes has been with us for a long time. It has been observed that the destruction of the Roman aqueducts by the Goths who lay the city under siege in 537 A.D. ended the rule of Rome (Winner, 2004). Already at that time infrastructures were fundamental for national security. Collier & Lakoff (2008) provide an overview of how this phenomenon has developed in more recent times. The Italian military theorist Douhet conceived what became known as the theory of strategic bombing, which was later widely applied in WW2. According to this theory “bombers would attack ‘the most vital, most vulnerable, and least protected points of the enemy’s territory”. Douhet identified five vital centres of a modern nation that were the key targets of strategic bombing: industry, transportation infrastructure, communication nodes, government buildings and ‘the will of the people’ (Collier & Lakoff, p. 6). Strategic bombing theory was later developed at the US Air Corps Tactical School (ACTS). In order to identify targets that were vital for the enemy they made use of a theory of the "industrial web". It was suggested that the modern economy was composed of 'interrelated and entirely interdependent elements'. By understanding the structure of the industrial web the strategic bombing theory would make it possible to identify the "relatively few objectives whose destruction would paralyze or neutralize" the enemy war effort (Collier & Lakoff, p. 7). As a way of preparing for such an attack ACTS theorists engaged in what was perhaps the first effort to catalogue the CIs of the US (Collier & Lakoff, p. 11).

While the strategic bombing theory and its idea of the industrial web had been concerned with symmetric warfare, i.e. conflicts between states, the issue of asymmetric warfare, i.e. conflicts between states and small groups or individuals, began to move into the centre of attention towards the end of the 20$^{th}$ century. International terrorism during the mid-1990s created renewed interest in CIs. As a result of this interest President Clinton signed the Executive Order 13010 in 1996, thereby setting up a list of prioritized infrastructure sectors as well as specific assets within those sectors, based on national importance. The following were considered to be critical infrastructures:

- telecommunications;
- electrical power systems;
- gas and oil storage and transportation;
- banking and finance;
- transportation;
- water supply systems;
- emergency services (including medical, police, fire and rescue) and
- continuity of government..

With time the list of CIs has expanded, and the Department of Homeland

Security today includes 16 critical infrastructure sectors[2]. The issue of protecting CIs began to be more widely discussed within EU following the train bombings in Madrid (2004) and London (2005). This led to the establishment of the European Programme for Critical Infrastructure Protection (EPCIP). EPCIP is among other things responsible for identifying critical infrastructures (MSB, 2006).

## 2.2 Socio-technical systems

CIs are analysed in the research presented in this thesis. CIs are generally socio-technical systems (STS) and the aim of the thesis is to study them as such, i.e. to include technical as well as organizational system aspects in the model that is used. It is therefore important to discuss the STS concept. The STS concept was introduced in conjunction with research done at the Tavistock Institute concerning the British coal mining industry (Trist, 1980, p. 7). Trist, who was involved in this pioneering work, explains that he had been inspired by the social philosopher Mumford into thinking that technology and society, although not connected by any linear causality, were "intertwined in a complex web of mutual causality. In the language of E.A. Singer they were co-products of each other" (Trist, p. 13). It is this "intertwinedness" of societal and technological entities that the STS concept is meant to convey. Trist et al. suggests that the STS analysis should be performed at three distinct levels: the primary work system; the whole organization; and the macro-social phenomena (Trist, p. 11). It is suggested by Trist that the technological and organizational aspects of a STS should be jointly optimized. If only one of these aspects is optimized the result will be overall sub-optimization (Trist, p. 24). In order to achieve this joint optimization a STS perspective is required.

What systems should then be considered STSs? Ottens et al. (2006) provide an answer by distinguishing between three different types of engineering systems: "(1) engineering systems that perform their function without either actors or social institutions performing a sub-function within the system [e.g. the landing gear of an airplane], (2) engineering systems in which actors perform sub-functions but social institutions play no role [e.g. an airplane] and (3) engineering systems that need both actors and some social/institutional infrastructure to be in place in order to

[2] http://www.dhs.gov/critical-infrastructure-sectors

perform their function [e.g. an airport].” (Ottens et al., 2006, p. 134-135) They conclude that members of category 1 are purely technical system while members of category 2 are human-technology systems. Members of category 3, however, are STSs. They furthermore suggest that most large infrastructure systems belong to this category. Something that distinguishes the STSs from the two other categories of engineering systems, defined by Ottens et al., is that they cannot be controlled or designed in the same way. Kroes et al. (2006) argues that: “At the socio-technical level many stakeholders are involved that all have their own goals and visions, and normally none of these actors can impose their decisions on the other actors. For this reason STSs cannot be designed, made and controlled from some central point of view, as for instance a car. Instead the STS is continuously being redesigned by many actors from within the system” (Kroes et al., 2006, p. 813).

A STS perspective can prove advantageous when performing risk and vulnerability analysis since it makes it possible to identify vulnerabilities and risks that exist not only in the social system domain or the technological system domain but rather in the interaction of these two domains. One case where a STS perspective could be of value is the growing disproportionality between our CIs and their governing structures that is pointed out by Bruijne & van Eeten (2007, p. 4). They argue that “while our CIs have become more complex and interconnected, the management of these CIs has become increasingly institutionally fragmented” (Bruijne & vad Eeten, p. 4). Bruijne & van Eeten here suggest that hazards of technological systems might fundamentally be due to the design of societal systems and the interactions of the societal and technological systems. This indicates that an analysis spanning the technological and societal domains is advantageous for identifying the vulnerabilities of our society.

## 2.3 Risk, vulnerability & resilience

In this thesis vulnerability and resilience of the distribution system and society are analysed while risk on the other hand is not investigated. However, since these three concepts are closely related, with the risk concept constituting a necessary back-ground to the other two concepts, they are all introduced in this section. Risk has been defined in several ways among which are the probability for an adverse outcome, the variability of the outcome and the product of the probability and the degree of an adverse outcome (Grimvall et al., 2003, p. 16-17). An especially influential definition is the so called quantitative definition of risk that was proposed by Kaplan & Garrick (1981). According to their approach risk assessments are done by answering three questions: what can happen, how likely is it and what are the consequences? These three questions are referred to as a risk triplet. Risk $R$ can in other words be defined according to the following equation:

$$R = \{< s_i, p_i, x_i >\}$$

Where $s_i$ is a scenario, $p_i$ is the probability of the scenario and $x_i$ is the consequence of the scenario. The curly brackets, $\{ \quad \}$, indicate a set that includes all scenarios, $s_1$ to $s_N$, with their respective probabilities and consequences. In order to obtain a true assessment of R three conditions must be met (Hassel, 2010, p. 31): 1) scenarios should be disjoint, i.e. they should not overlap, 2) the set of scenarios should be complete, i.e. all scenarios should be considered although not necessarily in detail and 3) in order for the assessment to be practically possible the number of scenarios must be finite. While these conditions can all be met in a relatively uncomplicated situations as for instance when assessing the risk of losing when playing the roulette, it is safe to say that in any moderately complex system these three conditions can never be fully met, and in such cases, only approximations of R can be achieved. Risk analysis can in these cases be defined as the search for ever better approximations of R. This is so since perfect knowledge of R would mean that we know all adverse scenarios that could be realised as well as the probability and degree of adversity of each such scenario. Possessing this knowledge nothing more could conceivably be gained concerning risk awareness and clearly there would, in such a case, be nothing left for risk analysis to accomplish. In order to act on the basis of a risk analysis the relative importance of probability and consequence as determinants of risk has to be decided. As argued by Kasperson et al. (1988) this is not easy. It might seem commonsensical to assume that society should be indifferent toward a low-consequence/high-probability risk (for instance causing one death per year) and a high-consequence/low-probability risk (causing one thousand deaths per thousand years). In fact people generally prefer the former. The perception of risk is also much affected by the kind of scenario that is considered, irrespective of the likelihood and consequence of the scenario.

A further problem with the risk definition proposed by Kaplan & Garrick is that the three questions are in certain cases notoriously difficult to answer. This tends to be the case when possibly radical shifts in the development of technology and society are involved (e.g. development of genetically modified organisms and nano technology). Clearly if it is not possible to say what can happen, how likely it is, or what the consequences would be, the quantitative definition of risk becomes untenable. In order to handle such situations the so called "precautionary principle" has been suggested and was adopted by the EU in 2000. Three versions of this principle have been proposed (Little, 2004, p. 54):

- Lack of full scientific certainty about a risk shall not justify postponing an action to prevent it;
- Uncertainty of a risk justifies action to prevent it;
- The proponent of an activity posing uncertain risk bears the burden of proving that the activity poses "no" or an "acceptable" risk before the activity can go forward.

According to the definition used here a risk analysis can be subdivided into two parts: threat analysis and vulnerability analysis. The first analyses concerns what can happen to a system, the second concerns how severe the consequences for the system will be (Holmgren, 2006). Accordingly, two main strategies for achieving risk reduction can be distinguished: 1) preventing or staving off threats and 2) reducing the vulnerability of the system to the threats. A main advantage of engaging in the latter is that in many cases the number of threats that the system could be exposed to is too great to make individual treatment of the threats possible. A more generic approach is then called for, which the vulnerability analysis can provide by pointing out general weaknesses of the system that could be exploited by multiple forms of hazards. As proposed by Hassel (2010) and Johansson (2010) vulnerability can be defined similarly to how Kaplan and Garrick define risk, i.e. by answering three questions: given a specific perturbation to the system what can happen, how likely is it given the perturbation and what are the consequences? These three questions are referred to as a vulnerability triplet. The vulnerability of a system to a certain perturbation can in other words be defined according to the following equation (Hassel, 2010, p. 37):

$$V_P = \{< s_i, p_i, x_i >\}_P : s_i \in s_P$$

Where $V_P$ denotes the vulnerability of a system to a perturbation P, and $s_P$ is the set of scenarios that can result from the perturbation P. The scenarios considered when determining $V_P$ all belong to $S_P$, i.e. $s_i$ is a scenario that can result given the perturbation P, $p_i$ is the probability of this scenario happening given the perturbation P and $x_i$ is the consequence of the scenario. The three abovementioned conditions that should be fulfilled by a risk analysis should hold true also for vulnerability analysis, i.e. the set of scenarios should be disjoint, complete and finite if a correct assessment of $V_P$ is to be obtained. As is the case for risk analysis the practical result of a vulnerability analysis can only be approximations of $V_P$ when sufficiently complex systems are analysed. While the definition of Johansson and Hassel can be applied to all kinds of systems Rocco et al. provide a formal definition of vulnerability specifically adapted for the analysis of networks. This definition is used here. They define robustness as "ability of a network to avoid malfunctioning when a fraction of its constituents is damaged due to random failures or intentional attacks." Vulnerability is then defined by Rocco et al. as the lack of robustness, i.e. as an inability of a system to avoid malfunction when a fraction of its components are removed (Rocco et al., 2012, p. 2556).

Resilience has been introduced within the system safety field as a counterweight to a perceived overemphasis on risk prevention (Comfort, 2010). It is founded on a critique against what is referred to as anticipation strategies. Anticipation strategies hinge on the idea that we can foretell what will happen and build defences. These anticipatory approaches are dominating work concerning protection of CIs (Bruijne & Van Eeten, 2007, p. 11). Wildavsky (1988) argues that the draw-back in relying on anticipation is that much resources are spent on specific defences, and he instead puts more emphasis on so called generalizable resources. While a specific defence, such as a flood protection system, will only be of use if a flood occurs generalizable resources can be of use in a large number of foreseeable and unforeseeable hazard events. Generalizable resources may include organizational capacity, knowledge, wealth, energy and communication. Resilience should not be considered the single solution but rather as a useful complement to anticipation, and the question is how to strike the right balance between these two strategies (De Bruijne & Van

Eeten). Wildavsky argues that anticipation, as opposed to resilience strategies, will be preferable in situations where we know what can happen and also how to manage what can happen. If either of these two kinds of knowledge is lacking we should rely more on resilience and less on anticipation and if both forms of knowledge are lacking we will have to completely rely on resilience. Wildavsky suggests that the high pace of technological as well as societal change in the modern society reduces our ability to foretell what can happen and how this can be managed, thus making resilience a crucial strategy. McDaniels et al. (2008) provide a formal definition of resilience. A system is resilient if it is robust (suffers low loss of system function in the event of a disturbance), and/or can recover its functionality quickly after a disturbance. The latter ability is referred to as rapidity. Figure 2.1 illustrates the two dimensions of resilience mentioned by McDaniels et al.

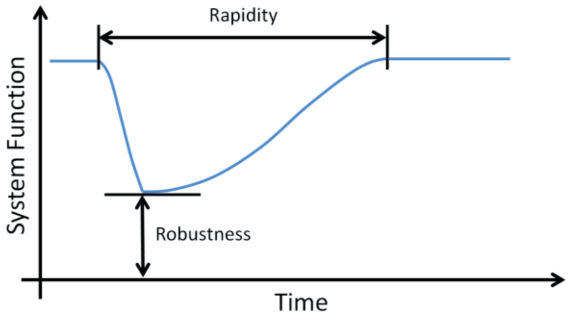


Figure 2.1: Resilience curve for a system affected by strain (Wilhelmsson & Johansson, 2009, p. 3).

Holmgren (2006) points out that there are two major approaches of CI protection corresponding to the two parts of the resilience concept, as defined by McDaniels et al. A system can be made more robust, i.e. it can be strengthened so that impact from disturbances is either avoided or reduced, or its rapidity can be improved, i.e. its capacity to recover after disturbance can be enhanced. The two definitions of resilience, that given by Wildavsky on the one hand and that given by McDaniels and Holmgren on the other hand, are not entirely coherent. Holmgren speaks of strengthening CIs or giving them capacity to recover. If by this is meant strength to withstand or recover from one particular hazard scenario the analysis that is done is definitely a form of anticipation strategy and thereby opposite of what Wildavsky refers to as a resilience strategy. If on the other hand, as is the case in this thesis, the analysis of strength of the network and its capacity to recover is not related to any particular hazard scenario the case is different. When this kind of analysis is performed an assessment is made of general resources that enable systems to withstand or recover from all forms of disruptions, rather than the systems defences against particular hazards. To assess the amount of general resources of the system is to assess resilience in the sense in which Wildavsky understands this word.

## 2.4 Network theory

The simulation method that has been used in the research work for analysing component failure scenarios in electric distribution networks is based on Network theory, and a presentation of this theory is therefore required. Network theory was first developed in the 18th century by Euler. A network, or graph, G(V,E) is defined by two sets, V consisting of the N nodes and E consisting of the M edges (or links), defined as (Johansson, 2010):

$$V = [\, n_1 \quad n_2 \quad \dots \quad n_N]$$

$$E = [\, e_1 \quad e_2 \quad \dots \quad e_M \,]$$

The complete set of components in the network $C$ is constituted by the sets $V$and $E$, i.e.:

$$C = [\, n_1 \quad n_2 \quad \dots \quad n_N \quad e_1 \quad e_2 \quad \dots \quad e_M \,]$$

$$= [\, c_1 \quad c_2 \quad \dots \quad c_{N+M} \,]$$

An adjacency matrix A can be used to represent the connections in the network:

$$A = \begin{pmatrix} a_{11} & \cdots & a_{1N} \\ \vdots & \ddots & \vdots \\ a_{N1} & \cdots & a_{NN} \end{pmatrix}$$

Where $a_{ij}$ is 1 if $n_i$ is connected to $n_j$ by means of an edge and 0 if no connection exists. When analysing electricity distribution systems two kinds of node failures can occur. One kind consists in the node becoming unable to transfer electricity through the network. If such a failure occurs in node $n_i$ this is simulated by setting all elements in row $i$ and column $i$ of the adjacency matrix $A$ to 0. The second kind of node failure consists in the node becoming unable to supply electricity to the customers connected to it while still being able to supply electricity through the network. In this case the connectivity of the network is unchanged but all customers connected to the node are left unsupplied. Finally, a failure of edge $e_i$connecting $n_j$ and $n_k$ is simulated by setting $a_{\mathrm{kj}}$ and $a_{\mathrm{jk}}$ to 0.

The main advantage as well as drawback of using network theory is that this approach abstracts away all except the most fundamental of the systems properties. This can be an advantage considering that the computational burden of simulating the system is thereby decreased while it can be a draw-back if a more detailed system description is desirable. In the research presented in this thesis decreasing the computational burden of simulations is valuable since it makes it possible to simulate large numbers of failure scenarios. Network theory can also be used to analyse the performance of the network when exposed to strain. Strain in this thesis means that one or several components in the network fails, i.e. become unable to deliver, transmit or receive electricity. In order to get an overview of the vulnerability of the network ideally all possible strain scenarios should be tested. This can be done by means of a strain vector containing all possible component failure combinations for a certain level of strain. For network strain of one and two components the strain vectors ($SV_1$ and $SV_2$) are defined as follows:

$$SV_1 = \begin{matrix} c_1 \\ c_2 \\ \vdots \\ c_{M+N-1} \\ c_{M+N} \end{matrix}$$

$$SV_2 = \begin{matrix} c_1 & c_2 \\ c_1 & c_3 \\ \vdots & \vdots \\ c_{M+N-2} & c_{M+N} \\ c_{M+N-1} & c_{M+N} \end{matrix}$$

If the simulated network is large, as is the case with the distribution system studied in this thesis, complete scenario vectors such as those shown above will however not be possible for higher levels of strain due to a combinatorial explosion that quickly creates unmanageable simulation times. If components are disrupted the number of possible failure scenarios is given by the following formula:

$$\frac{\prod_{i=1}^{x}(M+N-i+1)}{x!}$$

When running the simulation tool that is used in Chapter 5, developed in Matlab®, on a lap-top computer[3] applied to the distribution network one scenario requires 15 ms of simulation time. If using complete scenario vectors this would give the simulation times shown in Table 2.1. The quick escalation of simulation time with strain size is clearly illustrated.

Table 2.1: Simulation time as function of strain size

| Strain size | Simulation time |
|---|---|
| 1 | 18 seconds |
| 2 | 3 hours |
| 3 | 50 days |
| 4 | 41 years |
| 5 | 10 millennia |

In order to be able to investigate scenarios with higher strain size sampled scenarios are used. The sampled scenario vector has the following form:

$$SV_{N-x} = \begin{matrix} c_{r1} & \cdots & c_{rx} \\ \vdots & \ddots & \vdots \\ c_{r1} & \cdots & c_{rx} \end{matrix}$$

[3] Intel® Core™ i5-460M Processor with 2 cores, clock speed 2.53 GHz and 8 GB memory.

Where $c_{ri}$ denotes the $i$:th component randomly chosen among the set of still functioning components. In order to assure that the result is valid the number of sampled scenarios should be sufficiently large.

# Chapter 3

# Electrical distribution systems

In the last chapter concepts were introduced that are of fundamental importance for the research presented in this thesis. In this chapter a presentation is given of the system that is studied in the thesis, the electricity distribution system. An overview is first provided of the Swedish power system. This is done in order to describe the context of the distribution system. This is then followed by a description of power system regulations in Sweden. These regulations are of interest here since two of them are used in the research concerning assessments of consequences from power outages presented in Chapter 5. Finally power system restoration is discussed. This is of interest here since the research presented in Chapter 6 concerns simulation of power system restoration processes.

## 3.1 Overview

The Swedish power system, as well as power systems in other parts of the world, is traditionally divided into three main parts: generation, transmission and distribution (Figure 3.1). In the generation subsystem primary sources of energy are converted to electrical energy in one or more steps typically involving turbines and synchronous generators. The voltage is then raised to the level which is used in the transmission system by means of a step-up transformer. The transmission system is divided into two parts, the extra high-voltage (EHV) system, with a voltage level higher than 300 kV, and the high-voltage (HV) system with a voltage level ranging from 36 to 300 kV (Lakervi & Holmes, 1995, p. 10). The reason for using EHV and HV systems is that, for a given power, higher voltage gives lower current and thereby reduces power losses, that are proportional to the current squared. Because of these systems electrical power can be distributed across countries and even continents. The Swedish distribution system is subdivided into the medium voltage (MV) system, with a voltage level ranging from 1 to 36 kV, and the low voltage (LV) system with a voltage below 1 kV. Today Sweden has approximately 170 network operators, each having a monopoly within a certain geographical region (Ei, 2014). As is indicated in Figure 3.1 the part of the overall power system that is studied in this thesis stretches from the transformer supplying the medium voltage system to the transformer supplied by the medium voltage system.

## 3.2 Power system regulations in Sweden

While the electric energy market is entirely open, the electricity distribution market in Sweden is a natural monopoly. The reason for this is that it is considered a waste of resources to build parallel power grids, owned by competing network operators (El-Gharbawi et al., 2011). Since competition on a free market can therefore not be relied upon as a means to achieve high power quality and low vulnerability regulations are needed. Ajodhia & Hakvoort (2005) distinguish between three different kinds of regulatory instruments that can be used to promote better power quality: indirect instruments, standards and incentive schemes. Indirect instruments promote the goal of better power quality by strengthening the information and negotiation position of the consumers. Standards dictate a minimum acceptable level for one quality aspect or other. If the standard is violated the network operator is fined. Two main kinds of standards can be distinguished, those that concern the entire system and those that concern individual consumers. Finally, quality incentive schemes can be considered as more advanced standards. When a quality incentive scheme is used the fine, or possibly reward, given to the network operator is closely related to the quality delivered (Ajodhia & Hakvoort). Quality incentive schemes have been introduced in a number of countries.[4] The former is a two-sided instrument, since it rewards high quality as well as punishes low quality, while the latter is one-sided since it only punishes low quality (El-Gharbawi et al., 2011). In the following these two regulations as well as Styrel (Energimyndigheten, 2012), a Swedish regulation meant to reduce adverse consequences of outages, are briefly introduced.

[4] For a review of regulations in European countries see Tahvanainen et al. (2004), for a review of regulations in American states see Sappington et al. (2001).

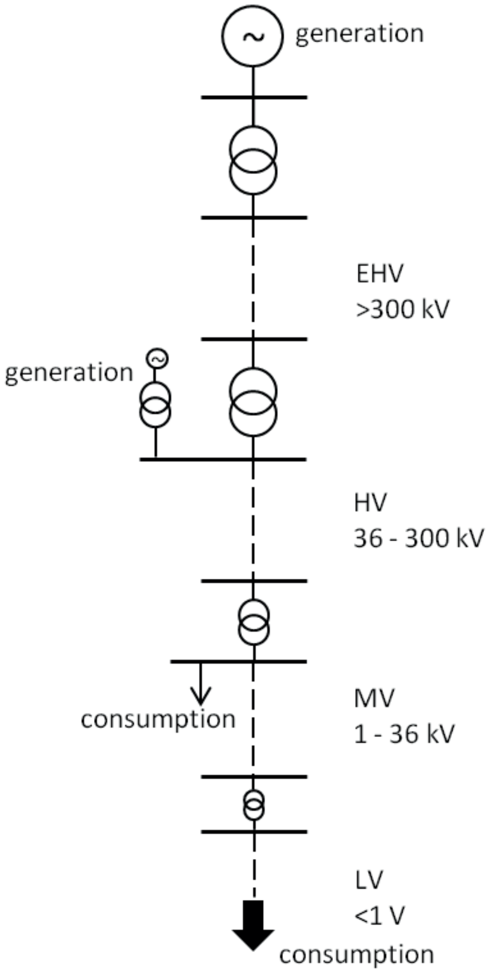


Figure 3.1: General schematic of the power system (Lakervi & Holmes, p. 10).

### Revenue frame

The Swedish Energy Markets Inspectorate (Ei) is responsible for the revenue frame for power quality regulation. The revenue frame is used to put a limit on how much the DSO can charge customers, in this way counteracting their monopolistic position on the market. The revenue frame is decided over a period of four years at a time. At present we are in the 2012-2015 period, in which a revenue frame has been decided individually for each of the approximately 170 network operators in Sweden. In order to estimate the appropriate revenue for each individual company, Ei assesses the costs of the company and the revenue frame is set so that these costs as well as a reasonable profit will be covered. Ei furthermore decides with what level of quality the company should supply its service during the four year period. In the present period the quality assessment is based on the reliability of the power supply. The electric quality of the electricity delivered, if it e.g. has variations in voltage magnitude or transients, is not considered. The reliability indices SAIDI and SAIFI are used to measure the reliability of the electricity supply, and they are calculated for all announced outages longer than 3 minutes as well as for unannounced outages between 3 minutes and 12 hours in length. Unannounced outages longer than 12 hours are not considered since the outage compensation regulation, described below, covers this category of outages and creates an incentive for the DSOs to avoid outages of this duration. During the present four year period the quality standard for the network operators is that they should not reduce their quality, i.e. increase SAIDI or SAIFI, relative to how they performed in the years before 2012. If a company performs below the quality standard the customer fees will be reduced accordingly, while the company will instead receive a benefit if it performs above the standard. The method for quality regulation is not yet fully developed. In the long term perspective the aim of the revenue frame is to achieve optimal power quality. This is achieved when the sum of the cost of customers due to outages and the cost of the DSO of preventing outages is minimized. In the future the regulation might also take power quality (for instance dips, flickers and transients) into account when determining supply quality (Ei, 2010; Ei, 2011; Ei, 2014).

### Outage compensation

While the revenue frame creates an incentive for the network operators to reduce the number of short unplanned power outages, as well as all planned outages, the outage compensation regulation instead creates an incentive for avoiding outages longer than 12 hours. The compensation increases with the outage time[5] (see Table 3.1) thereby motivating the network operators to improve the reliability of their systems so that long power outages will be less likely.

Table 3.1: Outage compensations for different power outage lengths

| Outage time (days) | Compens-ation (% of yearly fee) | Minimum compensation (SEK) |
|---|---|---|
| >0.5 | 12.5 | 900 |
| >1 | 37.5 | 1,800 |
| >2 | 62.5 | 2,700 |
| >3 | 87.5 | 3,600 |
| >4 | 112.5 | 4,500 |
| >5 | 137.5 | 5,400 |
| >6 | 162.5 | 6,300 |
| >7 | 187.5 | 7,200 |
| >8 | 212.5 | 8,100 |
| >9 | 237.5 | 9, 000 |
| >10 | 262.5 | 9,900 |
| >11 | 287.5 | 10,800 |
| >12 | 300 | 11,700 |

[5] www.energimarknadsbyran.se/El/Konsumentratt1/Klagoguide/Avbrottsersattning

### Styrel

The Swedish Energy agency has in cooperation with the Swedish Civil Contingencies Agency and Swedish national grid developed Styrel. It is meant to be used during times of power shortage at a national level to prioritize consumers based on their importance to society. Consumers are grouped into nine predefined priority classes and each consumer is also given a number of points (see Table 3.2). National, county and municipal levels are all involved in the process of deciding which power customers to prioritize. (Energimyndigheten, 2011, p. 15) In the municipality that has been studied in the research work (but not necessarily in other municipalities) the prioritizations of customers to supply in case of power shortages are made according to the following rules:

1. The overall number of non-supplied customers with priority 0 or 1 should be minimized

2. The sum of points for all non-supplied customers with priority 2 or less should be minimized

3. Rule 1. has precedence over rule 2.

Table 3.2 Consumer categories as defined in Styrel (The number of points given to customers is in most, but not all cases, in accordance with below)

| Priority class | Point | Power customer |
|---|---|---|
| 0 | 8 | Critical facilities belonging to the power company |
| 1 | 8 | Consumers that in a short time span (hours) have a large impact on life and health |
| 2 | 7 | Consumers that in a short time span (hours) have a large impact on the functioning of society |
| 3 | 6 | Consumers that in a longer time span (days) have a large impact on life and health |
| 4 | 5 | Consumers that in a longer time span (days) have a large impact on the functioning of society |
| 5 | 4 | Consumers that represents large economic values |
| 6 | 3 | Consumers that have a major importance for the environment |
| 7 | 2 | Consumers that have importance for societal and cultural values |
| 8 | 1 | Other consumers |

## 3.3 Power system restoration

Power System Restoration (PSR) is the process by which power is restored to customers following an outage. In some cases this may be done quickly by switching connections in the network, in other cases it will be much more cumbersome and physical repair work will be required to bring power back to all customers. Oftentimes restoration of the distribution network does not involve repair work of any kind. This is the case when a power line in the distribution system trips due to overloading. The circuit-breaker feeding the line then opens (Bertoli et al., 2003). However, since the distribution system is operated radially during normal conditions the entire area that was supplied by the power line is left without power. PSR, in this case, consists in changing the configuration of the network by opening and closing breakers so as to resupply a maximum of non-faulty lines on the lost areas (Bertoli et al., 2003). Restoration activities might also be caused by component damages and in this case physical repair work is required in order for power to be restored to customers. Shinozuka et al. (1998) discuss power system restoration, in the distribution grid as well as at higher voltage levels, following earth quakes. They conclude that the restoration process proceeds non-linearly, i.e. most customers get their power restored quickly and proportionally fewer customers are restored as time elapses.

## 3.4 Summary

The power system, in Sweden and elsewhere, can traditionally be divided into three main parts: generation, transmission and distribution. The system studied in this thesis belongs to the last mentioned. It can also be concluded that the power distribution market, due to being a natural monopoly, is in need of regulations and that three main kinds of regulations can be distinguished: indirect instruments, standards and incentive schemes. Two Swedish incentive schemes, the revenue frame and outage compensation, were described in more detail as well as the Styrel system. This has given background to the research work presented in Chapter 5 where the outage compensation scheme and the Styrel system are made use of to assess consequences from power outages. Concerning power system restoration it can be concluded that restoration can in some cases be achieved merely through switching of breaker positions in the power network, whereas in other cases repair work on damaged components will be required. This has provided some background to the research presented in Chapter 6 where restoration processes in a power distribution system are studied.

# Chapter 4

# Review of socio-technical system models

In the previous chapter the power system, part of which is studied in this thesis, was in focus. In this chapter it is method that will be our concern. The hypothesis underlying the research presented in this thesis is that it could prove highly rewarding to analyse CIs as STSs. In order to enable an analysis of this kind approaches for simulating STSs are reviewed in this chapter. Seven categories of modeling approaches are identified and each is briefly presented. The ability of each approach to meet three requirements specified by the author, related to vulnerability analysis of CIs, is discussed.

Several researchers claim that new methods are needed in order to grapple with CIs and their vulnerabilities (Rasmussen, 1997; Leveson, 2004; Hansman et al., 2006; Qureshi, 2007). One of the recurring statements is that CIs must be analysed in a more holistic way, not delimiting the analysis to only technical or organizational aspects. The analysis of CIs should, according to these researchers, take into account that CIs are STSs, systems encompassing technical as well as organizational parts. In order to get an understanding of modeling and simulation of STSs, a review is here presented of the literature within the field. Based on the reviewed material a suggestion is made of combining two of the identified modeling approaches. A model similar to the suggested one is used in the research work presented in Chapter 6.

## 4.1 Method for selecting papers to review

Relevant research literature was searched for using two databases, Engineering village (EV) and Google Scholar (GS). A structured search was performed in EV giving a total of 111 papers for the following search query:

“socio-technical system*”

AND “computer model*”

AND (“vulnerability”

OR “risk”

OR “infrastructure*”

OR “interdependen*”)

In Google Scholar (GS), it seems that structured search approaches, as used in EV, is not possible. A less structured search was therefore used. The search terms used were “socio-technical systems” in various combinations with the other terms listed above, giving in total roughly 500 papers. A primary selection was performed based on title and/or content of abstract for the papers from the two databases, which gave 20 and roughly 50 papers from EV and GS respectively. A second selection was based on the content of the paper giving a total number of 13 and 22 papers from EV and GS respectively. Eight papers were found in both databases, giving a total of 27 papers.

In a third step the references of the papers that passed the second selection were screened with the same selection process as above, adding 2 new papers to the review. The papers, 29 in total, finally included in the review were categorized according to the modelling approach used. Seven modelling approaches were identified, see Table 4.1.

Table 4.1: Categories of STS modeling approaches identified in the review and number of papers in each category.

| Modelling category | No. Papers |
|---|---|
| Agent based | 11 |
| Bayesian belief network | 3 |
| Hybrid | 5 |
| Network theoretical | 7 |
| Petri-net | 1 |
| SHELL | 1 |
| System dynamics | 1 |
| Total | 29 |

Three identified approaches were evaluated concerning their usefulness for analysing three issues which are crucial for risk and vulnerability analysis of CIs:

a) socio-technical factors as a cause of critical infrastructure disruptions;

b) restoration processes concerning critical infrastructure and;

c) societal consequences from infrastructure disruptions.

In the following each of the identified approaches is briefly presented as well as the research work that have been made based on the approaches. It is also discussed how useful the seven identified approaches are for simultaneously simulating aspects a), b) and c).

## 4.2 STS modelling approaches

In this section, for each of the seven identified approaches, a general introduction is provided in an initial paragraph, followed by a paragraph presenting the papers in which the approach was used and a final paragraph briefly discussing the applicability of the approach for simultaneously simulating the three aspects specified above.

**Network theoretical models**

Network theory is here briefly presented, (for a more thorough introduction to network theory models see section 2.4). Networks consist of only two kinds of components, nodes and links. Nevertheless they have proved useful for describing and analysing a wide range of different systems, such as complexes of interacting molecules (e.g. Shannon et al. 2003, Bader et al. 2003) and critical infrastructures (e.g. Walski et al. 1987, Crucitti et al. 2005). Many NTMs have also moved beyond merely analysing network topology and are including more physical system aspects into the model.

Johansson et al. (2007) have developed a socio-technical model inspired by the network theoretical approach and traditional engineering approaches. The model allows them to estimate societal impact caused by disruption of critical infrastructures. In the model each network node is assigned a certain societal importance, which is measured in "customer equivalents", and it hence demonstrates a possible way to incorporate societal consequence into the analysis of technical systems. Wilhelmsson & Johansson (2009) and Johansson et al. (2011) have also addressed the issue of system interdependencies and restoration processes concerning an interdependent railway infrastructure. Bird et al. (2009) and Ducheneaut (2005) have developed NTMs for analysing socio-technical IT systems. In the models two kinds of entities are differentiated: software components and software developers. Networks are constructed where software and programmers constitute nodes and the relationships between these are represented as links. Pestov & Varga (2009) use a NTM to analyse vulnerability of interdependent critical infrastructures. In their model many individual infrastructure networks are joined into one overall "metanetwork". In this way they analyse a fictitious example of a prison break in which police, fire department, telecom and water utility are involved. Several interdependencies between the CIs are included in the model. For instance the telecom network depends on cooling which is dependent on the water system and the fire brigade depends on both the previous CIs. Using the network model they are able to show how the network performance deteriorates over time. Ramaswamy et al. (2007) use a NTM to simulate the national telephone network in USA on a call-by-call resolution. User behaviour is captured in a realistic way by using census data.

What sets NTMs apart from other modelling approaches is that it abstracts away much of the complexity of the modelled system by representing it, to a large extent, as a collection of nodes and links, although some approaches also include more physical system properties. This simplification can, depending on the research question, be either an advantage or a disadvantage. NTMs have clear advantages within the field of critical infrastructure research first of all since CIs are generally based on physical networks and they therefore lend themselves well to being modeled as networks. The NTM also abstract away much details of the system thereby enabling simulation of a large number of system states. This abstraction can be an advantage or a disadvantage depending on the aim of the research in question. A further question is if the NTM approach will be useful in order to model not only technical aspects of the critical infrastructures but societal ones as well. Johansson et al. (2007) have shown that it is possible to include the societal consequences of infrastructure breakdown in a NTM context where the nodes are given different weights in accordance with their societal importance. Similarly they have shown that restoration times can be accounted for in the NTM modelling environment. Furthermore, Bird et al. (2009) and Ducheneaut (2005) have proved the feasibility, at least within the field of software development, of using socio-technical hybrid networks, in which social and technical components are represented side by side.

**Bayesian belief network models**

Bayesian belief network (BBN) models are, like NTMs, made up of nodes and links, but while the nodes in NTMs represent entities of some kind and the links represent relationships between the entities, BBN nodes instead represent events and the links represent the likelihood that one event, the child node, is true given that another event, the parent node, is true. BBNs can in this way be used to infer the probability of one event from knowledge of other events. This inference is made possible by Bayes's theorem, which in the $18^{th}$ century was suggested by Thomas Bayes as useful for updating beliefs.

Gregoriades et al. (2003) use BBN to assess the level of human reliability in a combat subsystem of a naval offshore patrol vessel. They compare the performance of two different system set-ups, one in which semi-automated equipment is used and one in which the equipment is fully automated and find that the latter system is more reliable. Greenberg & Cook (2006) use

BBNs to analyse low probability high consequence (LPHC) events. The main idea that they put forward is that social entities are the primary reason behind this kind of events. This claim is supported by the fact that 60-90% of LPHC events can be attributed to human operators either as a contributing factor or as a root cause. They have analysed two different kinds of systems using a BBN approach, exemplifying possible uses: a transportation company encompassing a number of individual drivers and operators controlling large industrial facilities. Léger et al. (2009) in their modelling approach distinguish between three different system levels, the technical, the level of the operator and the organizational level. The first level is controlled by the second and the second by the third. They use BBN to integrate the different levels in one single model. In addition to the three system levels they also identify two contextual levels, organizational and natural environment. The bow-tie method, which essentially consists in integrating a fault tree and an event tree, is used to study failures in the technical system.

The main advantage of the BBN approach seems to be modelling of systems that can be described in terms of a fairly small number of states or events which are correlated in a known way. The systems analysed by Gregoriades et al. (2003) and Greenberg & Cook (2006), a military patrol vessel, driver systems and operators in industrial facilities, do indeed fit this description. The BBN approach could be useful for detailed modeling of some essential parts of infrastructure systems. One such part is the organization directing the restoration process after a disruption. A model that could take account of the work going on within such an organization would in many respects be similar to the model developed by Gregoriades et al.

**Petri-net models**

Petri-net (PN) models were introduced by the German mathematician Carl Adam Petri in 1962 (Olsson & Rosen, 2005, p. 211). PN models have been used extensively in computer and automatic control research and can be of use for modeling a wide variety of different systems. PN models have two basic constituents: places represented as circles, connected to each other as inputs and outputs, and transitions represented as bars. When the model is run tokens are passed to output places in case all its input places have at least one token (David & Alla 2005). In an industrial automation application (see Figure 4.1) places could represent availability of a component, availability of a robot and availability of a machine. In case these three places all have a token, indicating that a component, robot and machine is available, their common output places will receive a token, i.e. tools will be loaded on machine.

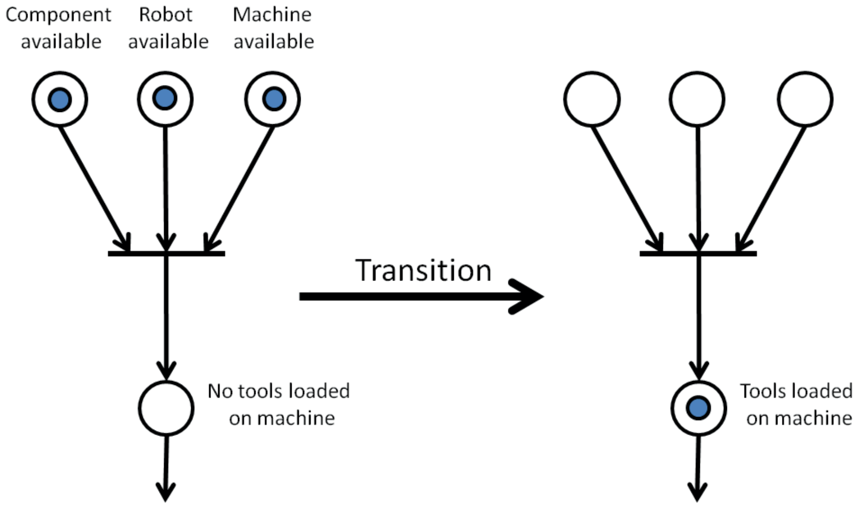


Figure 4.1: Petri-net applied in industrial automation (Olsson & Rosen, 2005, p. 212).

Basnyat et al. (2007) use PN to model socio-technical barriers, i.e. barriers that can encompass hardware, software as well as human elements. A hazard barrier target (HBT) model provides a context for the PN models. The approach is used to analyse a system for transportation of fuel to a kiln in a cement production facility and make use of data from a prior fatal mining accident. Barrier models include operators responsible for making technological equipment operational. Their model parameters are based on the accident report as well as on manufacturer data.

PN models are versatile, and can favourably be used in circumstances where several processes that make use of common resources are going on in parallel and concurrently (David & Alla, 2005). STSs in general meet these criteria. Basnyat et al. (2007) use PN to model barriers within industrial facilities. In a critical infrastructure context socio-technical barriers protecting facilities such as power stations and water plants are essential, and a model similar to that of Basnyat et al. could therefore be of great value. They are furthermore able to analyse system safety by simultaneously taking account of the overall view of the system and looking in detail at socio-technical safety barriers within the system. Concerning the analysis of critical infrastructures, system level models will most likely have to be combined with models that provide insight into the workings of certain system parts.

**System dynamics models**

System dynamics (SD) models include stocks, i.e. amounts of different kinds of things, connected by means of three basic relationships: delays, positive-, and negative feedback loops. The main benefit of SD models lies in their ability to take account of the highly non-linear behaviour that characterizes many real world systems. SD modelling was developed during the 1950s by Forrester. The attempt was to provide tools for management of companies which would be similar to those used by engineers and natural scientist. SD has been applied to fields such as urban planning and national economics (Forrester et al., 1976; Han et al., 2009). The modelling approach has also been used to predict the future development of the entire socio-economic world system (Meadows et al., 2004).

Leveson (2004) has developed the STAMP (System-Theoretic Accident Model and Processes) and the STPA (STAMP based hazard analysis) models which are based on SD. The models are capable of analysing so called system failures that emerge from the interaction of technical and societal system components. There are two basic aspects of the model: 1) hierarchy which describes the relationship between the higher (controlling) and lower (controlled) parts of a socio-technical system and 2) process which describes in what way control is performed between the different levels. Leveson has used the STPA model to, for example, analyse an anti-collision system used in aircrafts and a Canadian public water system.

System failures, failures which are not caused by the malfunction of any particular system component but rather derive from the inappropriate interaction among system components, are likely to be of major importance in a critical infrastructure modeling context. Leveson's STAMP and STPA models are designed especially to enable analysis of system failures and they could therefore be useful in a critical infrastructure modeling context. An advantage of the SD approach is its ability to take organizational aspects into account. Such organizational aspects of an infrastructure are of importance during normal operation and even more important in a major crisis situation, where it might even be necessary to include governmental institutions in the crisis management process. The approach does not seem to be able to simulate the behaviour of individual parts of a CI and their relationships, or the individual behaviours of repair workers responsible for restoration of CIs. If simulation of CI failure events and the restoration from such failure events is to be based on information concerning the component parts SD will not be a suitable approach. This is a major drawback since data concerning component parts is more readily obtainable than system level dynamics, which is what SD is built around. An approach that could, based on component level data, derive system level dynamics is more promising as a means for gaining insight in CI failure events and CI restoration.

**Agent based models**

Agent based models (ABMs) are rooted in the work on cellular machines that was done by John von Neumann during the 1940s. The agent, that is at the core of every ABM, can be characterized as autonomous, interdependent, acting according to simple rules, and adaptive. One commonly testified advantage of the approach (e.g. Smith et al., 2007; Bonabeau, 2002) is its ability to generate emergent behaviour, a phenomenon that can be described with the words of Epstein (2006, p. 21): “We get macro-surprises despite complete micro-level knowledge”. The kinds of situations that are preferably analysed by means of ABM are those that lack central coordination as well as an overall fixed structure.

ABM is the approach that was applied most frequently in the reviewed papers. While being grounded in the same fundamental principles, the different models varied considerably concerning what features of the ABM approach that were highlighted. Ferscha et al. (2011), Zia et al. (2010, 2011) and Sharpanskykh (2009, 2011) analyse behaviour of crowds during emergency situations. In order to do this, the psychological characteristics of the agents are rendered in great detail, including intentions and emotions as well as personality among the agent characteristics.

They use the modelling approach to simulate evacuations from railway station during bombing situations. While the agents modelled by Ferscha et al., Zia et al. and Sharpanskykh are psychologically refined, Joslyn (1999, 2000) instead develops the ability of the agents to perform symbolic manipulations. By endowing the agents with the ability to create, communicate and interpret signs and symbols they are in effect made able to ”talk” to each other. These so called semiotic agents are achieved by going halfway between traditional ABM on the one hand and artificial intelligence on the other. Joslyns approach is intended to deal with Socio Technical Organizations (STOs) in general but the STOs in focus are “911” organizations, search and rescue teams and military organizations. While the previously mentioned papers are elaborating the individual characteristics of the agents Barrett et al. (2004) have developed models that can render the collective action of large agent populations. In their transport system model, TRANSIM, they are able to model entire cities and their populations. Such a model has been created for Portland, Oregon, USA. Apart from TRANSIM they have STS modelling programs using the ABM approach that are capable of simulating the spreading of diseases and the behaviour of markets. In the ABMs mentioned so far the emphasis lies decidedly on the social side of the system. In the work of Shah & Pritchett (2005) and Lee et al. (2007) technical and societal system aspects are however equally well developed. They have created an ABM of Air Traffic Management (ATM) systems. It is suggested when designing socio-technical systems, one should be able to manipulate design variables in agents as well as in their environment. Lee et al. suggest that “in simulating ATM systems by agent-based simulations, the overall behaviour of the systems can be considered as emergent phenomena” (Lee et al., 2007, p. 2). They provide the following definition of emergent phenomenon: “A system property in which system behaviours at a higher level of abstraction are caused by behaviours at a lower level of abstraction which could not be predicted, or explained, at that lower level. (Ibid.)“ Lee et al perform a case study on an ATM system of Los Angeles International Airport. Here they compare two different safety strategies and investigates which of the strategies that leads to fewer violations of safety distances.

One of the claims that are recurring in the reviewed papers using ABM is its superior ability to provide insight into emergent phenomena. It is also claimed to be specifically well suited for modelling systems that are not centrally controlled, but are rather impacted by the decisions of a multitude of uncoordinated choices being made by unrelated actors. Some critical infrastructures, such as road transportation, at least partially fulfil these criteria and ABM therefore seems to be a promising approach for modelling these systems. The ABM approach of Shah & Pritchett (2005) and Lee et al. (2008) seems to be the approach that is most suitable for modelling disruptions and restoration processes in a critical infrastructure context. They have achieved a well integrated STS model that takes equal account of technological and social system aspects when analysing how different behavioural rules of the agents or availability of resources affect the probability of goal attainment in the system at large. This would most likely be of interest also as concerns restoration processes performed in a wide range of critical infrastructures. In the work that has been done by Wilhelmsson & Johansson (2009) restoration times were obtained through interviews with experts from the infrastructure owner. One thing that was found in the study was that the restoration time increases non-linearly as the level of strain on the system increases. Since ABMs have the ability to model non-linear systems where emergent phenomena occurs, it should be of interest to apply it to the issue investigated by Wilhelmsson & Johansson.

**SHELL models**

SHELL is an abbreviation where L stands for liveware (meaning a human operator), H for hardware, S for software and E for environment. The additional L is included to emphasize the importance of operator-operator interaction.SHELL is a conceptual model for analysing human factors in aviation systems. It was initially created by Edwards in 1972 (Wiener & Nagel, 1988) and was further developed by Hawkins.

Cacciabue et al. (2003) use object oriented programming to run computer simulations based on the SHELL model structure. They analyse the task performance of aviation maintenance technicians and are able to show in what way the value of a large number of performance influencing factors (such as fatigue, motivation, stress of the operators) changes during the performance of a maintenance task.

As is stated by Cacciabue et al. (2003) the SHELL model is very generic and it should therefore be possible to implement it in contexts other than aviation systems. It could be a fruitful approach when modeling task performance of critical infrastructure repair workers during a CI restoration process. The main drawback of the approach is its level of detail. Each single operator as well as its interactions with the environment is represented individually and with such a level of detail that full scale CI restoration processes where tens if not hundreds of repair workers can be involved would prove too computationally demanding.

**Hybrid models**

Hybrid models (HMs) make use of two or more different modelling approaches and unite them in the context of one single modelling environment. HMs thereby makes it possible to combine the advantages of several modelling approaches.

Nikolic & Gerard (2006) have developed the Action-Oriented Ecology Framework using ABM, NTM, game theory, and artificial intelligence to look at industrial ecologies. They claim that any large scale STSs can be represented through their framework. Artificial intelligence is used to model in what way agents learn, game theory in what way they choose to act and NTM is useful to describe in what way agents will interact with each other and what relationships they will form. Using the approach they have analysed a number of suggestions for the future development of two industrial areas. Mohaghegh and colleagues (Mohaghegh et al., 2009; Mohaghegh, 2010) have developed SoTeRiA (Socio Technical Risk Analysis), a hybrid model consisting of three different models: a BBN model, a Probabilistic Risk Assessment model for technical systems and a SD model. The SD model is used to integrate the two other models. They use the approach to analyse safety within the aviation domain and to predict management's commitment to safety as well as the probability of errors made by the technicians over a period of 15 years. Lu et al. (2012) have used Mohagheghs et al. SoTeRiA model to analyse a subway system. Brandt et al. (1999) have developed the Human-Integrated Petri-net Simulation (HPS) which combines Human Integrated Simulation (HIS) and PN simulation. They use the modelling approach to analyse intermodal traffic. The HIS is used to simulate human cooperation between three involved operators and in parallel the PN is used to simulate movements of wagons, containers and cranes.

The general advantage of HM is that it enables the strengths of different modeling approaches to be combined. This could be useful when modeling critical infrastructures, since these systems are extremely heterogeneous as concerns their components and the system levels they encompass. It is unlikely that any single modeling approach will be optimal for modeling all the components and levels of a critical infrastructure and a HM approach could therefore be advantageous, maybe even necessary. Mohaghegh et al. (2009) and Mohaghegh (2010) have shown that a HM including SD models can be used to provide long term predictions of commitment to safety. This modeling approach could be of use for analysing the probability that critical infrastructures are disrupted as well as their ability to get restored after disruption. The likelihood of operator error and the ability of the people working with restoring the system to do their job are surely dependent on the commitment of the management to safety issues. Lu et al. (2012) used Mohagheghs et al. modeling approach to analyse risks in subway systems, exemplifying its applicability for other critical infrastructures than the airline industry. The main drawback of using hybrid models is that they can become to computationally demanding. When several sub-models are run in parallel this naturally creates extra demands concerning computer power.

## 4.3 A STS-model meeting the requirements

The aim of the review is to identify STS models that are able to simultaneously simulate a) socio-technical factors as a cause of critical infrastructure disruptions b) restoration processes concerning critical infrastructure and c) societal consequences from infrastructure disruptions. It has been found that several papers cover aspect a) Gregoriades et al. 2003, Lee et al. 2007, Léger et al. 2009, Lu et al. 2012, Greenerg & Cook 2006, Shah & Pritchett 2006, Pestov & Verga 2009, Cacciabue 2003, Leveson 2004, Basnyat et al. 2007, Mohaghegh et al. 2009, Mohaghegh 2010, some cover aspect b) Wilhelmsson & Johansson 2009, Johansson et al. 2011, and some cover aspect c) Ramaswamy et al. 2007, Barrett 2004, Johansson et al. 2007, Sharpanskykh 2009, Zia et al. 2010, Zia et al. 2011, Ferscha et al. 2011, Sharpanskykh 2011. Some papers also cover none of the three aspects, Bird et al. 2009, Brandt et al. 1999, Ducheneaut 2005, Joslyn & Rocha 2000, Nicolic & Dijkema 2006, Tsvetovat & Carley 2004. In Table 4.2 it is shown which modelling approaches that have been used to address the three issues of relevance for risk and vulnerability analysis of CIs. None of the approaches however simultaneously cover all aspects within one single modelling approach.

Table 4.2: Table showing which modelling approaches that have been used to analyse the three aspects crucial for risk analysis of CIs.

| Application in paper | N.o. papers | ABM | NTM | Hybrid | BBN | SD | PN | SHELL |
|---|---|---|---|---|---|---|---|---|
| Socio-technical disruption factors | 12 | X | X | X | X | X | | X |
| Infrastructure restoration | 2 | | X | | | | | |
| Societal consequence | 8 | X | X | | | | | |

In the following suggestions are given concerning how a model can be obtained that meets the three requirements. A hybrid model, including both NTM and ABM approaches, could be advantageous since critical infrastructures, from a socio-technical point of view, are both complex and in some parts emergent. The NTM approach is well-suited to model complex systems consisting of a vast number of interconnected parts. This is for instance illustrated by the work performed by Ramaswamy et al. (2007) who simulate the entire telephone network of the US with a network model. The ABM approach on the other hand makes it possible to model emergent phenomena. This is argued with particular force by Sha & Pritchett (2006) and Lee et al. (2007). BBN can be of use for gaining deeper insights about certain highly critical parts of infrastructures or society. PN models can provide understanding of socio-technical barriers used for protecting facilities within the critical infrastructures. SHELL models can be useful to model task performance of operators. SD on the other hand can be used to model higher level decision structures as well as more long term dynamics of the systems. A hybrid modelling approach, centring around the NTM and ABM approaches, and perhaps using BBN, PN and SHELL for describing lower level, and SD for describing higher level systems could be well suited for simulating the specified aspects of critical infrastructures, see Figure 4.2.

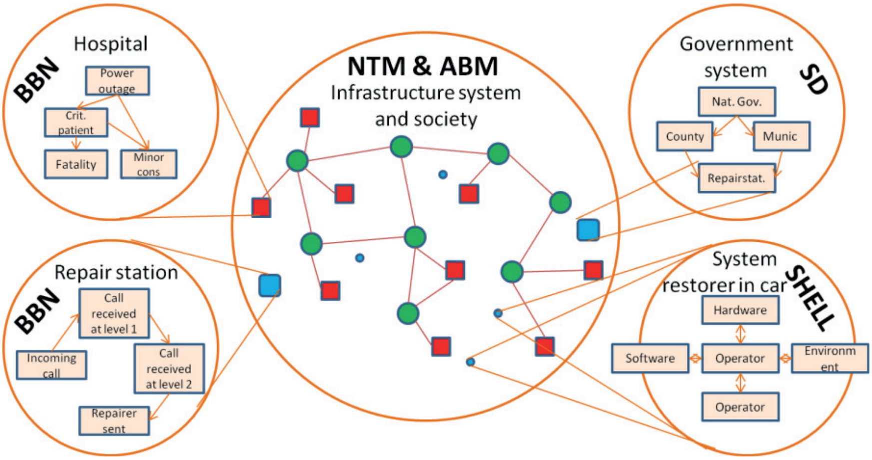


Figure 4.2: Architecture of hybrid model drawing on various STS modelling approaches.

There may very well exist papers that are relevant to the present review but that have been missed in the search process. The reason might be that they use different terminologies, that they are not present within the databases used or that they have been overlooked in the screening-process due to misleading/misinterpreted titles and/or abstracts. This should be considered with respect to the conclusions drawn.

## 4.4 Summary

Seven approaches for simulating STSs have been identified in the research literature. It was also found that none of the papers identified in the review have been used to address the three issues of simulating a) socio-technical factors as a cause of critical infrastructure disruptions b) restoration processes concerning critical infrastructure and c) societal consequences from infrastructure disruptions. It is finally concluded that a hybrid model centred around ABM and NTM but perhaps also drawing on BBN, PN and SHELL for representing lower level systems and SD for representing higher level systems is a good candidate for meeting the three requirements. The insights gained in the review presented in this chapter have been of use in the work presented in the two coming chapters. In

Chapter 5 a socio-technical NTM, describing an infrastructure network as well as the customers served by the network, is used to analyse consequences from power outages. In Chapter 6 a hybrid model, built around NTM as well as ABM, is used to analyse restoration processes.

# Chapter 5

# Quantifying societal consequences of power outages

In the previous chapter approaches for modeling STSs were introduced. In this chapter an STS perspective is applied to a particular part of a CI in order to gain insights concerning societal consequences from disruptions in CI networks. Here there clearly is an interplay of technical and societal system aspects that together come to determine the outcome and it should therefore be important that both these aspects are taken into account. A case study is performed on an electrical distribution system and the societal consequences from the simulated failure scenarios are estimated using two different measures, each based on one electricity regulation in use in Sweden. The result obtained using the two measures are compared and the differences found are discussed.

When RVAs are performed we seek to assess some adverse outcome. Such outcomes can be economic, or concern health and safety. Common for adverse outcomes is that they generally occur within society, rather than in the technical system that might be the initial root of the consequences. In other words, in order to assess the adverse outcomes of CI disruptions, it is not enough to analyse the technical infrastructure system itself, it must also be made clear what the societal consequences would be if CI services stopped. Much depends upon how we assess consequences of CI functionality loss. In which order should, for instance, power be brought back to customers following an outage, in order for the societal consequences to be minimized? A typical electric utility in the US will restore service to its customers in the following order: a) life and safety-related (e.g. hospital, police and fire facilities), b) emergency communications (e.g. 911 facilities), c) other critical facilities (e.g. water and wastewater facilities), then d) major feeders where the largest number of customers can be brought back at once (Mili et al., 2004). This ordering might seem commonsensical. However, as pointed out by Mili et al, relationships between societal resources and CIs are complex and to determine whether the consequences of disconnecting a customer will be deadly or harmless is not necessarily easy. Total consequences of power outages are difficult to determine mainly because consequences of CI disruptions cascade through social and economic systems and that they potentially can extend far beyond the directly affected customer in both time and geographic area. As yet little has been done within this field, as pointed out by Mili et al. ”there is virtually no unified theory to guide risk management based on realistic estimates of both the direct and indirect costs of power system outages” (Mili et al., 2004, p. 1). In the following two possible ways of measuring societal consequences from power outages will be compared.

## 5.1 Assessing societal consequence

Several factors influence costs of power outages, making it difficult to make precise assessments. Among the influencing factors are: timing (season and time-of-day), advance notice, frequency, duration and severity (Woo & Pupp, 1994). Not only the influencing factors but also the consequences of outages are of several kinds. Linares and Rey (2012) suggest that the consequences can be classified into three categories:

1. direct economic impacts;
2. indirect economic impacts;
3. social impacts.

They claim that an optimal analysis should capture all three impact categories. Some regulations in place in Europe and America (Tahvanainen et al., 2004, Sappington et al., 2001) do take explicit account of the first of these categories. The second and third categories are however not explicitly taken into account. Linares & Rey point out that a major obstacle to attaining an optimal analysis is lack of data. It is hard to find credible data concerning the indirect and the overall societal consequences from power outages. To this end assessments that have been done as part of a Swedish electricity regulation, Styrel, are here used as a proxy for the social impact of electric power outages.

A large number of studies assess the economic costs incurred by power outages. Woo and Pupp (1992) review 16 such studies. Four principal methods for making these economic assessments can be distinguished (Woo and Pupp, 1992; Balducci et al., 2002; De Nooij et al., 2007; Losa & Bertoldi, 2009), they are briefly presented below:

*Customer surveys:* This method, which is the one used most frequently, consists in asking consumers questions concerning perceived consequences of a power outage of certain durations. The questions can be either direct or indirect. In the former case the customer is asked to assess the cost of the outage. In the latter case the customer will instead be asked questions concerning what they would pay to avoid the outage, known as the willingness to pay (WTP), or how much the customer would demand in return for accepting to suffer the outage, known as the willingness to accept (WTA).

*Case studies:* When using this method past power outages are analysed in order to determine the consequences that resulted. Widely studied power outages are the New York outage in 1977 and the blackout of Northeast US in 2003.

*Market based methods:* This is also known as revealed preference, as opposed to the stated preference obtained through surveys. When using this method the consequences of an outage are assessed based on the customers' behaviour on the market. Expenditures on backup facilities and the use of interruptible contracts can, for instance, provide information on how households or industries value power supply.

*The production function approach:* This method estimates the consequences of outages through lost production (for firms) or lost leisure time (for households). The cost is calculated as the ratio of an economic measure (e.g., gross output, gross domestic product GDP) and a measure of electricity consumption. The main benefit of the approach is that it makes use of readily obtainable data. The draw-back is that it makes assumptions that may be unrealistic. For instance it says that if a company suffers blackouts during x% of a year its productivity during this year will decrease by x%. This assumption could lead to overestimations in case some form of production can go on also without power supply and it can lead to underestimations if power outages cause reduction in productivity not only during the time of the outage but afterwards as well due to long term damages.

Once data has been gathered concerning outage consequences, they can be used to create a cost model. Three main kinds of cost models are used by power system planners (Raesaar et al., 2006; Bozic, 2000):

1. Customer damage function models represent the costs as a function of the interruption duration.

2. Cost of Energy not Supplied models represent the costs as a function of the unsupplied energy.

3. Combined Cost Models represent interruption costs as a sum of two components: one is a function of the interrupted load demand, another is a function of the expected energy not served.

Among the three impact categories defined by Linares & Rey (direct and indirect economic consequences and societal consequences) present methods for assessing consequences from power outages are likely to take direct economic impacts into account in a satisfactory way. However, it is less likely that the other two are taken into account satisfactorily. Customer surveys seeking to ascertain the WTP or WTA establish only the economic consequences for the informant not for those actors depending on the informant or the interests of society in general. The market based approach reflects only the interests of the consumer, which is likely to be mostly concerned with how outages will affect their own revenue or household economy. Therefore it will mainly assess the size of primary economic consequences. The product function approach by its very nature will focus on the direct economic consequences. The case study is clearly advantageous for assessing societal consequences since in hindsight the relevant data is obtainable, although perhaps not easily so. Its weakness though is that it is far from clear what inferences that can be justifiably drawn from past accidents with respect to future ones. When, for instance, studies based on evidence from the 1977 New York black-out are used as guides to understanding the consequences from present day outages it should be borne in mind what remarkable changes society and technology have undergone in the meantime. Conclusions should therefore be based primarily on the relatively few events that have occurred in recent time. In the following a new way of measuring societal consequences, based on Styrel assessments, is presented. In contrast to the above mentioned approaches this way of assessing societal consequences does not mainly measure direct economic consequences or create problems with a too poor empirical material. The results given by the Styrel approach is compared to those given by a Swedish quality of supply regulation.

## 5.2 Simulating power outages

In order to contrast present Swedish outage regulation against societal consequences that arise as estimated through Styrel a case study has been carried out. In the case study a network model of the distribution system of a midsize city in Sweden (see Figure 5.1) is used. The system has also been studied in (Jönsson et al., 2008). It is an 11kV system, in the network model it consists of altogether 1203 components. Network stations, transformers, bus bars and feeder station breakers are represented as nodes (539 in all) and cables are represented as edges (664 in all). The network is supplied from 10 in-feed transformers from higher voltage levels and serves roughly 40,000 customers. Only topology is considered in the network model which can be said to reproduce only if components and customers are energized. Flows of current and power and associated limits are not included in the model. The drawbacks of only considering topology are discussed in 5.5.

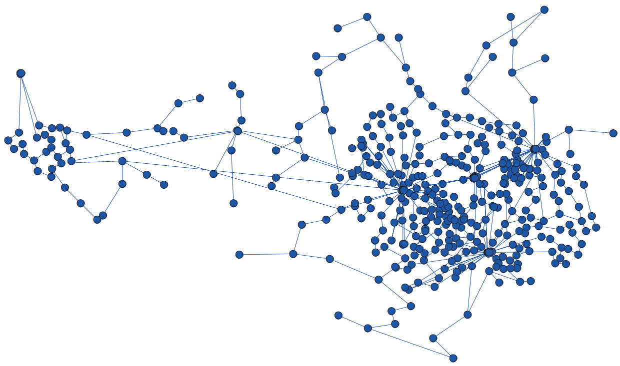

Figure 5.1: The electrical distribution network.

The network model is used to simulate outages. Altogether 6 different strain sizes are investigated: N-1, N-2, N-3, N-6, N-9 and N-12 (N-x denotes a failure and associated disconnection of x components among the total number of components, N, in the system). For N-1 and N-2 all possible failure scenarios are tested. For higher strain sizes scenarios are sampled from the full set, due to the vast number of possible failure scenarios. One failure scenario takes about 15 ms to calculate[6], therefore a complete N-3 analysis, encompassing about 578 million scenarios, would require a bit more than 7 weeks of simulation time.

The simulated outages are ranked using the two approaches; outage compensation and Styrel (see section 3.2). The overall outage compensation (OC) for a certain scenario is calculated in the following way:

$$OC = \sum_{i=1}^{N} \max\left(Fee_i * NormComp(t), MinComp(t)\right)$$

$N$ is the number of customers without power. $NormComp$ and $MinComp$ are functions of the outage time of the particular distribution stations (see Table 3.1). In this paper the outage time for all customers is assumed to be 12 h meaning that $NormComp$ is 12.5% and $MinComp$ is SEK 900. As is seen in Figure 5.2 the number of customers that will get the minimum compensation after a 12 h outage is relatively high since all customers with a yearly fee of SEK 7,200 or less will get this. If an outage with 12 h duration affects all customers 87% of the customers will receive the minimum compensation. This means that small customers will carry more weight, relatively, than if a longer outage time was chosen.

[6] The simulations were run on a computer with Intel® Core™ i5-460M Processor with 2 cores, clock speed 2.53 GHz and 8 GB memory.

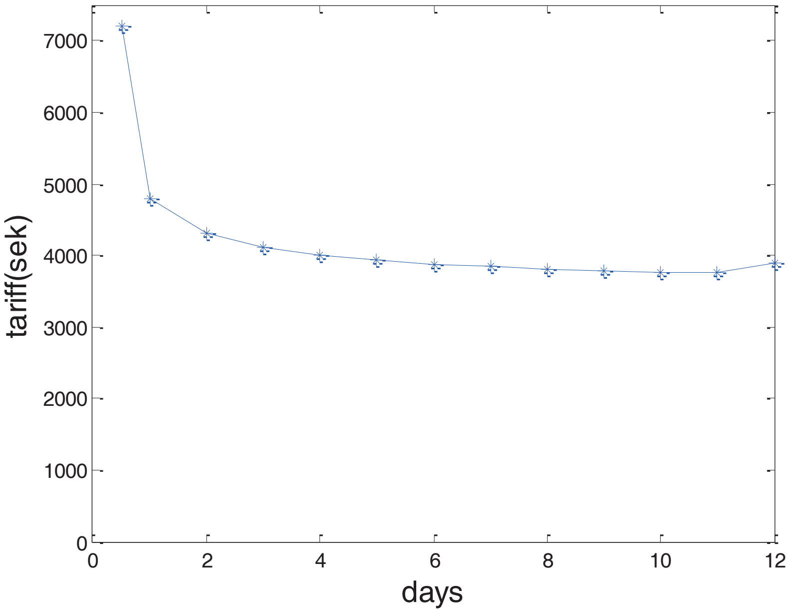


Figure 5.2: Highest yearly fee that will give minimum compensation as function of days of outage..

The OC consequence values for all simulated scenarios are ranked using the following formula, termed outage compensation normalised rank (ONR):

$$ONR = \frac{L - Rank_o}{L - 1}$$

$Rank_o$, meaning ranking based on outage compensation, is obtained by ranking scenarios in descending order and scenarios with the same consequence are given the same rank, L is the number of different rank levels.

The Styrel normalized rank ($SNR$) is determined by using the Styrel prioritization rules (described in more detail in section 3.2). A scenario A is worse than a scenario B if:

- the number of non-supplied customers with priority 0 or 1 is larger in A than in B;
- the number of non-supplied customers with priority 0 or 1 is the same in A and B and the sum of points for all non-supplied customers with priority 2 or less is higher in A than in B.

When the scenarios for a certain strain level have been ranked according to this ranking procedure the Styrel normalized rank ($SNR$) of each scenario is described as follows:

$$SNR = \frac{L - Rank_s}{L - 1}$$

$Rank_s$, meaning ranking based on Styrel, is, as before, obtained by ranking scenarios in descending order and giving scenarios with the same consequence the same rank. L is the number of different rank levels. The following simple example illustrates how $ONR$ and $SNR$ are calculated: a scenario ranked nr 577 (concerning outage compensation or Styrel) among a total number of 1000 rank levels will be given the $ONR$ or $SNR$: (1000-577)/1000=0.423. The $ONR$ and $SNR$ will always vary within the interval [0,1]. In order to test how well the outage compensation results converges the coefficient of variation, $\alpha$, is calculated for the outage compensation results. The formulas for calculating the coefficient of variation are:

$$v_i = [x_1, x_2, \dots, x_i]$$

$$\alpha_i = std(v_i)/\text{mean}(v_i)$$

$std$ denotes standard deviation and $v_i$ is a vector containing the first $i$ simulation results. It is found that after the replication of 1 million failure scenarios, the coefficient of variation has converged for all the strain levels, meaning that one million samples should be sufficient. This number of samples is therefore chosen for the N-3, N-6, N-9 and N-12 scenario simulations.

## 5.3 Correlation between consequence measures

Using the ranking method described in the previous section the outage scenarios are ordered in accordance with how a DSO would prioritize them based on the two schemes. This is done for the six different strain sizes (N-1, N-2, N-3, N-6, N-9 and N-12). The horizontal axis shows the ONR, i.e. the scenarios as ranked by the outage compensation scheme, the vertical axis shows the SNR, i.e. the scenarios as ranked based on the Styrel scheme. By arranging the plots in this way the decision making perspective of the DSO is captured and it can easily be seen if the two ways of reaching a decision concerning investments in the network are consistent or not. If there is indeed a close agreement between the two measures SNR will be a nondecreasing function of ONR, meaning that the rank correlation between OPV and SPV is 1. On the other hand, any major aberration from this nondecreasing function, meaning a rank correlation significantly lower than 1, indicates that the OPV is not reflecting the societal consequences shown by the SPV.

The results from the simulations of N-1, N-2 and N-3 are given in Figure 5.3. As can be seen in Figure 5.3, for N-1 there is a high rank correlation between the results given by the two ranking schemes although several scenarios get high $SNR$ and low $ONR$ and vice versa. In N-2 and N-3 (Figure 5.3) patterns emerge that are not evident at the N-1 strain level. The scenarios are divided into several distinct segments. Each such segment contains scenarios in which a certain number of top priority customers (priority 0 or 1) are affected. The lowest segment contains scenarios with no affected top priority customers, the next higher segment contains scenarios in which one top priority customer is affected, the following segment contains scenarios with two affected top priority customers, and so forth. The total number of these segments increases with the magnitude of the strain since the likelihood of several top priority customers being out simultaneously increases with increasing strain size. It can be seen also that within each segment there is a rank correlation between $SNR$ and $ONR$ and that the scenarios are distributed so that the maximum $SNR$ appears to be an exponential function of the $ONR$. The latter means first of all that no scenarios get higher $SNR$, within the segment, than $ONR$, while the opposite may be the case. The fact that the maximum $SNR$ appears to be an exponential function of the $ONR$ means that the scenarios that get more than average $SNR$ will get very high $ONR$.

The graphs for the higher strain levels repeat the pattern seen in the N-2 and N-3 graphs, and they are therefore left out. As can be seen in the graphs there is a poor overall correlation between the ranking results for strain sizes larger than 1.

For the complete set of scenarios as well as for the subset of scenarios without affected top priority customers (customers with Styrel priority 0 or 1) the rank correlation between the two ranking methods are analysed. In order to do this we use Spearman's rank correlation coefficient. While the frequently used linear correlation measure Pearson's R will give perfect correlation between two parameter (R=1) sets X and Y if all elements in X when multiplied by a certain factor will give the elements in Y Spearman's rank correlation on the other hand is not equally strict. It will give perfect correlation between X and Y if the ranking order among the elements in X is equal to that of the elements in Y. We are only interested in how differently scenarios are ranked by ONR and SNR and Spearman's rank correlation coefficient is therefore used instead of other correlation measures.

In Figure 5.3 (lower right) Spearman's rank correlation is shown as a function of the level of strain on the network when including scenarios where top priority customers are affected (full scenario set) as well as when disregarding scenarios where top priority customers are affected (reduced scenario set). As can be seen the rank correlation is rather high for the lower levels of strain irrespective of if scenarios where top priority customers are affected are taken into account or not. The difference in rank correlation however grows larger with increasing strain size. This reveals that although there is a poor rank correlation between $ONR$ and $SNR$ for higher levels of strain when all scenarios are included, there is a relatively high degree of rank correlation when only scenarios where lower prioritized customers are affected are taken into consideration. As discussed further in section in section 5.4 this implies that top priority customers need to be treated separately and that they perhaps are not sufficiently considered in the outage compensation scheme.

It can be seen in the graphs that the scenarios are grouped into several separate segments for all strain sizes except N-1. For each segment there is a clear correlation between SNR and ONR. It can be seen that the maximum SNR for the scenarios, within these segments, appears to be an exponential function of the ONR. This means that scenarios that have moderately high SNR will have a very high ONR. In Figure 5.4 all the scenarios in which no top-priority customer is affected are shown. The red horizontal line marks out the average SNR. The red vertical line marks out the corresponding ONR. As these lines show for the N-1 strain level scenarios with more than middle SNR will be among the 40% of the scenarios with highest ONR. For the N-2 and N-3 strain levels scenarios with more than middle SNR will be among approximately 10% of the scenarios with highest ONR. For the N-6, N-9 and N-12 strain levels, finally, scenarios with more than middle SNR will be among approximately 5% of the scenarios with highest ONR. This shows that, when the influence of priority 0 and 1 customers is disregarded, the outage compensation reflects societal criticality of outages as measured with Styrel. Scenarios that lead to more than average societal consequence, as measured with Styrel, will, without exception, be among the most costly scenarios for the DSO.

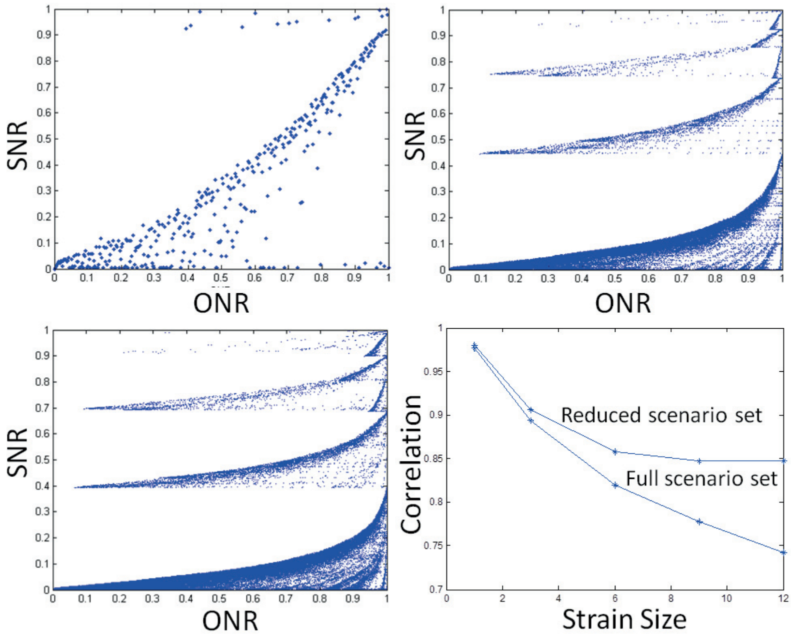


Figure 5.3: (upper left): All N-1 scenarios, (upper right): All N-2 scenarios, (lower left): N-3, 1M iterations, (lower right): Rank correlation between $ONR$ and $SNR$ as a function of size of strain.

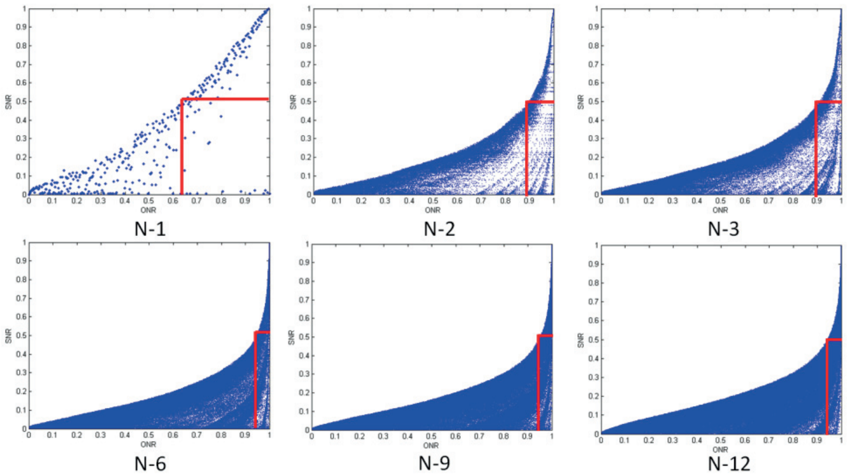


Figure 5.4: All scenarios with no affected top priority customers for N-1, N-2, N-3, N-6, N-9 and N-12 strain levels. Red horizontal line marks out the average SNR. The red vertical line marks out the corresponding ONR.

## 5.4 Discussion of the results

The result presented in the previous section show that for single component failures there is a high degree of rank correlation between results given by the two ways of measuring consequences from power outages. For larger strain sizes the rank correlation however drops and for the N-12 level of strain the rank correlation is below 0.75. When scenarios in which top priority customers are affected are removed from the scenario sets the rank correlation is improved. The degree of improvement also increases with the level of strain. For the reduced scenario set the rank correlation is still decreasing somewhat but at the N-12 level of strain it is only slightly less than 0.85. This result shows that the influence of top priority customers is lowering the rank correlation between the results given by the two measures.

Strandén et al. (2010) discuss the outage compensation scheme used in Finland, which is similar to the Swedish one, and point out that with present day regulations small, even if very critical customers, are more or less ignored. This as well as the inverse situation, when large although socially non-critical customers are given a high priority, is the reason behind the discrepancies found between results given by the ranking approaches. A possible way to improve this situation is to take $SNR$, or other indicators of the societal criticality of power customers, into account when calculating the compensation that DSOs should pay to customers that have suffered outages. It is especially important that top priority customers (customers with priority 0 or 1) are given more weight in the outage compensation regulation. If such changes were made it would be likely to steer the investments in the power grid so that the overall societal consequences from power outages are reduced. In the results large discrepancies were found between $ONR$ and $SNR$. The change that would be brought about by giving top priority customers more weight in the outage compensation scheme would however not necessarily be as indicated by these results. In fact some electricity customers that are critical for society have in the past been prioritised, despite the lack of explicit regulations demanding so. The major change that has been brought about by the introduction of the Styrel system is that this informal praxis of prioritising customers that are critical for society has become founded in regulation. Informal views on which customers that are critical for society and which are not has also, thanks to Styrel, been formalized. To let the outage compensation be influenced by criticality of power customers would thereby mean that a long since ongoing practice of prioritising certain customers over others based on societal demands would receive a more firm regulatory foundation.

The validity of the presented results depends on several factors. One factor is that only topology, but not capacity, is taken into account in the network model. This might lead to underestimations when larger strain sizes are simulated. For instance, when capacity is not considered, the entire system could be supplied from one single infeed transformer. Another issue is how well the Styrel priority values reflect the actual societal criticality of the power customers. The Styrel priorities are decided in cooperation between all political levels in Swedish society, which means that detailed knowledge as well as overview of the customers' criticality for society should be reflected in the prioritizations. However, it could be questioned if the points given to customers can indeed, as is the practice of the DSO, be used as weights. This implies that 4 normal households, which have 1 point each, carry as much weight as a large industrial facility (which has priority 5) and that 7 households have equal weight as one customer that has large impact on the functioning of society in the short time span (which has priority 2). This means that outages that create big economic losses or that leads to a degradation of societal functions can, based on Styrel, be ranked lower than outages that affect a relatively small number of normal households. This apparent weakness should be considered when judging the results. Another concern is, as mentioned in part 2, that the outage duration was assumed to be 12 hours for all affected customers. For a 12 hour outage all customers with a yearly fee of SEK 7,200 or less will get the minimum compensation (see Figure 5.2), meaning that they are given a higher compensation than what they would get if the compensation in percentage (12.5 %) was used. As the outage time increases the number of customers that are raised to the minimum amount will decrease and they will thereby become relatively less important. Overall small customers will, due to this, carry less weight in determining outage compensation as the outage time increases.

## 5.5 Summary

Two Swedish regulations, Styrel and outage compensation, were used to obtain two different measures of social consequences from power outages, $SNR$ and $ONR$. Simulations of outages in a distribution grid were performed and the results revealed that there is a high degree of rank correlation between $SNR$ and $ONR$ for the N-1 strain size while for larger sizes of strain the scenarios are divided into several distinct segments and the rank correlation between $SNR$ and $ONR$ is consequently low. Within each segment there is a clear relationship between the $SNR$ and $ONR$ of the scenarios. The maximum SNR that a scenario can get is appears to be an exponential function of the $ONR$. Due to this scenarios with more than average $SNR$ have a very high $ONR$. In other words, within each segment $ONR$ reflects $SNR$ in the sense that more than average $SNR$ implies a high $ONR$ although the reverse is not the case. Since the scenarios are divided into segments based on the number of affected top priority customers (customers with priority 0 or 1) it is the existence of such customers that is responsible for the big overall disagreements between the $SNR$ and $ONR$ when higher strain levels are analysed. This conclusion was further confirmed by calculating the Spearman ranking correlation between the results given by the two measures. This implies that customers given top priority in the Styrel system need to be treated separately and are not sufficiently considered in the outage compensation scheme. For the future it will be of interest to investigate why the maximum $SNR$ within each segment appears to be an exponential function of the $ONR$.

# Chapter 6

# Analysing restoration processes

In the last chapter a STS perspective was applied in order to study societal consequences from power outages. In this chapter the STS lens is instead focused on the issue of restoration processes in electrical distribution systems. A model is presented that enables analysis of outage time and how this depends on the amount of resources available for restoration. The model is then used in a method to address issues that are crucial for assessing resilience of CIs. The approach is demonstrated for the same municipal electrical distribution system as described in previous chapter, but it might be applicable to other CIs as well.

In order to design CI systems to be resilient it must be possible to assess the outage time of the CIs given a disturbance and how this outage time depends on decision variables such as number of repair crews and repair material. Such an analysis can aid decision makers regarding investments in the number of workers and resources needed to achieve restoration within a specified time. In the aftermath of the Hurricane Gudrun it turned out that the damages on the power system exceeded the coping capacity of the repair system. "Both personnel and spare parts ran out as the havoc was cleared and had to be called and ordered from abroad. Some of them such as the cables ran totally out, and had to be delivered to the affected areas straight from the factories" (Haanpää et al., 2006, p. 23). It should be of interest to be able to identify beforehand what the coping capacity of the repair system is and at what point available resources will be exhausted. Decision makers will thereby be able to identify resources that at present are at risk of becoming exhausted in case of a disruption in the network and they can also, conversely, identify overcapacities, i.e. resources that are stored in too great numbers. When given this information decision makers will get better opportunities for acting proactively by counteracting under- as well as overcapacities. Rasmussen (1997) argues that risk management should be considered as a control function, and he concludes that the most promising general approach to improved risk management appears to be an explicit identification of the boundaries of safe operation together with efforts to make these boundaries visible to the actors and to give them an opportunity to learn to cope with the boundaries. The method presented here is intended to enable identification of safety boundaries for electricity distribution systems.

## 6.1 Background

A system can be considered resilient if it is able to survive chocks of different kinds either by maintaining its functionality or, if functionality is momentarily lost, by quickly regaining it (see section 2.3). Considering the crucial societal importance of CIs and the fact that these systems are subject to disturbances of many kinds it is important that these systems are designed in order to be resilient. Woods (2006) points out four system properties that have to be addressed in order to make it possible to monitor and manage resilience:

1. buffering capacity: the size or kind of disruptions the system can absorb;

2. flexibility versus stiffness: the system's ability to restructure itself in response to external changes or pressures;

3. margin: how closely or how precariously the system is currently operating relative to one or another kind of performance boundary;

4. tolerance: how a system behaves near a boundary – whether the system gracefully degrades as stress/pressure increases or collapses quickly when pressure exceeds adaptive capacity.

The first of these properties is what has been referred to as robustness and the second is what has been called rapidity (McDaniels et al., 2008) and they together constitute the present resilience of a system.

Properties 3 and 4 concern how the resilience of the system will change as system parameter values are changed, something that could be depicted as movement of the system within a parameter space. The margin tells us how far the system can move within this parameter space before its resilience is below what is acceptable. Tolerance on the other hand concerns in what way the resilience of the system will change as the margin decreases and the boundary is crossed. Will resilience be lost entirely or will it decrease only moderately? To only pay attention to the two first points on the list could be a dangerous practice since CI systems are prone to undergo continuous change in several parameters. When the analysis is done the system might be located on a local optimum where robustness and rapidity are satisfactory, while at the same time in surrounding areas in the parameter space rapidity and robustness are unsatisfactory. If the system moves within the parameter space its resilience could then be found to have changed, thereby invalidating the conclusions that were drawn from the analysis. For this reason it is important to not only consider the two first points on Woods list, buffering capacity and flexibility, but also the issues of margin and tolerance when a resilience analysis is carried out. When the two last properties are investigated it becomes possible to go beyond the investigation of the systems present level of resilience and to take into consideration the way in which resilience might increase or decline as the system continues to move within the parameter space.

Restoration and resilience are two closely connected concepts, a system can be classified as resilient if it either suffers no degradation of its functionality or else is able to restore its functionality quickly when it is impacted. In other words, methods for analysing restoration should be a good starting point when investigating the issues enumerated by Woods as important for analysing resilience. Approaches for assessing restoration times have been reviewed by Liu et al. (2007) and Tabuchi et al. (2010). Six different approaches can be distinguished: 1) empirical curve fitting, 2) deterministic resource constraints, 3) markov process approach, 4) statistical regression, 5) optimization approach and 6) simulation. Below these are briefly presented, and an evaluation is then made regarding their usefulness for analysing the four system properties described by Woods. The intention is that a useful modelling approach should be used in a method, capable of treating the four system properties. This method, and not the modelling approach used, constitutes the novelty in the here presented research.

Empirical curve fitting (ECF) makes use of data obtained from previous events and/or expert opinion to fit restoration curves describing the fraction of facilities that are expected to be operational as a function of time (Liu et al., 2007). Reed et al. (2009) and Shinozuka et al. (1998) use ECF to evaluate the resilience of interdependent infrastructure systems to natural hazards such as earthquakes and hurricanes.

Deterministic resource constraints (DRC) models represents the restoration process by means of a set of simple equations. Isumi & Shibuya (1985) use DRC to analyse restoration of gas, electricity and water systems in Sendai city, Japan. A number of factors, such as climate weather and time of day, are taken into account when assessing the efficiency of repair workers.

The markov process (MP) approach represents the restoration as a Markov process (MP) where the transition probabilities can be determined by the amount of rescue resources, geographical condition as well as structural character of the lifeline system. It has been used to study strategies for restoration of lifeline systems after an earthquake (Kozin & Zhou, 1990; Zhang, 1992). Several lifeline systems can be modelled in parallel and interdependencies between different systems is then taken into account. The influence of CI dependencies as well as number of rescue resources are taken into account by letting the transition probabilities in the markov process be functions of the structural characteristic of other CI systems as well as number of rescue resources.

Statistical regression (SR) is used by Liu et al. (2007) to investigate restoration of the power system after hurricanes and ice storms. A large number of variables are taken into account for the statistical fitting of the restoration model to real life data, such as maximum wind speed, ice thickness and the total number of outages.

The optimization approach (OA) is distinguished from the other approaches by not only being concerned with predictions of likely restoration time but also with optimization of the restoration process. Important questions concern how to prioritize repairs and how many of each type of restoration crew to have. Coffrin et al. (2012) and Cavdaroglu et al. (2013) use a mathematical approach where the time required for travelling a certain route, interconnecting a set of sites, can be inferred from the time required for travelling between each pair of sites. The power system network functionality is analysed using a linearized DC model. Xu et al. (2007) use a genetic algorithm to optimize restoration. The algorithm is applied to a discrete event simulation model that is also used in (Tabuchi et al., 2008; Tabucchi et al., 2010).

The last among the six approaches that have been used for analysing restoration times is the simulation approach. Two main kinds of simulation have been used to determine restoration times, Monte Carlo simulation (MCS) and discrete event simulation (DES). Brown et al. (1997) and Balijepalli et al. (2005) use a two stage MCS to assess impacts of storm events on the power system. Tabuchi et al. (2008) use DES to model post-earthquake restoration of the LA water system. They take into account decision variables such as number of repair crews and repair prioritization rules. They estimate time needed to restore supply to 90%, 98% and 100% of the customers. Restoration time is determined separately for each region within the service area. They also model uncertainty in the simulation results explicitly, presenting 90% confidence intervals for the results. All event durations are modelled as triangularly-distributed random variables. Four kinds of output are generated by the modelling approach: a) Restoration curves b) Spatial distribution of restoration c) Crew usage d) Material usage (Tabucchi et al., 2008; Tabucchi et al., 2010).

In the following it is discussed what is required of a modelling approach for it to be applicable for treating the four issues mentioned by Woods. Concerning 1. And 2. buffering capacity as well as flexibility are largely decided by the structure of the CI network and characteristics of the repair system. Buffering capacity can be obtained by having redundancies in the network so that customers can be supplied through alternative network paths in case some fail. Flexibility can be obtained by having a network that makes it possible to change the network topology through switching of breaker positions so that customers can be re-supplied. It is also decided by the repair system and its ability to repair damaged parts of the network. Concerning 3. and 4. these two issues can be investigated in the different approaches with respect to variables that are included in the model. The analysis will then be done by changing the variable in the model and see how much change is needed before the systems resilience is intolerably bad (this amount of change is the systems margin to the unsafe area of the parameter space), as well as how the resilience of the system changes as the margin becomes smaller (this is the tolerance of the system). Below the six modelling approaches that have been used for assessing restoration times are evaluated with respect to how useful they are for analysing the properties of resilience suggested by Woods.

Buffering capacity and flexibility can to some extent be studied with ECF since we can see how restoration times should increase with the size of the disruption. The main limitation of this approach in this respect is however that it requires that the network being analysed is similar, concerning its resilience characteristics with those networks from which data for the restoration curve is gathered. The way in which buffering capacity or flexibility can change based on choice of network design, for instance concerning number of redundant paths by which customers can be supplied, or based on design of repair systems will not be possible to analyse by empirical curve fitting. If properties 1) and 2) can be analysed only to some extent with ECF this is impossible concerning properties 3) and 4) since this requires that system parameters are varied. Varying of variables is only possible to a very limited degree with the ECF approach.

DRC can be used to analyse buffering capacity as well as flexibility of CIs if the CI network is included in the model. One crucial part of flexibility can however not be conveyed very well with the model, this is component repair. Due to the simplicity of the modelling approach component repairs cannot easily be treated in an individual manner, based on component and failure type. Concerning properties 3) and 4) variables such as number of repair teams and weather conditions can be varied in the model and it thereby becomes possible to analyse the system's margin and tolerance with respect to these variables. However, since component failures cannot easily be treated in an individual manner concerning their demand for different kinds of resources it is not possible to analyse how the restoration would be affected by variations in amounts of available resources. For this reason properties 3) and 4) cannot be treated with respect to this important set of decision variables. This constitutes a major draw-back of the approach.

If a model of the network is used MP could be of use for analysing buffering capacity and flexibility since it can then be seen how widespread the effects will be from a certain degree of damage of a CI as well as how quickly the recovery will take place. The accuracy of the analysis of flexibility will however be limited by the fact that MP models cannot take individual repair times for components into account. Also it cannot easily take decision variables such as amounts of available repair resources into account. Due to this, margin and tolerance cannot be studied with respect to this set of system parameters.

In SR the network is not explicitly represented and buffering capacity and flexibility regarding the network can therefore not be analysed. Concerning aspects 3) and 4) variables such as maximum wind speeds and amount of customers affected are used in the model. SR can consequently be used to analyse margin and tolerance with respect to these variables. In the regression model we would then vary a certain parameter, for instance the wind speed, and see how this affects the overall restoration time. A large group of decision variables, namely repair resources, are however not easy to include in the model and the SR therefore is not useful for analysing margin and tolerance of the system with respect to these decision variables. It is especially useful to analyse margin and tolerance with respect to decision variables and for this reason SR is an inappropriate approach in the present context.

Examples of OA that were identified in the literature can be used to analyse buffering capacity and flexibility if the CI network is explicitly represented in the model. Concerning properties 3) and 4) the approach can include variables such as number of repair workers but as with previously mentioned approaches, repair resources cannot easily be taken into account. For this reason this approach is unfavourable in the present context.

Simulation can be used to analyse buffering capacity as well as flexibility of CI systems, if the CI network is explicitly included in the model. Flexibility can also be represented in a more precise way since the repair times of component failures can be treated individually. A strength of this approach is also that resources as well as other system variables can be explicitly included in the model thus making it possible to analyse margin and tolerance with respect to these variables.

Summing up what has been said of the different approaches for assessing restoration times, it can be concluded that the simulation approach is most promising for enabling an analysis of the four properties mentioned by

Woods. This approach is hence used for modelling restoration processes here. Although the simulation approach is capable of addressing all of the four properties mentioned by Woods there is, to the best of the authors' knowledge, a lack of a method that address them in a transparent manner. In order to identify the margin and tolerance (point 3. and 4. in Woods list) restoration processes should be simulated for a wide variety of system parameter values. Only in this way can it be seen where in the parameter space that the system goals are reached and how the outage time varies over the parameter space. Based on this knowledge the margin (property 3.) can be decided as the distance of the system from the safety boundary and tolerance (property 4.) can be decided as the steepness with which outage time rises or falls in the parameter space surrounding the system. In contrast in papers where the simulation approach has been used (e.g. Tabucchi et al., 2008; Tabucchi et al., 2010) restoration times are investigated under given conditions but not for a large number of different system parameter values. Xu et al. (2007) vary system parameter values in order to identify optimal parameter values but margin and tolerance is not analysed. In the work presented in this chapter a simulation approach is introduced to model the system and a method is then put forward to analyse the four properties which according to Woods are crucial for assessing resilience.

## 6.2 Model

A hybrid model is used to perform simulations of restoration processes in the distribution system. It consists of two sub-models. The first model is a network model for representing the power network and used to calculate the number of customers affected by a given failure scenario (see section 2.4). The second model is a queuing model for representing the repair system and calculate the repair time given resource constraints. The model that was developed and used in the research presented here is an agent based, rather than equation based model (Parunak et al., 1998) and the main reason for choosing this approach is the modularity of the agent based models, i.e. model components can be developed and changed easily while the overall model structure remains the same. In the repair system model that was developed component failures are represented as waiting in a queue that is served by repair teams. The model does not consider the geography in which the network components are located and in which repair personnel move about. The reason for this is that the present method is intended to be used for analysing restoration processes in electricity distribution systems. In these systems distances are short enough to be disregarded in the model. However, if CIs covering a region or country were studied, for instance the electricity transmission grid, it would likely demand that geography was taken into consideration. Also, the model does not consider movable stations or back-up power.

Below the repair system model is described using ODD (Overview, Design concepts and Details). ODD has been developed in order to make model reimplementation easier. See Railsback & Grimm (2011) for more details on ODD. No input data or sub-models are used and the last two sections of ODD, dealing with input data and sub-models, are therefore left out.

*Purpose*

The model should make it possible to analyse how quickly faults occurring in an electrical distribution network are repaired and how the repair time is affected by variations in amount of available resources and repair teams.

*Entities, State Variables and Scales*

The model has four kinds of entities: faults, queues, repair teams and a storage. They are described below:

- Faults have a repair time and a vector specifying resources needed for repair as well as a specification concerning size of needed repair team.
- The queue holds faults that await being serviced by a repair team.
- Repair teams serve the first failure in the queue that is serviceable. In case this is required repair teams can cooperate (i.e. two two-man teams can form a four-man team).
- The storage has resources of different amounts (specified by a vector).

*Process Overview and Scheduling*

On each time step the storage checks if the inventory should be updated (a matrix specifies when and by how much the inventory should be refilled). On each time step the repair teams do one of the following:

- If the repair team is currently repairing a fault it does one of the following:
    - Return non-consumable resources (trucks or excavators) if the required usage time has passed.
    - If the fault has been serviced during its required repair time the fault is removed and the repair team becomes ready to take new assignments.
- If the repair team is not currently repairing a fault it does one of the following:
    - Joins a currently ongoing repair operation that is understaffed (i.e. a 2 man team is working on the fault although a four man team is preferable).
    - The first fault in the queue that can be serviced with the given amount of available resources and repair teams is removed from the queue and repair is begun.

The simulation ends once all customers are supplied with electricity.

*Design concepts*

Repair times of individual faults are important in this model and it is assumed that by simulating the system at a component level the overall restoration process and the repair time can be studied. The choice of what kinds of failures that are simulated as well as the repair time and resource that they require should be based on interviews with personnel responsible for restoration of failures in the CI of interest.

*Initialization*

The faults in the queue at the start of the simulation are given by the simulation of component failures in an electricity distribution network. Their position in the queue is decided based on rules of priority which may vary among DSOs. Only faults that need to be repaired in order to restore electricity to customers are placed in the queue.

The above describe model was implemented in object oriented programming in Matlab. The model was verified both against hand calculations and against a similar model created in NetLogo, a different programming language.

## 6.3 Conceptual approach

The method that is presented here is intended to enable identification of boundaries of safe operation for electrical distribution systems. The concept of safety boundaries is here understood in the following way (see Figure 6.1): it is assumed that the state of a system can be described by a certain number of parameters, for instance they could be X, Y1 and Y2. The system can be said to be positioned in an N-dimensional parameter space, where N is the number of parameters defining the system. In this example N is 3. Ideally the behaviour of the system should be analysed with respect to all parts of the N-dimensional parameter space. However, due to the large number of possible parameter combinations that would result for only moderately large values of N the here proposed method analyses the systems behaviour with respect to only two parameters at a time. A more fundamental parameter X (meaning the number of repair teams) is in each two dimensional parameter space related to one less fundamental parameter Yi (meaning the i:th member in a list of different kinds of resources that are used by the repair teams to perform repair operations). In the above mentioned example the systems position will therefore be described by two 2-dimensional parameter spaces, defined by the parameters X and Y1 and X and Y2 respectively. It is further assumed that the value of the system parameters is in constant evolution. This evolution can be seen as a drift through the parameter space over time. In the example shown in Figure 6.1 it can be seen that the system is far from the safety boundary in the (X,Y2) parameter space but is approaching the boundary in the (X,Y1) parameter space. Assuming that we want to keep a margin towards the safety boundary an appropriate decision that could be made if an analysis gave this particular result is to avoid decreasing variable X and Y1 and possibly increase them while keeping Y2 constant or possibly decreasing it.

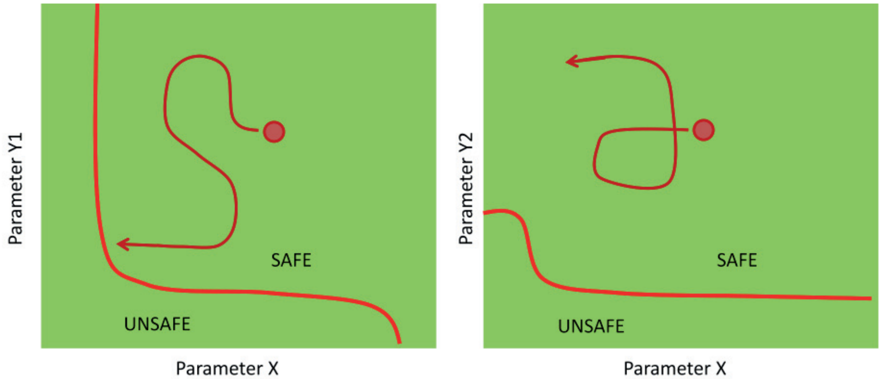


Figure 6.1: system state (circle) located in two parameter spaces defined by parameter X and Y1 and X and Y2 respectively. A boundary (red line) separates the safe part of the parameter spaces, where the system safety goal is met, from the unsafe part, where the system goal is not met. The system is in constant evolution and is thereby drifting through the parameter spaces (curly arrow).

## 6.4 Case study

The method is applied to the same distribution system that was studied in the previous chapter. Component failures in the network are simulated using the network model. Six different strain sizes are studied: N-1, N-2, N-3, N-4, N-5 and N-6. Only a sample of all possible scenarios, i.e. randomly generated failure scenarios, are used due to the excessive simulation times that would result if a complete scenario set was used. When generating the failure scenarios each component is equally likely to be included in a given scenario.

### Empirical data to populate the model

Interviews were conducted with employees at the DSO concerning what amount of repair teams and different kinds of resources that are available in the repair system at different time points. We did not receive information concerning two resources, station transformers and switchgear, and for this reason the amount of these resources was assumed. The result is shown in Table 6.1. The interviewed employees said that one repair team is immediately available during all times. Remaining repair teams will arrive after 3 hours. This arrival rate was emulated in the model. Electricity network operators are cooperating and when one operator has failures in their network it can thereby get repair teams and resources from neighbouring operators[7]. The system experts that were interviewed believe that due to this cooperation they can get whatever they need in terms of repair teams and resources within 12 to 24 hours. In order to take this uncertainty into account two different cases are analysed in the following, one assuming that delivery of additional resources occurs after 12 hours and the other assuming that delivery takes place after 24 hours.

Table 6.1 Arrival of repair teams and resources. Brackets indicate interval.

| | Immediately available | Delivery 1 | Delivery 2 | Delivery 3 |
|---|---|---|---|---|
| Time(h) | 0 | 3 | 12 | [12,24] |
| Two-man team | 1 | 13 | 0 | ∞ |
| Cable (m) | 2000 | 0 | 0 | ∞ |
| Station transformer | 5 | 0 | 0 | ∞ |
| Truck | 2 | 0 | 0 | ∞ |
| Excavator | 3 | 0 | 0 | ∞ |
| Switchgear | 3 | 0 | 5 | ∞ |
| Fstat breaker | 8 | 0 | 0 | ∞ |

The prioritization of repair activities is, according to the informants, decided according to the following rules: network stations (housing switchgear and transformers) are repaired before cables, and cables are repaired before breakers. Stations with more customers are repaired before those with fewer customers and cables connecting stations with more customers are repaired before cables connecting stations with fewer customers. In the simulation failures are therefore placed in the queue in the order given by these prioritization rules.

Failure mode of the components, and thus repair time and resources needed for repair, was decided based on information from employees at

[7] www.elsamverkan.se

the DSO (Table 6.2). A two man team can perform a repair job that requires a 4-man team, but the repair time will then double. As was mentioned in section 2.4 there exists two kinds of node failures. Transformer failures in network stations are of the second kind, i.e. they only lead to loss of power supply for customers connected to the network station in question while leaving the network connectivity unchanged. All other node failures are of the first kind, i.e. they lead to disconnection of the node from the network. The two last rows in Table 6.2 concern failures on feeder station transformers and bus bars respectively. These failures have a repair time that is much greater than the simulation time (6 days for transformers and one month for bus bars). These failures are therefore considered to be irreparable in the restoration model.

Table 6.2: Component failure data, brackets indicate rectangular random distribution within the interval.

| Fault type | Fault Mode | Relative likelihood | Required resource | Required repair team | Repair time (h) |
|---|---|---|---|---|---|
| Station | Cable Fault | 80% | Truck, Excavator, Cable (20 m) | 4-man | 7 |
| Station | Transformer | 10% | Truck, Transformer | 2-man | [4,8] |
| Station | Switch-gear | 10% | Truck, Excavator, Cable (20 m), Switch-gear | 4-man | [7,10] |
| Feeder Stat. Cable | Cable fault | ... | Truck, Excavator, Cable (20 m) | 2-man | [5,7] |
| Other Cable | Easy to find | 90% | Truck, Excavator, Cable (20 m) | 2-man | [2,24] |
| Other Cable | Hard to find | 10% | Truck, Excavator, Cable (20 m) | 2-man | [48,72] |
| Breaker | Breaker fault | ... | Truck, Cable (20 m), Breaker | 2-man | 0.5 |
| Feeder Stat. Transformer | ... | ... | ... | ... | >>24 |
| Feeder Stat. Busbar | ... | ... | ... | ... | >>24 |

Seven decision variables are analysed: X=2-man repair teams, Y1=breakers, Y2=cable, Y3=excavators, Y4=switch-gear, Y5=transformers, Y6=trucks. The safety criterion that is used is that power is restored to all customers within 24 hours. The reason for choosing this safety definition is that a Swedish regulation that has been in place since 2011 demands that no customer should suffer an outage longer than 24 hours (Swedish Energy Agency 2009).

**Application of the method**

An important question is how many samples that will have to be used in order to get valid results. In this chapter the maximum repair time is of interest and it is therefore measured how quickly the maximum repair time converges to a final value as the number of samples increases. N-5 failures are simulated and it is assumed that 10 repair teams are available. The analysis is performed for seven different initial resources levels:

- scenario 1 = normal level of resources (shown in Table 6.1);
- scenario 2 = normal except for no excavators at start of simulation;
- scenario 3 = normal except for no trucks at start of simulation;
- scenario 4 = normal except for no cable at start of simulation;
- scenario 5 = normal except for no breakers at start of simulation;
- scenario 6 = normal except for no switch-gear at start of simulation;
- scenario 7 = normal except for no transformers at start of simulation.

For each scenario the convergence is calculated three times, to get additional certainty. The average of the three calculated results can be seen in Figure 6.2. Markers indicate were the average is increasing. It can be seen that the results have converged for all scenarios after 600 samples and therefore ideally the number of samples should be greater than 600. Due to the long simulation times required in the research work 300 samples have been used. According to the convergence analysis this should lead to errors of at most a few hours which is here considered acceptable.

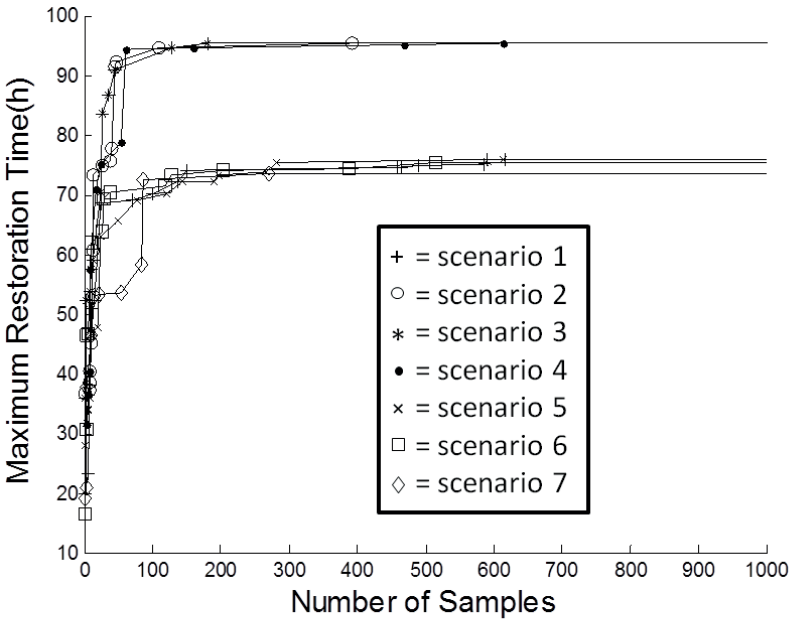


Figure 6.2: Maximum restoration time as function of sample size.

Sensitivity experiments consist in changing one or more system variables over a wide range and see how the system responds (Railsback & Grimm, 2011). Here sensitivity experiments are performed for two variables at a time, number of repair teams and amount of different kinds of available resources, thus creating one two-dimensional parameter space for each kind of resource, here called a safety map. One axis shows the amount of two man repair teams available in the repair system while the amount of resource is shown on another axis. One of these repair teams is available from the beginning of the simulation while the others arrive 3 hours into the simulation. The height of the bars in the parameter space represent the maximum time required to restore power to all customers, when back-up power is not considered. Each map encompasses 10*10 variable combinations and for every combination the restoration model is sampled 300 times. In other words, each safety map is based on simulation of 30,000 restoration processes. The area in the parameter space where power supply is brought back to all customers within 24 hours, i.e. where the system safety goal is achieved, in a given fraction of the total number of simulation samples is the safe space. In the result presented below this fraction is 0.95. Parts of the scenario space were this is achieved are considered safe and are consequently green, while other parts are considered unsafe and are red. The reason why the fraction has not been chosen to be 1 is that this target cannot be met under given circumstances since a tenth of the cable failures have a repair time that is significantly longer than 24 hours. The position of the system in the parameter space is marked out with a yellow circle and it can thereby be seen if the system is located within the safe or unsafe part of the maps.

## 6.5 Result

In the following safety maps are shown for six different kinds of resources (breakers, cable, excavators, switch-gear, transformers and trucks) as well as for six different levels of strain of the system (N-1, N-2, N-3 and N-4, N-5 and N-6). The employees that were interviewed estimated that extra resources and repair teams would arrive within an interval bounded by the lower limit 12 hours and the upper limit 24 hours. Hence, two analyses are here performed, one assuming that the supply will occur after 12 hours and one that it will occur after 24 hours.

When supply is supposed to occur after 12 hours the safety maps shown in Figure 6.3 and Figure 6.4 are obtained. We can see that the system at its present position in the safety maps has a maximum restoration time of a bit more than 50 hours for the N-1 strain scenarios, a bit more than 70 hours for the N-2, N-3 and N-4 strain sizes, and approximately 80 hours for the N-5 and N-6 strain sizes. We can furthermore see that in most safety maps the maximum restoration time cannot be reduced by changing the position of the system in the safety maps. Only in the maps for the N-4 and N-6 level of strain the maximum restoration time is slightly reduced as the number of trucks is increased from the present amount. Changing the position of the system in the safety maps can however in many cases mean that the maximum restoration time is increased. At the N-1 strain level if trucks, excavators or length of cable is reduced to zero the maximum restoration time will increase from approximately 50 to approximately 60 hours. At the N-2 level of strain the situation is similar to that at the N-1 strain level. The maximum restoration time is only increased if number of trucks, number of excavators or length of cable is zero. In these cases maximum restoration time will increase from approximately 70 to approximately 80 hours. At the N-3 level of strain the maximum restoration time is increased slightly if the number of trucks or excavators is reduced to one and the maximum restoration time increases to about 80 hours if either number of trucks, number of excavators or length of cable is reduced to zero or if the number of repair teams is one. At the N-4 level of strain having zero trucks, excavators or length of cable or having only one repair team will increase the maximum restoration time to almost 80 hours. It can however be noticed that the maximum restoration time is here slightly shorter than at the N-3 strain level. This shows that the result, as was expected based on the convergence analysis, have not converged entirely. Maximum restoration time is also increasing gradually as variables values are reduced. Having only three repair teams, as well as only one excavator or only one or two trucks will cause slightly longer maximum restoration times. At the N-5 strain level the maximum restoration time increases from about 70 hours to about 80 hours when number of trucks, number of excavators or length of cable is reduced to zero or when number of repair teams is reduced to one. At this strain level only a very slight gradual increase is seen in maximum restoration time is seen for excavators, trucks and repair teams, indicating that the results, as expected, have an error margin of a few hours. Finally at the N-6 level of strain the maximum restoration time increases from slightly less than 80 hours to slightly more than 80 hours when number of trucks, excavators or length of cable is reduced to zero or when number of repair teams is reduced to one.

It is visualised with color in the safety maps for what parameter values a safety goal, restoration within 24 hours in 95% of the simulated scenarios, is achieved. For strain levels N-1 and N-2 the safety goal is attained in all parts of the parameter spaces. Trusting that repairers and resources will arrive after no longer than 12 hours and that the straining of the system will not be larger than N-4 it will be safe to place the system in any part of safety maps. When looking at the maps for the N-3 and N-4 level of strain it can be seen that there is a region in each of the safety maps where the safety requirement is not fulfilled. In all of the maps it can be seen that it will be unsafe to have only one repair team. Furthermore it can be seen in the maps for trucks, cable and excavators that it will be unsafe to have no trucks, no cable and no excavators. Finally concerning the performance of the system at the N-5 and N-6 strain level it can be seen that for all safety maps the safety requirement will not be attained anywhere. Finally it can be concluded, by looking at the circle marking out the position of the system in the safety maps that the system is at present safe from all the simulated strain sizes except N-5 and N-6 if extra resources arrive after 12 hours. It can be seen that the tolerance of the system to variable changes is high. Maximum restoration time is not drastically changed in different parts of the safety maps and changes are never much longer than 10 hours which is not so high considering that the maximum restoration times are in all parts of the maps longer than 40 hours.

When supply is supposed to occur after 24 hours the safety maps shown in Figure 6.5 and Figure 6.6 are obtained. It can be seen here that the maximum restoration time is approximately 60 hours for the N-1 strain scenarios, a bit more than 60 hours for the N-2 scenarios and almost 80 hours for the N-3, N-4 and N-5 scenarios. For the N-6 strain level the maximum restoration time is however slightly shorter, about 70 hours, indicating that there is some uncertainty in the results. We can furthermore see that at the N-1 strain level the maximum restoration time is insensitive to changes in all parameter values except number of trucks, number of excavators and length of cable. If the latter are reduced to zero the maximum restoration time will increase from approximately 60 to approximately 80 hours. At the N-2 level of strain the maximum restoration time increased from a bit more than 60 hours to a bit more than 80 hours if number of trucks, number of excavators or length of cable is zero. The restoration time is also increased to almost 80 hours if the number of repair teams is one. At the N-3 level the maximum restoration time is increased slightly if the number of trucks or excavators is reduced to one and the maximum restoration time increases to almost 100 hours if either number of trucks, number of excavators or length of cable is reduced to zero or if the number of repair teams is one. At the N-4 level of strain the maximum restoration time is increased from less than 80 to almost 100 hours if trucks, excavators or length of cable is reduced to zero, and it increases to almost 90 hours when the number of repair teams is reduced to one. At the N-5 level of strain decreasing the number of trucks, excavators or length of cable to zero or having only one repair team leads to a maximum restoration time close to 100 hours. It can be seen that the maximum restoration time increases gradually as the number of trucks, excavators and repair teams is reduced. Having only one excavator, one or two trucks or only 4 repair teams leads to increased maximum restoration time. Finally at the N-6 level of strain the maximum restoration time increases to about 90 hours when the number of trucks, excavators or cables is zero or the number of repair teams is only one. The maximum restoration time is also slightly increased when the amount of excavators is reduced to one and when the number of trucks is reduced to one or two as well as when the amount of repair teams is four.

At the N-1 strain level for three of the maps, those for switch-gear, transformers and breakers, the safety requirement is attained in all parts of the safety maps. In the remaining three maps, those for trucks, excavators and cable the safety requirement will not be attained if the amount of trucks, excavators or cable is zero. On the N-2 and N-3 strain levels there are unsafe regions on all six safety maps. In all of the maps it can be seen that it will be unsafe to have only one repair team. Furthermore it can be seen in the maps for trucks, cable and excavators that it will still, as was the case already at the N-1 strain level, be unsafe to have no trucks, no cable or no excavators. On the N-4, N-5 and N-6 strain levels there will be no safe regions in any of the safety maps. It can be concluded, by looking at the circle marking out the position of the system in the safety maps that the system is at present safe from N-1, N-2 and N-3 strain sizes while it is not safe from higher levels of strain.

The tolerance of the system to variable changes is lower than when supply of extra resources is supposed to occur after 12 hours. Reducing the number of trucks, excavators or cables to zero now leads to increase of maximum restoration time with 20 hours or more in all safety maps.

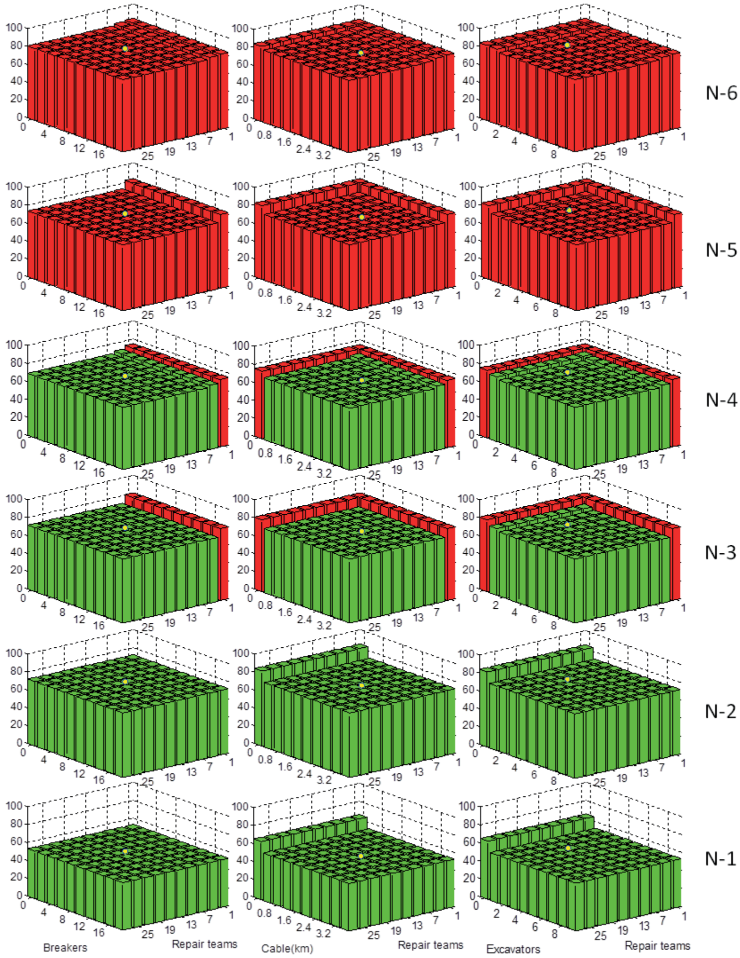


Figure 6.3: Strain level for each row of bar graphs (N-1 up to N-6) is indicated on the right side. Bar graphs in the first column show safety with respect to amount of breakers and amount of repair teams, column 2 shows safety with respect to length of cable (km) and amount repair teams and column 3 shows safety with respect to amount of excavators and amount of repair teams. Height of bars show maximum restoration time (hours), not considering back-up power. 300 samples are used. Repair teams and resources are infinite after 12 h. Restoration time is slightly shorter on the N-4 level than on the N-3 level of strain showing that the result has not converged entirely. Regions in the safety map where restoration is achieved within 24 hours in 95% of the scenarios are green.

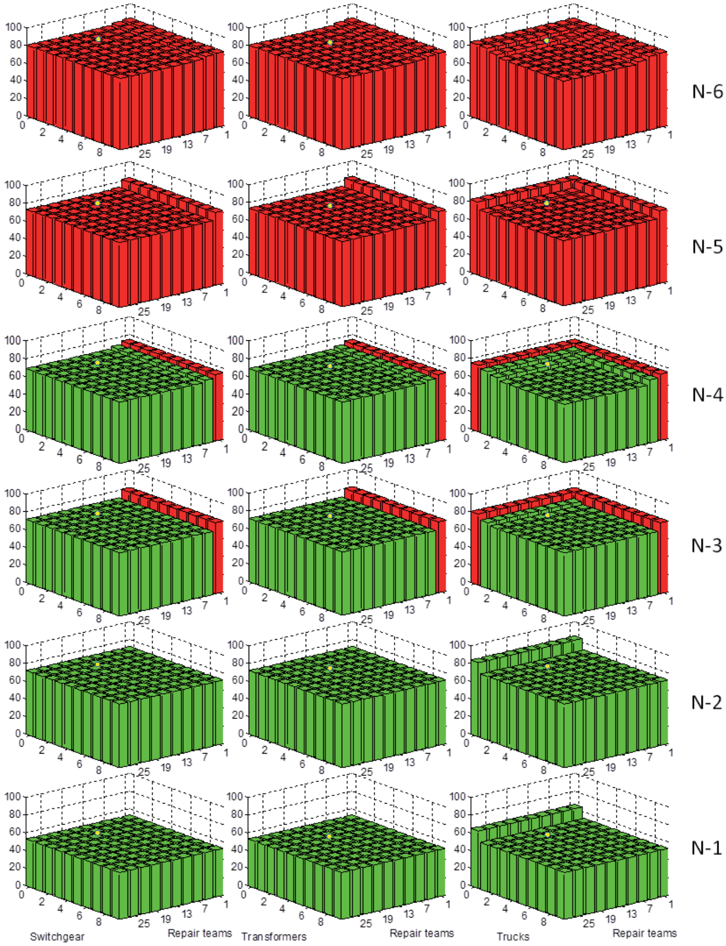


Figure 6.4: Strain level for each row of bar graphs (N-1 up to N-6) is indicated on the right side. Bar graphs in the first column show safety with respect to amount of switchgear and amount of repair teams, column 2 shows safety with respect to amount of transformers and amount repair teams and column 3 shows safety with respect to amount of trucks and amount of repair teams. Height of bars show maximum restoration time (hours), not considering back-up power. 300 samples are used. Repair teams and resources are infinite after 12 h. Restoration time is slightly shorter on the N-4 level than on the N-3 level of strain showing that the result has not converged entirely. Regions in the safety map where restoration is achieved within 24 hours in 95% of the scenarios are green.

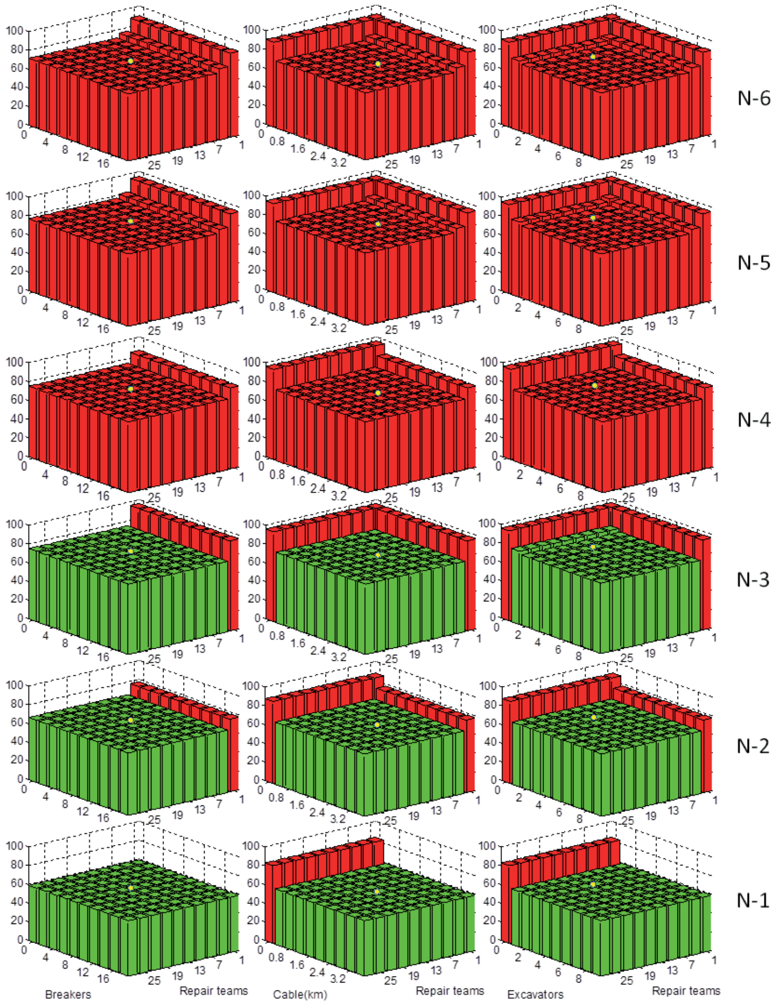


Figure 6.5: Strain level for each row of bar graphs (N-1 up to N-6) is indicated on the right side. Bar graphs in the first column show safety with respect to amount of breakers and amount of repair teams, column 2 shows safety with respect to length of cable (km) and amount repair teams and column 3 shows safety with respect to amount of excavators and amount of repair teams. Height of bars show maximum restoration time (hours), not considering back-up power. 300 samples are used. Repair teams and resources are infinite after 24 h. Regions in the safety map where restoration is achieved within 24 hours in 95% of the scenarios are green.

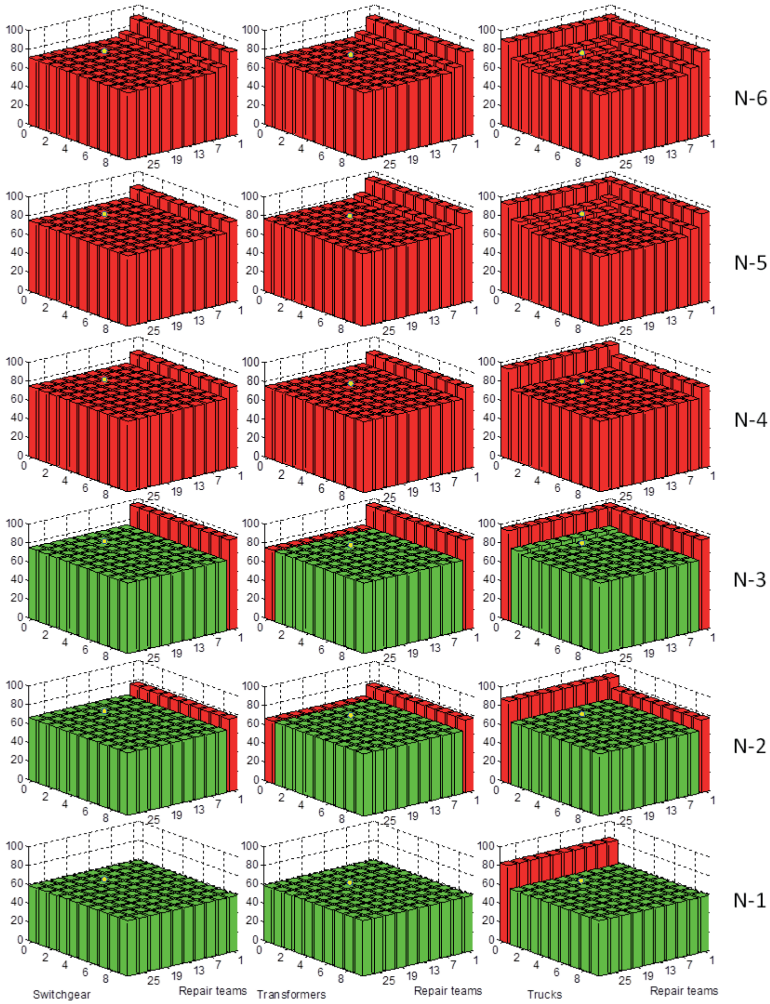


Figure 6.6: Strain level for each row of bar graphs (N-1 up to N-6) is indicated on the right side. Bar graphs in the first column show safety with respect to amount of switchgear and amount of repair teams, column 2 shows safety with respect to amount of transformers and amount repair teams and column 3 shows safety with respect to amount of trucks and amount of repair teams. Height of bars show maximum restoration time (hours), not considering back-up power. 300 samples are used. Repair teams and resources are infinite after 24 h. Regions in the safety map where restoration is achieved within 24 hours in 95% of the scenarios are green.

## 6.6 Discussion of results

In the previous section a number of safety maps were shown describing the way maximum restoration time of an electricity distribution system depends on a number of decision variables. The analysis shows that the demand made by the Swedish law, i.e. restoration of all customers within 24 hours, cannot be fulfilled in all simulated cases when the use of back-up power is not considered. Maximum restoration time, shown on the vertical axis in the safety maps, is significantly longer than 24 hours for all levels of resources, for all strain sizes and all assumptions of time of supply of additional resources. This result is not surprising since, as is seen in Table 6.2, a tenth of all cable failures have repair times that are within the range 48 to 72 hours. When customers loose power due to such failures there is no way of achieving restoration within 24 hours by having more repair teams or repair resources.

The results show that the four system properties mentioned by Woods as crucial for analysing resilience can be treated by the here suggested method. The crucial novelty of the here presented method, that makes it useful for analysing these properties is that sensitivity analyses are performed, based on the simulation approach, showing how outage time depends on decision variables. Through the sensitivity analyses the effect of simultaneously changing two variables can be studied. It can also be seen for what variable values that the system goal (in this case restoration of all customers within 24 hours in 95% of the simulated scenarios) is reached and by what degree the performance of the system changes. Based on this knowledge the margin (property 3) can be decided as the distance of the system from the safety boundary and tolerance (property 4) can be decided as the steepness with which outage time rises or falls in the parameter space surrounding the system. Concerning the issue of tolerance it can for instance be seen that the system has a better tolerance for reductions in number of transformers than for reduction in number of trucks. At the N-3 strain level, and assuming supply of extra resources after 24 hours, reducing the number of trucks to zero will result in significantly higher maximum restoration time while reducing the number of transformers to zero, although moving the system across the safety boundary, will not imply any change in maximum restoration time. Furthermore, thanks to explicitly simulating the network and the repair system buffering capacity and flexibility (properties 1 and 2) are taken into account. While in the present research it was analysed how removal of network components affect restoration time it could also be possible to analyse the opposite, that is, how addition of redundant network components enforces the network and improves it robustness.

By addressing margin and tolerance the presented method does not only take into account the present resilience of the system but also the way the systems resilience would change if parameter values were changed. The benefit of this widened scope is illustrated by comparing the results that are obtained when assuming that additional resources are supplied after 12 hours with the results that are obtained when additional resources are supplied after 24 hours. For these two cases the performance of the system with respect to the safety goal is the same for most levels of strain. The only difference is that the safety goal is attained for the N-4 level of strain if supply of extra resources occurs after 12 hours but is not attained if resources occurs after 24 hours. However the margin and tolerance of the system is different for these two cases. When supply of resources is assumed to occur after 12 hours the system can, for strain levels of N-1 and N-2 be placed at any given location in the safety maps and still live up to the safety goal. When supply of resources is supposed to occur after 24 hours certain parts of the safety maps will be unsafe for all levels of strain and changing the position of the system within the safety map may now lead to a loss of safety. The tolerance is also different for these two cases. When supply of resources is assumed to occur after 12 hours difference in maximum restoration time at different parts in the safety maps are in most cases very small and they are never larger than 10 hours. In contrast, when supply of resources is assumed to occur after 24 hours parameter changes can in most safety maps lead to changes in maximum restoration time with 20 hours or more. If margin and tolerance is not taken into account in the analysis the difference, as concerns achievement of the safety goal, between getting extra resources supplied in 12 hours compared to getting resources after 24 hours does not appear great. When the here presented analysis, that takes margin and tolerance into account, is used it is seen that there is a clear difference between these two cases and that the system, in the latter case, as it continuous to move through the parameter space is prone to lose its resilience. This will not be as likely in the former case.

Several researchers have previously simulated CI restoration processes (Tabucchi et al., 2008; Tabucchi et al., 2010). To the author's knowledge, no previous papers have however used the simulation approach to analyse margin and tolerance of an electricity distribution repair system. Tabucchi et al. (2009, p. 278) point out the usefulness of the simulation approach for performing the kind of analysis presented in this chapter: “Another primary intended use of the model is to help evaluate the effectiveness of possible risk reduction strategies. One can simulate implementation of strategies under consideration (e.g. increasing the number of repair crews or adding redundancy to the system), and then compare the resulting output with the original output to determine their effectiveness in making the restoration faster and more efficient”. Tabucchi et al. in the quote suggest research work that is similar to that which has been carried out here. It is said for instance that the number of repair crews could be varied in order to see which impact the change has on the time required for achieving restoration. While Tabucchi et al. suggests something that closely resembles the analysis method presented here they have not explicitly made the connection between their work and Woods (2006) four principal issues of resilience that are considered here. While treating buffering capacity and flexibility they are not explicitly addressing the issues of margin and tolerance of the repair system.

A severe limitation of the method presented here is that it enables analysis of only a very limited part of the entire N-dimensional parameter space. Using the approach it can be seen how the simultaneous change of a fundamental variable X (representing number of repair teams) and a less fundamental variable Yi (representing one kind of resource) affects the system performance. It can however not be seen how the simultaneous change of two or more less fundamental variables, Yi, Yj, Yk etc. (representing two or more different kinds of resources) would affect the systems performance. This is a draw-back of the method since in reality STSs are likely to continuously undergo change in multiple variables at once. For this reason it could be of interest to explore larger portions of the overall parameter space.

When determining the validity of the here presented results it should be emphasized that the presented method, although potentially useful for analysing resilience of a wide range of CIs, is at present only applicable for analysing disturbances affecting single electricity distribution systems. If a hazard scenario affects a wider region the results given by the here presented method will not be reliable. This is so since the method assumes that a practically infinite amount of resources will be available after between 12 and 24 hours, thanks to support from neighbouring municipalities. In case several regions are hit at once, as has for instance been the case after hurricane disasters in the past, this assumption will not hold true. In these cases the repair teams and repair resources that could have been supplied from neighbouring network operators will be likely to be unavailable. It should also be noted, concerning the validity of the model, that some simplifications have been made in the representation of the system. As was discussed in the previous chapter, only topology, but not capacity, is taken into account in the network model. This might lead to underestimation of both number of affected customers and outage time when the largest strain sizes are simulated. Another simplification that is made is that switching of breakers in the network in order to resupply customers is assumed to occur instantaneously. This in fact is not always the case since some breakers in the network are operated manually, meaning that an operator needs to travel to where the breaker is located. The assumption of instantaneous switching which is made is motivated by the fact that travel times can be disregarded in electricity distribution network due to their moderate size. Furthermore double stations, i.e. stations housing two sets of transformers were treated as single stations, i.e. the two transformers were treated as one. Furthermore satellite stations, i.e. stations in the periphery of the network that do not contain switch-gear, were treated as normal stations. They could therefore have switch-gear failures which in reality are not possible. Furthermore the possibility to use spare stations was not considered. In reality these can be used as a substitute for failed network stations and this will reduce the need for transformers and switch-gear. The possibility to use back-up power supply to supply customers was also disregarded. It should be of interest to take these issues into account in future research. If back-up power is taken into account the possibility to restore power to customers within 24 hours should be increased considerably. Another issue concerns the possibility of deriving deterministic results from probabilistic data. Data concerning repair times is in the form of intervals within which repair jobs are rectangle distributed. The justification for presenting deterministic results rather than results in the form of probability intervals is the convergence analysis that has been performed. In this analysis it was shown that the maximum restoration time, which is of interest here, had converged when the number of samples was 600. The analysis also showed that for the number of samples used here, 300, the result would have an uncertainty of a few hours. This uncertainty was reflected in the results, since it was seen that restoration time was in some cases slightly shorter for higher strain sizes, despite assuming the same amount of repair teams and resources.

## 6.7 Summary

Simulation of restoration processes previously done by (Tabucchi et al., 2008; Tabucchi et al., 2010) has in this chapter been used to address four issues crucial for analysing resilience of CIs, buffering capacity, flexibility, margin and tolerance. Using the method a number of decision variables, number of repair workers and amount of different kinds of materiel, can be evaluated with respect to achieving a desired safety goal. The method can thereby provide support concerning design of resilient CIs. The case study used in present paper concerned an electrical distribution system but the method could potentially be of use for a wide range of CIs.

# Chapter 7

# Discussion

In the three previous chapters the research results of the thesis work have been presented. In this chapter it is discussed how well these results fulfil the overarching objectives of the thesis. It is also explained in what way the results contribute to meet challenges within the CI research field. Possible improvements are discussed as well.

## 7.1 Fulfillment of the research objective

As was stated in 1.2 the objective of this thesis is to develop methods that can be used to:

1. Analyse societal consequences from disruptions of CI networks;

2. Analyse safety boundaries for CIs based on simulation of CI restoration processes.

It was furthermore proposed that these objectives can best be reached by simultaneously modelling three separate system domains: the network, the repair system and society. Three main research activities have been presented in this thesis (in Chapters 4, 5 and 6 respectively). Chapter 4 is concerned with all three system domains while Chapters 5 and 6 cover only a part of the three system domains (see Figure 1.3). Below each of the three main research activities is discussed under a separate heading.

### Review of STS models

In the review of approaches for simulating STSs (Chapter 4) it was found that none of the identified approaches for simulating STSs had been used for simultaneously simulating three aspects that are crucial for performing risk and vulnerability analysis of CIs:

a) socio-technical factors as a cause of critical infrastructure disruptions;

b) restoration processes concerning critical infrastructure and;

c) societal consequences from infrastructure disruptions.

These three aspects can be connected to the three system domains that are of interest in this thesis. Simulation of restoration processes is clearly related to the CI repair system and societal consequences from CI failures has an obvious relationship to society. The aspect of socio-technical factors as a cause of critical infrastructure disruptions is related to both the repair and the network system domains. In the review no papers were found that treated the three aspects, and also at present no such literature has been identified by the author. In the review it was also concluded that a hybrid model drawing primarily on agent based and network theory modelling, but perhaps also using other modelling approaches, could be of use for achieving the overarching objective.

### Comparing measures of consequences from power outages

In the work concerning comparisons of measures of societal consequences from power outages (Chapter 5) it was analysed to what extent Styrel assessments as well as the outage compensation regulation are in agreement. It was found that there was a close agreement between the results given by the two measures only for single component failures. Furthermore it was found that it the scenarios in which top priority customers are affected by outages lowers the rank correlation. For this reason it was suggested that these customers should be treated separately in the outage compensation regulation. Styrel assessments were used as an indicator of societal consequences from power outages. The Styrel assessments are advantageous in this respect since a distinction is made between consumers depending on how critical they are for society. Three main issues should however be considered if the Styrel assessments are to be used in the future as a measure of societal consequences from power outages: the importance of time as a determinant of societal consequence, the possibility of deriving quantitative results from the Styrel assessments and the degree to which Styrel assessments take CI interdependencies into account. Concerning the first issue it can be concluded that the time duration of the outage affects the result. In the research presented in Chapter 5 it was assumed that the time duration of the outage is constant. This is a simplification since in fact outage times will vary among different customers. In order to improve the representation of the societal consequences the model of the repair system, presented in this thesis, can be used to obtain the outage times in different parts of the network.

The second issue that should be kept in mind when Styrel assessments are used to estimate societal consequences has to do with the possibility of deriving quantitative results from the Styrel assessments. This mainly concerns the use of weights. When the Styrel system is used to weigh customers against each other based on their respective number of points, as in this thesis and in the studied municipality, this seems to give too much weight to normal customers in relation to customers with medium priority. The implication of the weights is for instance that 4 normal households, which have 1 point each, are as critical to society as a large industrial facility. Similarly, it implies that an outage suffered by 7 households have equal societal importance as that suffered by one customer that has large impact on the functioning of society in the short time span. It can be doubted if these weights are useful as indicators of societal importance of customers. Rather than summing up the weights of the affected customers it could be preferable to instead draw conclusions only from the definition of the priority categories and the time durations of the outage (provided by the model of the repair system). The definition of power consumers with priority 1 is that they have a large impact on life and health in a short time span (hours). Similarly the definition of power consumers with priority 2 is that they have a large impact on the functioning of society in a short time span (hours). Based on these definitions it can be concluded that if at least one customer with priority 1 is without power during several hours this will mean that life and health of the population is at risk while if at least one customer with priority 2 is without power during several hours this will mean that the functionality of society is likely to be degraded. While the advantage of this approach is that it does not require summing up weights of customers the draw-back is that it lumps together vastly different scenarios into a few categories: threatening/not threatening life and health and threatening/not threatening societal function.

The third issue concerns the degree to which the Styrel assessments take CI interdependencies into account. As pointed out by Shinozuka et al. (2003, p. 66), when analysing the consequences of power outages, it should be described how the loss of power "would affect households, businesses, and other units of society, not only directly but also indirectly through the cascading failure of other utilities". It is a stated aim of the Styrel system that interdependencies should be taken into account in the assessments that are made (Energimyndigheten, 2011, p. 18). Although this intention exists it can be doubted if the interdependencies have in fact been sufficiently covered when the Styrel assessments were made. Potentially the chains of causation can extend far beyond the primary and secondary consequences. When such long chains of causation are put into play analysis by the unaided human mind becomes difficult if not impossible. In order to take into account indirect effects and cascades occurring among actors in society it can therefore be necessary to use approaches involving computer simulation. The analysis of flows as performed by Améen & Andersson (2013) and Lindström & Wikman (2013) as well as work done by Setola et al. (2009) could be of interest, since these authors have demonstrated the possibility of using computer simulation to analyse the issue of cascading failures among CIs. It could be useful to compare the result given by computer based analysis approaches such as these with the Styrel assessments.

**Analysing electricity distribution system restoration processes**

Simulations were performed of an electricity distribution repair system (Chapter 6), a system that has a key role in maintaining the resilience of society with respect to disturbances in the electricity distribution system. Several authors have previously simulated infrastructure restoration processes (e.g. Tabucchi et al., 2008; Tabucchi et al., 2010). A benefit of the approach presented here is that it makes it possible to address four issues that are crucial for analysing resilience of CIs in accordance to Woods (2006): 1) buffering capacity, 2) flexibility, 3) margin to a performance boundary and 4) tolerance. Three issues should be considered if the simulation approach used in Chapter 6 is to be used further: firstly whether or not geography should be included in the model, secondly what levels of the STS that should be included in the model and thirdly with what level of detail the agents should be rendered. Concerning the first issue the model used in the research work did not take geography into account. However in an agent model that was created using NetLogo 5.0.4 (Wilensky, 1999) geography was considered. In the NetLogo model failures are located in space and the agents need to travel in order to reach them. The reason for not taking geography into account in the model that was used in this research work is that the system that is studied is a municipal distribution system supplying a relatively small city and since the distances are so short travel times can be disregarded. If on the other hand an entire region was studied, for instance the area affected by the Hurricane Gudrun, travel times would have to be taken into account due to the longer distances that need to be traversed by repair workers.

The second issue that should be considered is what levels of the STS that should actually be included in the model. In the method that was used in Chapter 6 only the two lowest levels, technology and operator, in the STS hierarchy that Rasmussen (1997) suggests is actually included. One reason for focusing on the two lowest levels is that the higher levels, such as management, legislative and governmental are in many cases hard to treat with quantitative approaches, although system dynamics has in some cases been used to simulate such higher organizational levels. Since quantitative approaches were aimed for in the present research it was decided to focus on the operator and technology levels. The method presented in Chapter 6 can be used to analyse what number of personnel and resources that is needed in order to attain a desired level of safety. This kind of analysis appears to be possible to carry out without taking higher levels of the STS into account. However, if we want to understand not only what configuration of system parameters that is safe but also the kind of dynamics that leads to the adoption of a certain safe or non-safe set of system parameters higher levels within the STS hierarchy will have to be taken into account.

The third issue that should be considered concerning simulation of restoration processes is the level of detail that should be used when rendering repair workers in the restoration model. In the model that was used here repair teams are more similar to machines than the human beings actually responsible for the repair work. They always work at the same pace, they don't make mistakes, and there is no limit to how long they can keep on working. As was described in Chapter 4 some ABMs have made considerable progress towards rendering human psychology in a realistic way. Some for instance take into account psychological traits such as trust, fear and expressiveness (e.g. Ferscha et al., 2011; Zia et al., 2011; Sharpanskykh, 2011). Similarly in work that has been done using SHELL (Cacciabue et al., 2003) it has been shown in what way the value of a large number of performance influencing factors (such as fatigue, motivation and stress of the operators) changes during the performance of a maintenance task. Further discussions should be held with the employees at the DSO in order to find out to what extent these factors are in fact affecting restoration processes. If these factors are indeed influencing the restoration processes to a high degree the restoration model should be adapted so that such factors are taken into account. Through interviews with experts it could be assessed how stress, fatigue and motivation is affected by working conditions such as duration or kind of work or the level of education of the repair workers and conditions of leadership. It could further be asked how the ability of repair workers to perform repair work quickly and correctly is affected by factors such as stress, fatigue and motivation. In this way a much more human-like representation could be achieved. The results given by a model such as this would be likely to be less optimistic, i.e. when repair teams can no longer work around the clock without loss of efficiency and accuracy this will lead to longer restoration times.

**Achievement of the research objective**

The overarching objective has been reached since the two methods that were demanded have been developed. However the three domains - network, repair system and society - that were covered in the research work have so far not been simulated within one modeling framework. It could be of interest to unite the simulation domains more intimately and the possibility of doing this is described in section 8.2.

## 7.2 Contributions to the research field

As was said in the introduction of this thesis several researchers argue that new methods are needed for making advances concerning analysis of CIs and their vulnerabilities (Rasmussen, 1997; Leveson, 2004; Hansman et al., 2006; Qureshi, 2007; Johnsson et al., 2013). The methods that have been presented here, see Chapter 5 and 6, enables estimation of consequences from power outages and estimation of outage time for electric distributions systems respectively. Concerning the work on estimation of societal consequences presented in Chapter 5 it is not known to the author that Styrel assessments have ever been used in the research literature to assess societal consequences from power outages, and if this has in fact not been done before it should be considered a contribution to the research field. Concerning the work on simulation of restoration processes presented in Chapter 6, simulation of restoration processes has been done before (e.g. Tabucchi et al., 2008; Tabucchi et al., 2010). However, in contrast to work done previously, the method presented here uses simulation to perform sensitivity analyses, thereby showing for what system parameter values that a certain restoration time can be attained. This functionality is answering to needs that have been voiced by researchers in the resilience engineering field (e.g. Rasmussen, 1997; Woods, 2006).

The method for simulating restoration processes takes into account the fact that the electricity distribution system is a STS and it accordingly explicitly represents the technical network at the core of the system as well as the repair system responsible for restoring the functionality of the network in case of failure. The method presented in Chapter 6 does not suffer from the limitation that Qureshi (2007) points out in traditional accident models, i.e. that they don't take into account the kind of accident causation that is typical for STSs, namely those where the cause cannot be attributed to a single component failure or human error, but rather to the interaction of technical, human and organizational factors. In the presented analysis the combined effect of technical component failures and shortages of repair workers or repair resources can be analysed, thereby bridging the gap between technical and organizational factors.

Hansman et al. (2006) suggests that in order to handle CIs integrated socio-technical models are needed. Little (2004) similarly suggests that a holistic strategy is appropriate for meeting the challenges of CI analysis. In such a holistic strategy technology, people and institutions should be included in the model. In this thesis a socio-technical model has been presented. It is not holistic, however, in the sense that all organizational levels of the STS are included in the model. Hansman et al. points out that the model should usefully describe the interactions between the technical infrastructure and its social context. This has here been achieved by using Styrel assessments as a proxy for the societal criticality of power customers.

The presented methods are intended to enable vulnerability analysis and therefore not so much has been said concerning concrete threats. As suggested in the introduction it was hard to predict the World Trade Center bombing prior to the actual event, and most likely today it is equally hard to predict the next major catastrophic event. This is a reason for using the kind of approach that has been presented here, namely one where vulnerability and resilience rather than risk and threat is at the centre of attention. No matter what threat that is realised, if it is terrorist bombings, a hacker attack, a major industrial accident, or a natural disaster such as a storm, a flood, a solar storm, a volcanic eruption or an earth-quake, the integrity of the CI systems will be at risk and it will be of crucial importance that the functionality of the CI systems can either be maintained or, if not, be restored within the required time. The work presented in this thesis enables analysis of these general issues and could therefore be useful for enabling preparations for a wide variety of foreseeable as well as unforeseeable threats.

# Chapter 8

# Conclusions

In the previous chapter the results of the thesis were discussed and related to the CI research field. In this last chapter conclusions from the thesis are given, beginning with a summary of the thesis. Possibilities for future work are discussed as well.

## 8.1 Summary of the thesis

In this thesis two methods have been presented, one for comparing societal consequences from disruption in electricity distribution systems and one for analysing restoration times in electricity distribution systems. The methods involve three separate system domains: repair system, network and society. The advantage of modelling these three domains is the following: the network model enables analysis of possible component failure and their consequences for the networks functionality, the repair system model enables analysis of the time duration of functionality loss of the network, and the society model finally makes it possible to determine the societal consequence of a network functionality loss of a certain magnitude and duration.

A review of work that has been done on simulation of STSs was performed (Chapter 4) and it was found that none of the identified papers presented a method in which three aspects, that are of interest for analysing risk and vulnerability of CIs, are simultaneously simulated. It was thus indicated that research remains to be done within this field. Based on the review it appeared that a hybrid model combining network theory modeling and agent based modeling would be well-suited for simulating the three system domains. In the method that was later developed and used in the research work presented in Chapter 6 a hybrid modelling approach is in fact used, in which network theory modelling and a queuing theory model drawing on agent based modelling are combined.

A case-study was carried out for a power distribution system in a municipality in southern Sweden where two ways of measuring societal consequences from power outages were contrasted (Chapter 5); one based on outage compensation and the other on the Styrel assessments. It was argued that the main draw-back of using the outage compensation regulation for this purpose is that it does not distinguish between critical and non-critical electricity customers since it only takes into account the fee the customer pays to the DSO. The Styrel system however distinguishes between critical and non-critical customers which makes it advantageous for assessing overall societal consequences from power outages.

The same municipal distribution system was also used in a case-study where outage times were analysed (Chapter 6). Sensitivity analyses were performed of outage time with respect to a number of decision variables: amounts of available resources and repair personnel. The method enables analysis of four crucial issues within resilience engineering: buffering capacity, flexibility, margin and tolerance. Based on the analysis results it can be seen what amount of resources and repair teams that will be required to achieve restoration within the required time in case of different magnitudes of strain on the network. In this way the method can support design of resilient CIs.

## 8.2 Future work

Two methods have been developed, each focusing on one part of the STS that CIs can be said to constitute. A possible future research task is to combine these two methods. Chapter 5 in this thesis describes how the network and society domains can be represented in a modelling context and Chapter 6 describes how the network and repair system domains can be simulated. In the future research these two parts should be bridged (See Figure 8.1).

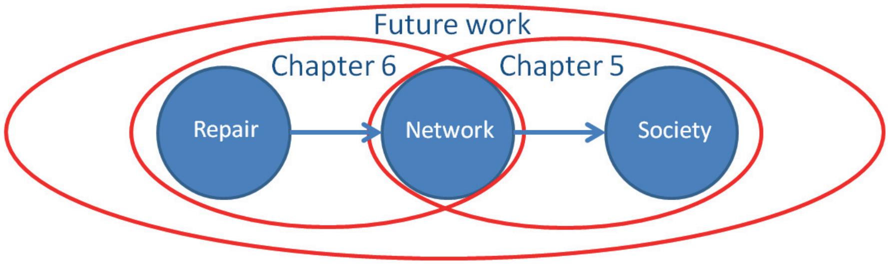


Figure 8.1: In the future research domains simulated separately in Chapter 5 and 6 will be bridged.

When this unification has been achieved an analysis similar to that presented in Chapter 6 can be performed, but whilst safety was here defined as "no customer is without power for longer than 24 hours" this safety definition that is based in Swedish law can then be contrasted against one that is based on the actual consequences of the outage. A safety definition of the latter kind could be one of the following:

1) No customer that is critical to life and health within hours (priority 1 customer) is without power for more than one or a few hours and no customer that is critical to life and health within days (priority 3 customer) is without power for more than one or a few days

2) No customer that is critical to the functionality of society within hours (priority 2 customer) is without power for more than one or a few hours and no customer that is critical to the functionality of society within days (priority 4 customer) is without power for more than one or a few days

If safety definition 1) is chosen we identify the area in the parameter space where life and health is not at risk for different magnitudes of strain on the network. If safety definition 2) is chosen we instead identify the area where the functionality of society is not at risk.

Another research track concerns applying the developed methodologies to other CIs in order to test its applicability. Work is today ongoing concerning applying the method described in Chapter 6 to a computer network. The goal is to identify safety limits concerning repair personnel and amount of spare parts. Another research track is concerned with capability assessment, meaning the assessment of the ability of actors in society to meet their objectives. Capability assessments are widely used in Sweden, but it is still far from clear how capability should be measured (Palmqvist et al., 2012). The method presented in Chapter 6 can in fact be seen as a means for performing capability assessments. In the case study the capability of an electricity distribution repair system to restore a network after a disruption was studied, as well as how this capability depends on decision variables. However, the method should be relatively easy to apply for analysing capability of other systems, for instance rescue services. A possible future research track is to investigate the general applicability of the method presented in Chapter 6 for assessing capability of actors critical for society.

Moving further into the future it is possible to expand the research project concerning its scope as well as its depth. Concerning the scope it will be of interest to move beyond analysing only the electricity distribution system and to study a number of interdependent CIs, each constituting a part of an overall System of Systems. Experiences from the hurricane Gudrun and other major hurricanes have shown that CI dependencies have major consequences for the functionality of the repair system. Roads need to be cleared from fallen trees in order to create access to failed components in the electricity network. The telecommunication network also stops working when the electricity supply is lost and since this system is needed to enable communication between repair teams and other parts of the organization the repair work is made more difficult. In the present research no CI dependencies were analysed, but it should be of interest to take this aspect into account in future research. Examples of systems that could be of interest in this respect are the transportation system, water and telecommunication. This work could build on research by Johansson (2010) and Johansson et al. (2011). When the systems are studied within one model possibilities open up for investigating a range of complex interrelationships which could give rise to unexpected behaviour. In Figure 8.2 possible dependencies between a number of CIs and their respective repair systems are indicated. All of these dependencies could be of crucial importance for the System of Systems ability to recover its functionality after a major disruption and research in this area can therefore provide deeper understanding concerning vulnerability of society with respect to disturbances of CI systems.

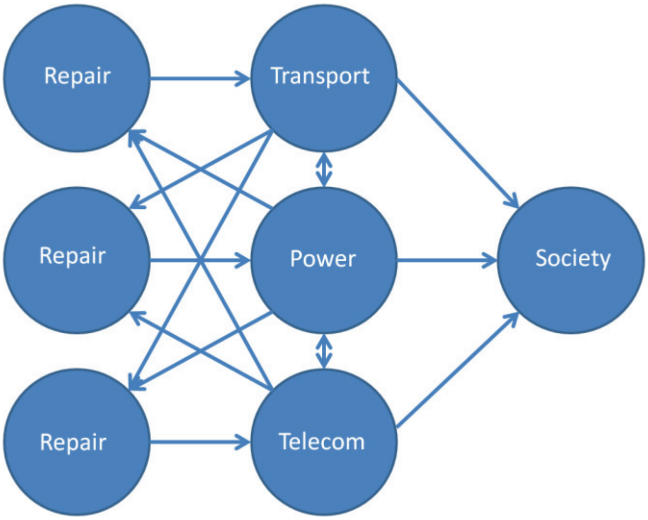


Figure 8.2: Possible interdependencies between CIs.

Concerning the depth of the research work it will be of interest to investigate individual repair systems in more detail. So far the repair system has been represented in a fairly abstract way. For the future it will be interesting to represent the repair workers less like servers in a queuing system and more like autonomous individuals. The agent based approach that has been used can be developed in this way more easily thanks to its modular structure.

The research can also gain in depth concerning the way that society is represented. Insight concerning the societal domain has so far been gained by using the Styrel assessments. One limitation of using the Styrel assessments, which was mentioned in section 7.1, is that it is not clear to what extent it takes the effects of cascading failures among CIs into account. For the future it will be of interest to compare the Styrel assessments with assessment derived through explicit simulations of cascading failures among CIs. The flow analysis method used by Améen & Andersson (2013) and Lindström & Wikman (2013) could be of use in this respect. The author has found no research that investigates the validity of the Styrel assessments in the research literature. It should be of interest to fill this apparent gap.

As has been indicated several possibilities for future research exists within the branch of the CI research field investigated here. Also, there should be no doubt that the future still has many challenges in store for us, and the majority of them are likely to be unknown to us at present. An assumption that has guided and motivated the research presented in this thesis is that armed with methods of the kind suggested here we will stand a somewhat better chance against the challenges that the future can bring. It has also been the intention that the research presented here should help bring forth a very different, more liveable world.

# References

Ajodhia, V., & Hakvoort, R. (2005) ‘Economic regulation of quality in electricity distribution networks’, *Utilities Policy*, Vol. 13, No. 3, pp. 211-221.

Allison, G. (2004) *Nuclear terrorism: The ultimate preventable catastrophe*, Henry Holt and Company, New York, US.

Améen, E., & Andersson, A. (2013) ’Beroendeanalys ur ett flödesperspektiv’, Master thesis Lund University, In Swedish.

Bader, G. D., Betel, D., & Hogue, C. W. (2003) ‘BIND: the biomolecular interaction network database’, *Nucleic acids research*, Vol. 31, No. 1, pp. 248-250.

Balducci, P. J., Roop, J. M., Schienbein, L. A., DeSteese, J. G., & Weimar, M. R. (2002) ‘Electrical power interruption cost estimates for individual industries, sectors and US economy’, *Pacific Northwest National Laboratory*.

Balijepalli, N., Venkata, S. S., Richter Jr, C. W., Christie, R. D., & Longo, V. J. (2005) ‘Distribution system reliability assessment due to lightning storms’, *IEEE Transactions on Power Delivery*, Vol. 20, No. 3, pp. 2153-2159.

Barrett, C. L., Eubank, S., Kumar, V. A., & Marathe, M. V. (2004) ‘Understanding large scale social and infrastructure networks: A simulation based approach’, *SIAM news*, Vol. 37, No. 4, pp. 1-5.

Basnyat, S,, Palanque, P., Schupp, B., & Wright, P. (2007) ‘Formal socio-technical barrier modelling for safety-critical interactive systems design’, *Safety Science*, Vol. 45, No. 5, pp. 545–565.

Bonabeau, E. (2002) ‘Agent-based modelling: Methods and techniques for simulating human systems’, *Proceedings of the National Academy of*

*Sciences of the United States of America*, Vol. 99, No. 3, pp. 7280-7287.

Bendrath, R. (2001) ‘The cyberwar debate: Perception and politics in US critical infrastructure protection’, *Information & security*, Vol. 7, No., pp. 80-103.

Bertoli, P., Cimatti, A., Pistore, M., & Traverso, P. (2003) ‘A Framework for Planning with Extended Goals under Partial Observability’, *ICAPS,* pp. 215-225.

Bird, C., Nagappan, N., Gall, H., Murphy, B., & Devanbu, P. (2009) ‘Putting it all together: Using socio-technical networks to predict failures’, *ISSRE'09*, *20th International Symposium on Software Reliability Engineering*, pp. 109-119.

Bird, C., Nagappan, N., Gall, H., Murphy, B., & Devanbu, P. (2009) ‘Putting It All Together: Using Socio-technical Networks to Predict Failures’, *20th International Symposium on Software Reliability Engineering*, pp. 109–119, IEEE.

Bozic, Z. (2000) ‘Customer interruption cost calculation for reliability economics: practical considerations’, *International Conference on Power System Technology, Proceedings. PowerCon 2000*, Vol. 2, pp. 1095-1100, IEEE.

Brandt, D., Hartmann, E., Sander, C., & Strina, G. (1999) ‘Designing and simulating sociotechnical systems: Concepts and strategies’, *Human Factors and Ergonomics in Manufacturing & Service Industries*, Vol. 9, No. 3, pp. 245-252.

Brown, R. E., Gupta, S., Christie, R. D., Venkata, S. S., & Fletcher, R. (1997) ‘Distribution system reliability assessment: momentary interruptions and storms’, *IEEE Transactions on Power Delivery*, Vol. 12, No. 4, pp. 1569-1575.

Cacciabue, P. C., Mauri, C., & Owen, D. (2003) ‘The development of a model and simulation of an aviation maintenance technician task performance’, *Cognition, Technology & Work*, Vol. 5, No. 4, pp. 229-247.

Balijepalli, N., Venkata, S. S., Richter Jr, C. W., Christie, R. D., & Longo, V. J. (2005) 'Distribution system reliability assessment due to lightning storms', *IEEE Transactions on Power Delivery*, Vol. 20, No. 3, pp. 2153-2159.

Cavdaroglu, B., Hammel, E., Mitchell, J. E., Sharkey, T. C., & Wallace, W. A. (2013) 'Integrating restoration and scheduling decisions for disrupted interdependent infrastructure systems', *Annals of Operations Research*, Vol. 203, No. 1, pp. 279-294.

Coffrin, C., Van Hentenryck, P., & Bent, R. (2012) 'Last-Mile Restoration for Multiple Interdependent Infrastructures', *Proceedings of twenty-sixth AAAI Conference on Artificial Intelligence*, pp. 445-463.

Collier, S., & Lakoff, A. (2008) 'The vulnerability of vital systems: How 'critical infrastructure' became a security problem The Politics of Securing the Homeland: Critical Infrastructure', *Risk and Securitisation*, pp. 40-62.

Comfort, L. K., Boin, A. & Demchak, C. C., (Ed.) (2010) *Designing Resilience*, University of Pittsburgh Press, Pittsburgh, US.

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

David, R., Alla, H., (2005) *Discrete, Continuous, and Hybrid Petri Nets*, Springer, Berlin, Germany.

De Bruijne, M., & Van Eeten, M. (2007) 'Systems that should have failed: critical infrastructure protection in an institutionally fragmented environment', *Journal of Contingencies and Crisis Management*, Vol. 15, No. 1, pp. 18-29.

De Nooij, M., Koopmans, C., & Bijvoet, C. (2007) 'The value of supply security: The costs of power interruptions: Economic input for damage reduction and investment in networks', *Energy Economics*, Vol. 29, No. 2, pp. 277-295.

Ducheneaut, N. (2005) ‘Socialization in an Open Source Soft-ware Community: A Socio-Technical Analysis’, *Computer Supported Cooperative Work*, Vol. 14, No. 4, pp. 323–368.

Edwards, P. N. (2003) *Infrastructure and modernity: Force, time, and social organization in the history of sociotechnical systems*, In *Modernity and technology*, Massachusetts Institute of Technology, Boston, US, pp. 185-225.

Ei (2014) ’Bättre och tydligare reglering av elnätsföretagens intäktsramar Förslag till ändringar i förordningen om fastställande av intäktsram inför tillsynsperioden 2016 – 2019’, In Swedish.

Ei (2011) ’Ram för elnätföretagens avgifter – Förhandsreglering’, In Swedish.

Ei (2010) ’Kvalitetsbedömning av elnät vid förhandsreglering’, In Swedish.

El-Gharbawi, J., Larsson, R. G., Molander, J., Yard, S., & Knops, V. (2011) ’Kvalitetsstyrningens påverkan av Energimarknadsinspektionens kvalitetsreglering’, Master Thesis Lund University, In Swedish.

Energimyndigheten (2011) ’Handbok för Styrel 2011 – Prioritering av samhällsviktiga elanvändare vid elbrist’, In Swedish.

Energimyndigheten (2012) ’Slutrapport från Energimyndighetens styrel-projekt’, In Swedish.

Epstein, J. M. (2006) *Generative social science: Studies in agent-based computational modeling*, Princeton University Press, Princeton, US.

Eusgeld, I., Kröger, W., Sansavini, G., Schläpfer, M., & Zio, E. (2009) ‘The role of network theory and object-oriented modelling within a framework for the vulnerability analysis of critical infrastructures’, *Reliability Engineering & System Safety*, Vol. 94, No. 5, pp. 954-963.

Ferscha, A., Zia, K., Riener, A., & Sharpanskykh, A. (2011) 'Potential of Social Modelling in Socio-Technical Systems', *Procedia Computer Science*, Vol. 7, pp. 235–237.

Finger, M., Groenwegen, J., & Kunneke, R. (2005) 'Quest for Coherence between Institutions and Technologies in Infrastructures', *The. J. Network Ind.*, Vol. 6, pp. 227-260.

Forrester, J. W., Mass, N. J., & Ryan, C. J. (1976) 'The system dynamics national model: understanding socio-economic behaviour and policy alternatives', *Technological Forecasting and Social Change*, Vol. 9, No. 1, pp. 51-68.

Greenberg, R., & Cook, S. (2006) 'A Generic BBN Safety Model', *2006 IEEE Symposium on Product Safety Engineering*, pp. 1–14.

Gregoriades, A., Sutcliffe, A., & Shin, J. E. (2003) 'Assessing the reliability of socio-technical systems', *Systems engineering*, Vol. 6, No. 3, pp. 210-223.

Grimvall, G., Jacobsson, P., & Thedéen, T. (2003) *Risker i tekniska system*. Studentlitteratur, Lund, Sweden, In Swedish.

Haanpää, S., Lehtonen, S., Peltonen, L., & Talockaite, E. (2006) 'Impacts of winter storm Gudrun of 7th–9th January 2005 and measures taken in Baltic Sea Region', *Astra Project*.

Han, J., Hayashi, Y., Cao, X., & Imura, H. (2009) 'Application of an integrated system dynamics and cellular automata model for urban growth assessment: A case study of Shanghai, China', *Landscape and Urban Planning*, Vol. 91, No. 3, pp. 133-141.

Hansman, R. J., Magee, C., De Neufville, R., & Robins, R. (2006) 'Research agenda for an integrated approach to infrastructure planning, design and management', *International journal of critical infrastructures,* Vol. *2,* No. 2, pp. 146-159.

Hassel, H. (2010) 'Risk and vulnerability analysis in society's proactive emergency management: Developing methods and improving practices', PhD thesis, Lund University.

Holmgren, Å. J. (2006) 'Quantitative vulnerability analysis of electric power networks', PhD thesis, Royal Institute of Technology.

Isumi, M., Nomura, N. & Shibuya, T., (1985) 'Simulation of post-earthquake restoration for lifeline systems', *International Journal of Mass Emergencies and Disaster*, pp. 87-105.

Johansson, J., Jönsson, H., Johansson, H. (2007), 'Analysing the vulnerability of electric distribution systems: a step towards incorporating the societal consequences of disruptions', *International Journal of Emergency Management*, Vol. 4 No. 1, pp. 4-17.

Johansson, J. (2010) 'Risk and vulnerability analysis of interdependent technical infrastructures', PhD thesis, Lund University.

Johansson, J., Hassel, H., & Cedergren, A. (2011) 'Vulnerability analysis of interdependent critical infrastructures: case study of the Swedish railway system', *International Journal of Critical Infrastructures*, Vol. 7, No. 4, pp. 289-316.

Johansson, J., Hassel, H., & Zio, E. (2013) 'Reliability and vulnerability analyses of critical infrastructures: Comparing two approaches in the context of power systems', *Reliability Engineering & System Safety*, Vol. 120, pp. 27-38.

Joslyn, C., & Rocha, L. (2000) 'Towards semiotic agent-based models of socio-technical organizations'. In *Proceedings of AI, Simulation and Planning in High Autonomy Systems (AIS 2000)* Tucson, Arizona, US, pp. 70-79.

Jönsson, H., Johansson, J., & Johansson, H. (2008) 'Identifying critical components in technical infrastructure networks', *Journal of Risk and Reliability*, Vol. 222, No. 2, pp. 235-243.

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

Kasperson, R. E., Renn, O., Slovic, P., Brown, H. S., Emel, J., Goble, R. & Ratick, S. (1988) 'The social amplification of risk: A conceptual framework', *Risk analysis*, Vol. 8, No. 2, pp. 177-187.

Kozin, F., & Zhou, H. (1990) 'System study of urban response and reconstruction due to earthquake', *Journal of Engineering Mechanics*, Vol. 116, No. 9, pp. 1959-1972.

Kroes, P., Franssen, M., Poel, I. V. D., & Ottens, M. (2006) 'Treating socio-technical systems as engineering systems: some conceptual problems', *Systems research and behavioural science*, Vol. 23, No. 6, pp. 803-814.

Lakervi, E., & Holmes, E. J. (1995) *Electricity distribution network design,* Institution of Electrical Engineers, London, UK.

Léger, a, Weber, P., Levrat, E., Duval, C., Farret, R., & Iung, B. (2009) 'Methodological developments for probabilistic risk analyses of socio-technical systems', *Journal of Risk and Reliability*, Vol. 223, No. 4, pp. 313–332.

Lee, S. M., Corker, K. & Pritchett, A. R. (2007) 'Evaluating transformations of the air transportation system through agent-based modelling and simulation', *Environment*, pp. 1-10.

Leveson, N. (2004) 'A new accident model for engineering safer systems', *Safety science*, Vol. 42, No. 4, pp. 237-270.

Lewis, T. G. (2006) *Critical infrastructure protection in homeland security: defending a networked nation*, John Wiley & Sons, Hoboken, New Jersey, US.

Linares, P., & Rey, L. (2013) 'The costs of electricity interruptions in Spain. Are we sending the right signals?' *Energy policy*, pp. 751-760.

Lindström, A., & Wikman, M. (2013) 'Beroendeanalys ur ett flödesperspektiv - Kartläggning och aggregering', Master thesis Lund University, In Swedish.

Little, R. G. (2004) 'Holistic strategy for urban security', *Journal of Infrastructure Systems*, Vol. 10, No.2, pp. 52-59.

Losa, I., Bertoldi, O. (2009) 'Regulation of continuity of supply in the electricity sector and cost of energy not supplied', *Enginet*.

Liu, H., Davidson, R. A., & Apanasovich, T. (2007) 'Statistical forecasting of electric power restoration times in hurricanes and ice storms', *IEEE Transactions on Power Systems*, Vol. 22, No. 4, pp. 2270-2279.

Lu, Y., Li, Q., & Song, L. (2012) 'Safety risk analysis on sub-way operation based on Socio-Technical Systems', *2012 International Conference on Quality, Reliability, Risk, Maintenance, and Safety Engineering*, pp. 180–184.

McDaniels, T., Chang, S., Cole, D., Mikawoz, J., & Longstaff, H. (2008) 'Fostering resilience to extreme events within infrastructure systems: Characterizing decision contexts for mitigation and adaptation', *Global Environmental Change*, Vol. 18, No. 2, pp. 310-318.

Meadows, D., Randers, J., & Meadows, D. (2004) *Limits to growth: the 30-year update*, Chelsea Green Publishing.

Mili, L., Krimgold, F., Alwang, J., & Bigger, J. E. (2004) *Integrating engineering, economic, and social modelling in risks of cascading failures across interdependent complex networks*, In *Probabilistic Methods Applied to Power Systems*, Pergamon Press, Oxford, UK, pp. 657-662.

Mohaghegh, Z., Kazemi, R., & Mosleh, A. (2009) 'Incorporating organizational factors into Probabilistic Risk Assessment (PRA) of complex socio-technical systems: A hybrid technique formalization', *Reliability Engineering & System Safety*, Vol. 94, No. 5, pp. 1000–1018.

Mohaghegh, Z. (2010) 'Combining System Dynamics and Bayesian Belief Networks for Socio-Technical Risk Analysis', *2010 IEEE International Conference on Intelligence and Security Informatics (ISI),* pp. 196-201.

Moteff, J., & Parfomak, P. (2004) 'Critical infrastructure and key assets: definition and identification', *Library of congress Washington DC congressional research service*.

MSB (2006) 'Faller en – faller då alla? En slutredovisning från KBM:s arbete med samhällskritiska beroenden', In Swedish.

Newitz, A. (2013) *Scatter, Adapt, and Remember*, Random House, Inc., New York, US.

Nikolic, I., & Dijkema, G. P. J. (2006) 'Shaping Regional Industry-Infrastructure Networks An Agent Based Modelling Framework', *IEEE International Conference on Systems, Man and Cybernetics*, pp. 901–905.

Olsson, G., & Rosen, C. (2005) *Industrial automation: applications, structures and systems*, Department of industrial electrical engineering and automation, Lund, Sweden.

O'Rourke, T. D. (2007) 'Critical infrastructure, interdependencies, and resilience', *Bridge-Washington-national academy of engineering*, Vol. 37, No. 1, pp. 22.

Ottens, M., Franssen, M., Kroes, P., & Van De Poel, I. (2006) 'Modelling infrastructures as socio-technical systems', *International Journal of Critical Infrastructures*, Vol. 2, No. 2, pp. 133-145.

Palmqvist, H., Tehler, H., Hassel, H., Svegrup, L., & Petersen, K. (2012) 'Utveckling av förmågebedömningar', *Rapport*, In Swedish.

Parunak, H. V. D., Savit, R., & Riolo, R. L. (1998) *Agent-based modeling vs. equation-based modeling: A case study and users' guide*, In Multi-agent systems and agent-based simulation (pp. 10-25) Springer, Berlin, Germany.

Pawson, R., Wong, G., & Owen, L. (2011) 'Known Knowns, Known Unknowns, Unknown Unknowns The Predicament of Evidence-Based Policy', *American Journal of Evaluation*, Vol. 32, No. 4, pp. 518-546.

Pestov, I., & Verga, S. (2009), 'Dynamical networks as a tool for system analysis and exploration, Computational Intelligence for Security and Defense Applications', *CISDA IEEE Symposium*, pp. 1-8, Ottawa, Canada.

Perrow, C. (2011) *The next catastrophe: Reducing our vulnerabilities to natural, industrial, and terrorist disasters*. Princeton University Press, Princeton, US.

Qureshi, Z. H. (2007) ‘A review of accident modelling approaches for complex socio-technical systems’, *Proceedings of the twelfth Australian workshop on Safety critical systems and software and safety-related programmable systems*, Vol. *86,* pp. 47-59, Mawson Lakes, South Australia.

Raesaar, E. P., Tiigimägi, E., & Valtin, J. (2006) ‘Assessment of electricity supply interruption costs under the restricted time and information resources’, *Proceeding of International Conference on Energy & Environment Systems IASME/WSEAS 2006,* pp. 409-415, Chalkida, Greece.

Railsback, S. F., & Grimm, V. (2011) *Agent-based and individual-based modeling: a practical introduction*, Princeton University Press, Princeton, US.

Ramaswamy, V., Thulasidasan, S., Romero, P., Eidenbenz, S., & Cuellar, L. (2007) ‘Simulating the national telephone network: A socio-technical approach to assessing infrastructure criticality’, *Military Communications Conference, MILCOM IEEE,* pp. 1-7, Orlando, US.

Rasmussen, J. (1997) ‘Risk management in a dynamic society: a modelling problem’, *Safety science,* Vol. *27*, No. 2, pp. 183-213.

Reed, D. A., Kapur, K. C., & Christie, R. D. (2009) ‘Method for assessing the resilience of networked infrastructure’, *Systems Journal, IEEE*, Vol. 3, No. 2, pp. 174-180.

Rees, M. (2013) ‘Denial of catastrophic risks’, *Science*, Vol. 339, No. 6124, pp. 1123.

Rocco, C. M., Ramirez-Marquez, J. E., & Salazar, D. E. (2012) ‘Some metrics for assessing the vulnerability of complex networks: An application to an electric power system’, *Advances in Safety, Reliability and Risk Management*, pp. 2556-2561.

Sappington, D. E., Pfeifenberger, J. P., Hanser, P., & Basheda, G. N. (2001) ‘The state of performance-based regulation in the US electric utility industry’, *The Electricity Journal*, Vol. 14, No. 8, pp. 71-79.

Schläpfer, M., Kessler, T., & Kröger, W. (2012) 'Reliability analysis of electric power systems using an object-oriented hybrid modelling approach', *arXiv preprint*:1201.0552.

Setola, R., De Porcellinis, S., & Sforna, M. (2009) 'Critical infrastructure dependency assessment using the input–output inoperability model', *International Journal of Critical Infrastructure Protection*, Vol. 2, No. 4, pp. 170-178.

Shah, A. P., & Pritchett, A. R. (2005) *Work-environment analysis: Environment centric multi-agent simulation for design of socio-technical systems*, In *Multi-Agent and Multi-Agent-Based Simulation*, pp. 65-77, Springer, Berlin, Germany.

Shannon, P., Markiel, A., Ozier, O., Baliga, N. S., Wang, J. T., Ramage, D. & Ideker, T. (2003) 'Cytoscape: a software environment for integrated models of biomolecular interaction networks', *Genome research*, Vol. 13, No. 11, pp. 2498-2504.

Sharpanskykh, A. (2010) *Integrated modelling of cognitive agents in socio-technical systems* In *Agent and Multi-Agent Systems: Technologies and Applications*, pp. 262-271, Springer, Berlin, Germany.

Sharpanskykh, A. (2011) 'Agent-Based Modelling and Analysis of Socio-Technical Systems', *Cybernetics and Systems*, Vol. 42, No. 5, pp. 308–323.

Shinozuka, M., Chang, S. E., Cheng, T. C., Feng, M., O'Rourke, T. D., Saadeghvaziri, M. A., Dong, X., Jin, X. Wang, Y. & Shi, P. (2003) 'Resilience of integrated power and water systems'. *Multidisciplinary Center for Earthquake Engineering Research*.

Shinozuka, M., Rose, A., & Eguchi, R. (1998) 'Engineering and socioeconomic impacts of earthquakes', *Engineering and socioeconomic impacts of earthquakes*.

Smith, E. R., & Conrey, F. R. (2007) 'Agent-based modelling: a new approach for theory building in social psychology', *Personality and* *social psychology review: an official journal of the Society for Personality and Social Psychology, Inc*, Vol. 11, No. 1, pp. 87–104.

Strandén, J., Krohns, H., Verho, P., & Sarsama, J. (2010) 'Modelling the interruption criticality of customers of distribution networks', In *The 9th Nordic Electricity Distribution and Asset Management Conference 2010, NORDAC 2010*, Aalborg, Denmark.

Tabucchi, T. H. P., Davidson, R. A., & Brink, S. (2008) 'Restoring the Los Angeles water supply system following an earthquake', In *14th World Conference on Earthquake Engineering*.

Tabucchi, T., Davidson, R., & Brink, S. (2010) 'Simulation of post-earthquake water supply system restoration', *Civil Engineering and Environmental Systems*, Vol. 27, No. 4, pp. 263-279.

Tahvanainen, K., Viljainen, S., Honkapuro, S., Lassila, J., Partanen, J., Järventausta, P., & Mäkinen, A. (2004) 'Quality regulation in electricity distribution business', In *Nordic distribution and asset management conference* pp. 23-24.

Trist, E. (1980) 'The evolution of socio-technical systems', *Conference on organizational design and performance*, Pennsylvania, US.

Tsvetovat, M., & Carley, K. M. (2004) 'Modelling complex socio-technical systems using multi-agent simulation methods'. *Kuenstliche Intelligenz*, Vol. 18, No. 2, pp. 23-28.

Walski, T. M., Brill, E. D. Jr., Gessler J., Goulter, I. C., Jeppson, R. M., Lansey, K., Lee, H., Liebman, J. C., Mays, L., Morgan, D. R. & Ormsbee, L., (1987) 'Battle of the Network Models: Epilogue', *Journal of Water Resources Planning and Management*, Vol. 113, No. 2, pp. 191-203.

Wiener, E. L., & Nagel, D. C. (Eds.) (1988) *Human factors in aviation,* Academic Press, San Diego, US.

Wilensky, U. (1999) {NetLogo}.

*social psychology review : an official journal of the Society for Personality and Social Psychology, Inc*, Vol. 11, No. 1, pp. 87–104.

Strandén, J., Krohns, H., Verho, P., & Sarsama, J. (2010) 'Modelling the interruption criticality of customers of distribution networks', In *The 9th Nordic Electricity Distribution and Asset Management Conference 2010, NORDAC 2010*, Aalborg, Denmark.

Tabucchi, T. H. P., Davidson, R. A., & Brink, S. (2008) 'Restoring the Los Angeles water supply system following an earthquake', In *14th World Conference on Earthquake Engineering*.

Tabucchi, T., Davidson, R., & Brink, S. (2010) 'Simulation of post-earthquake water supply system restoration', *Civil Engineering and Environmental Systems*, Vol. 27, No. 4, pp. 263-279.

Tahvanainen, K., Viljainen, S., Honkapuro, S., Lassila, J., Partanen, J., Järventausta, P., & Mäkinen, A. (2004) 'Quality regulation in electricity distribution business', In *Nordic distribution and asset management conference* pp. 23-24.

Trist, E. (1980) 'The evolution of socio-technical systems', *Conference on organizational design and performance*, Pennsylvania, US.

Tsvetovat, M., & Carley, K. M. (2004) 'Modelling complex socio-technical systems using multi-agent simulation methods'. *Kuenstliche Intelligenz*, Vol. 18, No. 2, pp. 23-28.

Walski, T. M., Brill, E. D. Jr., Gessler J., Goulter, I. C., Jeppson, R. M., Lansey, K., Lee, H., Liebman, J. C., Mays, L., Morgan, D. R. & Ormsbee, L., (1987) 'Battle of the Network Models: Epilogue', *Journal of Water Resources Planning and Management*, Vol. 113, No. 2, pp. 191-203.

Wiener, E. L., & Nagel, D. C. (Eds.) (1988) *Human factors in aviation,* Academic Press, San Diego, US.

Wilensky, U. (1999) {NetLogo}.

Wildavsky, A. B. (1988) *Searching for safety,* Transaction publishers, New Jersey, US.

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

Winner, L. (2004) 'Trust and terror: the vulnerability of complex socio-technical systems', *Science as Culture,* Vol. 13, No. 2, pp. 155-172.

Woo, C. K., & Pupp, R. L. (1992) 'Costs of service disruptions to electricity consumers', *Energy*, Vol. 17, No. 2, pp. 109-126.

Woods, D. D. (2006) *Essential characteristics of resilience*. In *Resilience engineering: concepts and precepts*, Ashgate publishing company, Burlington, US, pp. 21-34.

Xu, N., Guikema, S. D., Davidson, R. A., Nozick, L. K., Çağnan, Z., & Vaziri, K. (2007) 'Optimizing scheduling of post-earthquake electric power restoration tasks', *Earthquake engineering & structural dynamics*, Vol. 36, No. 2, pp. 265-284.

Yusta, J. M., Correa, G. J., & Lacal-Arántegui, R. (2011) 'Methodologies and applications for critical infrastructure protection: State-of-the-art', *Energy policy*, Vol. 39, No. 10, pp. 6100-6119.

Zhang, R. H. (1992) 'Lifeline interaction and post-earthquake urban system reconstruction', *In Proc of 10th World Conference on Eearthquake Engineering*, Vol. 5, pp. 5475-5480.

Zia, K., Ferscha, A., Riener, A., Wirz, M., Roggen, D., Kloch, K., & Lukowicz, P. (2010) 'Scenario based modelling for very large scale simulations', *Proceedings of the 2010 IEEE/ACM 15th International Symposium on Distributed Simulation and Real Time Applications*, pp. 103-110.

Zia, K., Riener, A., Ferscha, A., & Sharpanskykh, A. (2011) 'Evacuation Simulation based on Cognitive Decision making model in a Socio-Technical System', *Proceedings of the 2011 IEEE/ACM 15th*

*International Symposium on Distributed Simulation and Real Time Applications*, pp. 98-107.

# Abbreviations

| Acronym | Concept |
|---|---|
| ABM | Agent Based Model |
| BBN | Bayesian Belief Network |
| CI | Critical Infrastructure |
| DES | Descrete Event Simulation |
| DRC | Deterministic Resource Constraint |
| DSO | Distribution System Operator |
| ECF | Empirical Curve Fitting |
| Ei | Energy Markets Inspectorate |
| HM | Hybrid Model |
| MCS | Monte Carlo Simulation |
| MP | Markov Process |
| NTM | Network Theory Model |
| OA | Optimization Approach |
| ONR | Outage compensation Normalized Rank |
| PN | Petri Net |
| RVA | Risk & Vulnerability Analysis |
| SD | System Dynamics |
| SHELL | Software Hardware Environment Liveware Liveware |
| SNR | Styrel Normalized Rank |
| SR | Statistical Regression |
| STS | Socio-Technical System |
| WTA | Willingness To Accept |
| WTP | Willingness To Pay |