Risk and vulnerability analysis in society's proactive emergency management: Developing methods and improving practices

Hassel, Henrik

2010

Risk and vulnerability analysis in society's proactive emergency management

Developing methods and improving practices

Henrik Hassel

LUND UNIVERSITY

Doctoral thesis

Department of Fire Safety Engineering and Systems Safety
Faculty of Engineering

Lund 2010

Risk and Vulnerability analysis in society's proactive emergency management: developing methods and improving practices
Henrik Hassel

Report 1045
ISSN 1402-3504
ISRN LUTVDG/TVBB--1045--SE
ISBN 978-91-628-8046-0

Number of pages: 225

Illustrations and figures: Henrik Hassel

Keywords: Risk and vulnerability analysis, technical infrastructures, municipalities, emergency response systems, preferences, emergency management, design research, method development.

Sökord: Risk- och sårbarhetsanalys, tekniska infrastrukturer, kommuner, responssystem, preferenser, krishantering, designvetenskap, metodutveckling

Abstract: Risk and vulnerability analyses can play important roles in the society's proactive emergency management. This thesis addresses two ways of improving the analysis of risk and vulnerability analysis in this context. First, by developing methods for risk and vulnerability analysis of technical infrastructure networks and emergency response systems. Secondly, by aiming to improve practices related to RVA through an evaluation of Swedish municipal RVAs and an empirical study of how various disaster characteristics affect people judgments of disaster seriousness. The research has to a large extent been carried out by using a design research approach developed in the thesis.

LUCRAM (Lund University Centre for Risk Analysis and Management)

Avdelningen för Brandteknik
och Riskhantering

Lunds tekniska högskola
Lunds universitet
Box 118
221 00 Lund

brand@brand.lth.se
http://www.brand.lth.se

Telefon: 046 - 222 73 60
Telefax: 046 - 222 46 12

Department of Fire Safety
Engineering and Systems Safety

Lund University
P.O. Box 118
SE-221 00 Lund
Sweden

brand@brand.lth.se
http://www.brand.lth.se/english

Telephone: +46 46 222 73 60
Fax: +46 46 222 46 12

Summary

Emergencies and disasters can affect any part of the world and cause extensive harm to life, health, the environment and the economy. The character of emergencies and disasters is however changing today, which leads to an increased need for working proactively with risk and emergency management in the society. The changing character of emergencies for example include increased complexity, increased interdependencies between actors and systems, such as between infrastructure systems, increased societal dependence on infrastructure services, larger potential for widespread effects of disasters, e.g. due to globalization, etc.

An important component in proactive emergency management is the performance of various types of risk and vulnerability analyses (RVA). The main purpose of performing RVA is to generate a good foundation for prevention and preparedness activities in the emergency management process and for informing risk-related decisions. In addition, another purpose of conducting RVA can be that the RVA *processes* themselves contribute to reduced risk and vulnerability by increasing risk awareness, stimulating reflection, creating social networks, affecting people's risk-relevant behaviour, etc. The importance of conducting risk and vulnerability analyses is increasingly recognised by many actors, for example leading to recommendations and regulations related to the performance of RVA, especially for actors having important roles in society's emergency management.

The aim of this thesis is to create good preconditions for societal risk and vulnerability reduction by developing methods and frameworks for RVA, and by studying and suggesting improvements in RVA practises. This research aim is highly normative, since it strives to construct or modify artefacts to fulfil some specified purpose. In order to carry out this normative research in a systematic and rigorous way, a design research approach has been outlined and employed for developing methods. The key points of the approach is to be explicit and transparent regarding the purpose that guides the method development, to be explicit and to justify the design criteria for the method development, to be explicit regarding how the suggested method is argued to fulfil the design criteria, and to evaluate the suggested method in the light of the design criteria and its intended purpose. The suggested process is iterative in the sense that applications of suggested methods should lead to an effort of learning from the application, e.g. in terms of modifying the method or modifying the design criteria.

Four main research activities can be discerned in the thesis. In the first two activities, the design research approach was applied for the development of methods. First, methods for vulnerability analysis of technical infrastructure

networks were developed. One method was developed with respect to single infrastructure systems and the method was then extended to also be able to analyse multiple infrastructure systems where both functional and geographical interdependencies were accounted for. It is stressed that there are many benefits related to analysing the vulnerability of such complex systems from several complementing perspectives and three perspectives are incorporated in the suggested methods. Second, a framework for post-event RVA of emergency response systems was developed. The main purpose of the framework is to facilitate the understanding of the response to past events, especially how different actors affect each other and how they affect the response system as a whole.

The two other research activities are related to RVA practises. First, an evaluation of RVAs performed by Swedish municipalities was carried out and ways of improving these analyses were suggested. Since this also mainly is a normative question, ideas from the design research approach described above were used to outline the employed evaluation approach. Second, an empirical study of how different disaster characteristics (e.g. number of fatalities) affect people's judgement of disaster seriousness was carried out in order to increase the knowledge of the value basis for RVA. It is argued that no RVA can be performed without a value basis and studies of this sort can inform the choice of value basis in RVAs conducted in practise.

Sammanfattning (summary in Swedish)

Olyckor och katastrofer kan orsaka enorma skador på människors liv och hälsa, på miljön och på samhällets ekonomi. Karaktären på olyckor och katastrofer håller på att förändras, vilket ger upphov till ett ökat behov av proaktiv krishantering. Förändringarna har exempelvis att göra med ökad komplexitet, ökade beroenden mellan olika aktörer och system (t.ex. mellan olika infrastruktursystem), ökade samhälleliga beroenden av infrastrukturers service, större potential för kraftigt utbredda effekter, t.ex. till följd av globalisering, etc.

En viktig del av proaktivt krishanteringsarbete är genomförandet av risk- och sårbarhetsanalyser (RSA). Det huvudsakliga syftet med att genomföra RSA är att skapa ett underlag för förebyggande och förberedande krishanteringsaktiviteter samt att informera riskrelaterade beslut. Ett annat syfte kan vara att RSA-processerna i sig bidrar till reducerad risk och sårbarhet genom att öka riskmedvetenhet, stimulera reflektion, skapa sociala nätverk, påverka människors beteende, etc. Mer och mer har betydelsen av att genomföra RSA insetts, vilket har lett till rekommendationer och lagstiftning gällande genomförande av RSA, speciellt för aktörer som har en viktig roll i samhällets krishantering.

Syftet med denna avhandling är att skapa goda förutsättningar för att reducera samhällelig risk och sårbarhet genom att utveckla metoder och ramverk för RSA samt genom att empiriskt studera och föreslå förbättringar i RSA-relaterade aktiviteter. Forskningen som presenteras här är starkt normativ eftersom den syftar till att konstruera eller modifiera artefakter så att något visst syfte kan uppnås. För att kunna genomföra normativ forskning på ett systematiskt och vederhäftigt sätt har en designteoretisk ansats utvecklats. Denna ansats har sedan använts för att utveckla metoder och ramverk för RSA. Huvudpoängerna med ansatsen är att vara explicit och transparent när det gäller vilket syfte som styr metodutvecklingen, att vara explicit och att motivera de designkriterier som gäller för metoden, att vara explicit när det gäller hur den föreslagna metoden uppfyller designkriterierna, samt att utvärdera metoden med avseende på designkriterierna och metodens syfte. Den föreslagna ansatsen för metodutveckling är iterativ i den meningen att en viktig del av metodutvecklingen är återkoppling och lärande från metodens användande. Detta kan ge upphov till behov av att modifiera metoden, modifiera designkriterierna eller till och med modifiera metodens syfte.

Denna avhandling består av fyra huvudsakliga forskningsaktiviteter. I de två första aktiviteterna användes ovan beskrivna ansats för att utveckla metoder och ramverk. För det första har metoder för sårbarhetsanalys av tekniska infrastrukturnät utvecklats. En metod har utvecklats för att kunna analysera enskilda

infrastrukturer, t.ex. ett eldistributionssystem. Denna metod användes sedan som utgångspunkt för att utveckla en metod som ska klara av att analysera flera infrastrukturer där funktionella och geografiska beroende tas hänsyn till. När det gäller komplexa system som infrastrukturer kan det vara svårt att skapa en bred bild av dess sårbarheter, därför analyseras sårbarhet från tre olika perspektiv i metoderna vilket ger en mer komplett bild av sårbarhet. För det andra så har ett ramverk för analys och utvärdering av responssystem utvecklats. Syftet med ramverket är att underlätta förståelsen för responsinsatserna vid en inträffad krishändelse. Det är speciellt hur olika aktörer påverkar varandra samt hur de påverkar responssystemet som helhet som ramverket fokuserar på.

De två andra forskningsaktiviteterna relaterar till studier av empiri med relevans för RSA. Den första av dessa aktiviteter handlar om en utvärdering av risk- och sårbarhetsanalyser som genomförts av svenska kommuner. Utvärderingen låg även till grund för förslag på olika sätt att förbättra kommunernas RSA-processer. Eftersom denna forskningsaktivitet till största delen är normativ användes många idéer från den designteoretiska ansats som föreslogs i samband med metodutveckling som grund för hur RSA-processerna utvärderades. Den andra forskningsaktiviteten utgjordes av en empirisk studie av hur olika attribut (såsom antal döda) påverkar hur allvarliga personer anser att katastrofer är. Denna aktivitet syftar till att öka kunskapen om människors värdegrund vilket är viktigt eftersom ingen RSA kan utföras utan en sådan. Studier av detta slag kan alltså vara ett underlag till valet av värdegrund för en analys.

Acknowledgements

Writing the acknowledgements on a cold, windy and grey February evening does not mirror the warmth and gratitude I feel towards so many people that have made this thesis possible. Without your academic and professional support I would never have been able to achieve the quality standards of a dissertation. Without your financial support I would never have had the opportunity to spend so much time on the subject. Without your emotional and empathetic support I would never have been able to finish the dissertation with a reasonable standard of sanity. And without your humour and high spirits it would simply not have been fun.

Thank you Kurt for all the great advice that always have helped me to choose the best path forward. Thank you Henrik for always having a thought-out answer to any of my questions. Your creativity and ability to see the simple things in the complex mess is really inspirational. Thank you Jonas for all the fun (but sometimes frustrating) times in front of Matlab, and for helping me better understand the broad area of technical infrastructures…. and beer. Thank you Marcus for all the great discussions we've had. Thank you Robert for making the last five years so administratively uncomplicated and for creating the best working environment one can imagine. Thank you Alex, Per, Lars, Kerstin, Jerry, Olof, Christian and Johan for all the intriguing discussions we've had. Thank you MSB for providing the necessary financial support. Thank you all other colleagues, including the FRIVA-group, for providing the perfect environment for a PhD-project. Thank you family and friends for all the great support. And finally, the last two persons I want to thank are also the two most important ones. Thank you Adelia, my fantastic daughter, for giving me the right motivation – the paternity leave – to finish the thesis. I can not wait to start teach you all about the theories of risk and vulnerability! Thank you Rima, my wonderful wife, for always giving me the best of all possible support. You know me better than I know myself and without your encouragement and emotional support this journey would have been much longer and more difficult.

Perhaps the thesis shows a rather straight path from A to B to C, however, this is not a true reflection of the many times very crooked path I've been travelling over the last 5 years. Although travelling along the crooked path probably has been longer, more cumbersome, and more frustrating than travelling the straight path, it has taught me so much more. When I started as a Ph.D. student after finishing the Master's thesis I thought I knew quite a lot of what there is to know in the field. Such a feeling gives good self-confidence but perhaps also some arrogance. During the five years as a Ph.D. student I have learned a lot, however, I have also learned that there are so many things I don't know. In fact, the "I know that I don't

know"-bubble has inflated much faster than the "I know"-bubble. This may give some lower self-confidence but more importantly it gives a great deal of humbleness, which I believe is an essential feature of researchers and risk analysts.

Barsebäck, February 28, 2010

Henrik Hassel

Table of contents

1 Introduction

Large-scale emergencies and disasters are pervasive phenomena that can affect any level of society, local, regional, national and international. In addition, disasters may also occur in every part of the world, including the more developed countries. A long list of recent events substantiate this claim, such as Hurricane Katrina in New Orleans (Farazmand, 2007, p. 8), the Storm Gudrun in Sweden (Johansson et al., 2006b), several large-scale power outages (e.g. Southern Sweden (Larsson and Ek, 2004), Auckland (Newlove et al., 2000) and North-Eastern USA/Eastern Canada (Amin and Stringer, 2008)), the terrorist attacks in New York (Kendra and Wachtendorf, 2003) and London (Hughes, 2006) and many more. This consistent track record clearly indicates that disasters will continue to occur in the future. However, in working proactively with risk and emergency management[1], society is able to affect how future events will unfold, thus hopefully reducing human suffering, environmental degradation and economic losses. It is this firm conviction that constitutes the underlying motivation for the work presented in this thesis.

The character of the emergencies and disasters occurring today is changing. Some significant trends include the increasing complexity of contemporary disasters (Perrow, 1999; Boin and Lagadec, 2000) and the increased potential for geographically dispersed effects. These trends stem from for example increased dependence on the services of infrastructure systems (Zimmerman, 2001; Boin and McConnell, 2007) and increased interdependencies and tighter coupling between critical infrastructure systems (Little, 2004). Renn for example argues that "[i]n an interdependent world, the risks faced by an individual, company, region or country depend not only upon its own choices, but also upon those of others" (Renn, 2008, p. 181), which clearly has significant effects for how we should work with risk and emergency management.

Other significant trends include the increased trans-national and trans-functional character of emergencies, e.g. due to globalization (Olsen et al., 2007; Quarantelli et al., 2007), the potential for climate changes, and much more. The trans-national character of modern disasters can be illustrated, for example, by the South East Asian Tsunami in 2004 that became one of the worst disasters in Swedish history

[1] Emergency management will be used in the present thesis to denote the processes of preventing, preparing for, responding to and recovering from emergencies and disasters. For a deeper discussion on different definitions of the related concepts of emergencies, disasters, catastrophes, etc. see Jönsson (2007).

(SOU, 2005:104)[2] and the recent outbreak of the "Swine flu" in Mexico causing extensive protective and precautionary actions throughout the world. In addition, people's expectations about future disasters are also changing, which may affect society's coping capacity. Citizens increasingly seem to expect that the government, or some other organizations, ought to actively protect them in the case of an emergency occurring – instead of the citizens' taking their own responsibility for disaster preparedness (Quarantelli et al., 2007; Palm, 2009). However, governmental and authorities' resources and response capability may in many cases be less today due to economic cutbacks and downsizing.

The changing picture of risk, caused by the trends described above, gives rise to an *increased need* of working proactively with risk and emergency management in society. The underlying assumption is that by taking *sound proactive actions*, societal risks and vulnerabilities can be reduced. Of course, numerous other societal objectives also exist, which means that value-based trade-offs always have to be made between using resources (e.g. economic, natural) to reduce risks and vulnerabilities and to achieve other societal objectives.

An essential component of such proactive work is the performance of various types of *risk and vulnerability analyses*, which is pointed out by many researchers, e.g. Quarantelli (1998), Perry and Lindell (2003) and Alexander (2005). The underlying reason for conducting the analyses is basically to create a sound *foundation* for risk-related decisions. This foundation includes how systems may "fail"[3], the negative consequences related to the failures and the associated uncertainties (KBM, 2006b; Paté-Cornell and Dillon, 2006; Aven and Renn, 2009b). More specifically, analyses are used to *inform* decision-making regarding risk reduction measures (Aven and Korte, 2003; Apostolakis, 2004), i.e. provide input to the question: is it possible to motivate the use of the necessary resources to implement a specific measure? In addition, it is sometimes argued that the *processes* of conducting the analyses in themselves have positive effects in that they create risk awareness, stimulate reflection, create social networks and affect people's risk-relevant behaviour (Hallin et al., 2004; Busby and Hughes, 2006; Jönsson, 2007; Pelling, 2007).

[2] Thailand is a very popular vacation destination for Swedish citizens. Approximately 20,000 Swedes were located close to the Thailand shores when the Tsunami occurred. More than 500 Swedish citizens died and many more lost family members. (Swedish National Encyclopedia – http://www.ne.se/lang/flodv%C3%A5gskatastrofen/915460/91546002, 2009-06-05).

[3] The notion of "failure" is here used to denote any deviation from what is considered the "success scenario" and which subsequently leads to damage to something considered of value.

The importance of conducting risk and vulnerability analyses is being increasingly recognised. In Sweden, for example, central authorities, municipalities, county administration boards, county councils and electric power companies are now obliged by law to regularly conduct RVA (SFS, 1997:857, 2006:544, 2006:942). In addition, several significant international actors, such as the United Nations (UN/ISDR and UN/OCHA, 2008) and the International Federation of Red Cross and Red Crescent Societies (IFRC, 1999), stress the importance of conducting proactive risk and vulnerability analyses. The goal of these initiatives is to reduce the risks and vulnerabilities in society, or at least have a good foundation for taking sound actions.

Here it is argued that the research society can create better preconditions for risk and vulnerability reductions in society in several ways in the context of risk and vulnerability analysis. The thesis will address two different ways creating preconditions for societal risk and vulnerability reduction. The first way is to *develop appropriate methods and frameworks for RVA* that can be utilised by various actors in the society. The second way is *to study and evaluate RVA practises and use insights to suggest how to improve such activities*.

1.1 Thesis outline

The thesis will be structured as follows: in the remainder of Chapter 1 the most important concepts and focus areas will be introduced, in Chapter 2 the aims and research questions will be described and Chapter 3 will define the concepts of risk and vulnerability in more detail. In Chapter 4, the main research methods used to address the research questions will be described. Chapter 5 will focus on each of the research questions and present the results and contributions related to these. In Chapter 6 the results will be discussed and some broader reflections of the implications of the results will be presented, as well as some suggestions for future research. In Chapter 7, the conclusions of the thesis will be briefly presented. Finally, the six papers that constitute the basis for this thesis are placed in appendices.

1.2 Brief overview of risk and vulnerability analysis

A risk and vulnerability analysis[4] is essentially about finding out what may happen in the future that give rise to negative consequences in some system of interest[5]. In

[4] The term "risk and vulnerability analysis" is frequently used in Swedish regulations. As for the discussion in the present section, the term can be treated as a synonym for risk analysis,

a risk and vulnerability analysis context there are always uncertainties about what will happen in the future, due to natural variation (aleatory uncertainties) and the analyst's lack of knowledge regarding the functioning of the system of interest (epistemic uncertainties). Most commonly, these uncertainties are characterised by using probabilities[6], but many applications of risk analysis also exist that make use of more semi-quantitative or qualitative characterisations of uncertainties, e.g. Aven (2008). The insights gained from the analysis are then used to inform decisions about whether to accept the current situation (e.g. an existing system or a proposed design) or whether and how the systems should be changed/redesigned.

1.3 Addressing the two core dimensions of RVA

The most obvious dimension that needs to be addressed in order to perform a risk and vulnerability analysis is *what the future will look like, i.e. to map out the potential future scenarios.* In addition to this dimension, an RVA must also consider *what outcomes should be regarded as desirable/not desirable or more or less desirable.* These two aspects correspond to a dichotomy sometimes expressed in risk and decision analysis research, see e.g. von Winterfeldt (1992), Keeney (1994), Renn (2001), and Gregory et al. (2006).

The first dimension addresses *knowledge about what will happen in the future*[7] in the system of interest and is usually addressed by collecting and synthesising "evidence" of various types, e.g. statistical data on system performance, statistical data on component performance, logical and system modelling, computer simulations, experimental studies, expert judgements and rational reasoning (SRV, 2003; Renn,

---

but in Chapter 3 the meaning of the term risk and vulnerability analysis will be more clearly defined.

[5] References on the foundations of risk and vulnerability analysis include Kaplan and Garrick (1981), Kaplan (1997), Kaplan et al. (2001), Paté-Cornell (2002), Apostolakis (2004), and Aven (2007).

[6] For some slightly diverging views on uncertainties and treatment of uncertainties in risk analysis, see Apostolakis (1990), Morgan and Henrion (1990), Paté-Cornell (1996), and Aven (2003). However, it is important to stress, as Aven (2004a) does, that *probability* is just a tool for expressing uncertainties. The popularity of the "probability approach" to risk analysis is due to the rigorous mathematical foundation of probability theory. However, note that other ways of expressing uncertainty exist, such as fuzzy probability, possibility theory, evidence theory (Zio, 2008) and info-gap theory (Ben-Haim, 2004).

[7] Different terms are often used to denote the question of knowledge about what will happen in the future. For example, Renn (2008) uses the term *evidence*, Cross (1998) uses the term *facts* and Gregory et al. (2006) use the term *science*. However, they basically refer to the same thing, namely the foundation for being able to accurately map out the potential future behaviour of some real or hypothetical system.

2008). The relevance of these sources of evidence for performing risk analyses and subsequently controlling risk differs for different types of systems. Rasmussen and Svedung (2000), for example, have proposed three different categories of accidents and control strategies. First, in the case of small-scale but frequent accidents (e.g. occupational safety), empirical epidemiological studies of the past performance of a large number of cases are used to estimate and control risk. Second, in the case of medium-size, infrequent events (e.g. aircraft accidents), analyses of individual past accidents can be used for controlling risk. Third, in the case of rare, large-scale accidents (e.g. nuclear calamities, natural disasters), risk cannot be controlled empirically only by extracting evidence from past accidents. Instead, predictive system modelling must be employed. Of course, empirical data may play a role for this category of events too, but with respect to the performance of components in the system rather than the system level performance. This thesis will primarily address the last category of risks.

The second dimension addresses *knowledge about values and preferences in relation to potential outcomes*[8]. This dimension is important since "preferences determine what counts as a harm" (Campbell, 2006, p. 227). Values here refer to what ends and goals one should pursue – i.e. "what we care about" (Keeney, 1992, p. 3), as well as how different values should be traded-off against each other. Renn is one risk researcher who stresses the value dimension of risk when defining risk as the "possibility that human actions or events lead to consequences that affect aspects of what humans value" (Renn, 1998, p. 51). What someone sees as an opportunity, potentially involving a "good" outcome, others see as a risk, potentially involving a "bad" outcome. For example, "[t]he tourist who hopes for a sunny week talks about the 'risk' of rain, but the farmer whose crops are threatened by drought will refer to the possibility of rain as a 'chance' rather than a 'risk' " (Hansson, 2005, p. 2). The difference in attitudes between the tourist and the farmer clearly does not have to do with their knowledge about what will happen in the future, e.g. their knowledge about the likelihood or intensity of rainfall. Instead, it has to do with their having different values in relation to the outcomes of the rainfall.

Since value statements regarding outcomes is a necessity in risk and vulnerability analysis, no analysis can be objective/value-free. This is *independent* on what epistemological stance[9] one has, e.g. whether one thinks that purely objective knowledge about the world is possible or not. The reason is that risk and vulnerability analyses always presume that outcomes can be classified as good or

[8] See e.g. Campbell (2006) for a discussion of preferences in the context of risk analysis.
[9] Different epistemological stances in a risk context can for example be positivism and social-constructivism.

bad – statements that are inherently subjective. Fischhoff et al. (1984, p. 124) express this view by arguing that the definition of risk always expresses "someone's views regarding the importance of different adverse effects in a particular situation". Thus, no risk and vulnerability analysis can ever be conducted without a value basis, whether it is implicitly assumed or explicitly expressed.

In addition to the obvious value dimension, discussed above, there is an additional value dimension of risk and vulnerability analysis. Namely the fact that the dimension related to knowledge about what will happen in the future may also be value-laden (Stern and Fineberg, 1996; Amendola, 2001)[10]. Thus, instead of a "black-and-white" distinction between the two there are many "shades of grey" (von Winterfeldt and Edwards, 1984). Anticipating possible future scenarios, for example, also involves value-laden judgements and assumptions – especially in the case of risk analysis of infrequent events, where the analyst is groping around in the domain of the nearly unknown and where there is a lack of relevant statistical data that can be used to predict the future. Of course, objectivity can in some sense be seen as a virtue in that one should strive to minimize the effect of preferences and judgement biases on the scenario projections (Paté-Cornell and Dillon, 2006). However, risk analyses will still always involve a wide array of subjective judgements and choices leading to a view where "[r]isk is primarily a judgement, not a fact" (Aven, 2004b, p. 2). Subjective judgements include assumptions regarding future trends in the system, how the risk problem is defined, how the system boundaries are drawn, how "facts" are interpreted, and how risks are

[10] Whether and to what extent science and knowledge are value-laden or value-free, socially constructed or objective, etc. is still an ongoing "battle" between different scientific worldviews (positivists/realists versus constructivists/relativists). See Bradbury (1989), Shrader-Frechette (1991b), Jasanoff (1993), and Klinke and Renn (2002) for deeper discussions of the two paradigms in a risk analysis context. Most of the concrete suggestions of frameworks for risk analysis that explicitly address the realist-relativist issue seem to argue for balancing the two extreme positions. Aven (2004b) for example argues that his predictive Bayesian approach lies between a positivistic and a relativistic approach. Similarly Renn argues that his Risk Governance "tries to avoid the naive realism of risk as a purely objective category, as well as the relativistic perspective of making all risk judgements subjective reflections of power and interests" (Renn, 2008, p. 3). In another suggestion of risk definition Aven and Renn argue that they provide a concept "without falling into the extreme of total subjectivism and relativism but also not pretending that risk is a measurable object similar to other physical entities" (Aven and Renn, 2009a, p. 10). Finally, Shrader-Frechette argues that her Scientific proceduralism approach is a "middle path between naive positivism and cultural relativism" (Shrader-Frechette, 1991a, p.239). The present thesis acknowledges that a middle path between the two extremes should be strived for, but it will not go into deeper philosophical and epistemological details on the matter.

expressed. In relation to expressing risk, Slovic (1999), for example, argues that any particular way of expressing mortality risks, such as deaths per million in the population, deaths per facility or loss of life expectancy, involves a value judgement. Realising that the virtue of objectivity can never be achieved is an important insight for anyone involved in risk analysis work, since it should affect how to design the risk and vulnerability analysis process and hopefully also trigger a humble attitude towards the outcome of the analysis.

In spite of the fact that there is no sharp distinction (in terms of objectivity/subjectivity) between knowledge about what will happen in the future and knowledge about values in relation to outcomes, the two dimensions will be treated separately in this thesis. This is in accordance with the advice offered by Renn, who argues that "[i]n managing risk one is forced to distinguish between what is likely to be expected when selecting option X rather than Y, on the one hand, and what is more desirable or tolerable: the consequences of option X or option Y, on the other hand" since "justifying claims for evidence versus values involves different routes of legitimization and validation" (Renn, 2008, p. 4). Similarly, Failing et al. (2007) argue that "fact-based" claims (descriptive claims about how the world *is*) and "value-based" claims (normative claims about how the world *should* be) should as far as possible be treated separately. It is for example likely that different people should play different roles in providing input to the two dimensions. For example, a geology expert can probably provide important input to the likelihood and magnitude of future earthquakes, but he has no special role in determining what values and preferences should be used regarding potential outcomes of earthquakes.

Both knowledge of future potential outcomes and knowledge of values related to these outcomes are essential for risk and vulnerability analysis. Therefore, *both these dimensions of RVA will be addressed in this thesis*.

1.4 Risk and vulnerability analysis in society's proactive emergency management

When an emergency or disaster strike some area of society, *actors*, including people (e.g. public, politicians, employees, rescue workers, volunteers), and organizations (e.g. industries, businesses, authorities, non-governmental organizations, first responders), *critical infrastructures* (e.g. electric distribution, transportation, water, sanitation), *resources*, *natural objects*, and *values* that are important to protect, come together in what can be described as a highly complex system. The affected part of a society could be neighbourhoods, districts, municipalities, counties, states, countries, continents, depending on the scale of the events.

Risk and vulnerability analyses play important roles in the society's proactive emergency management activities and analyses can be conducted on various subsystems of a society as well as with different perspectives. In order to specify the focus of the thesis further, it is necessary to briefly describe the Swedish emergency management system (since the point of departure of the thesis is a Swedish context) – especially emphasising the role of risk and vulnerability analysis.

The Swedish emergency management system is built around three principles: the principle of responsibility, the principle of parity and the principle of proximity (Palm and Ramsell, 2007)[11]. The principle of responsibility says that all actors, organizations and authorities retain their normal responsibilities in case of an emergency. This type of responsibility is called *sectoral responsibility* in the Swedish emergency management system. Furthermore, the principle of parity says that an actor's organization and localisation should as far as possible remain the same in an emergency as in normal operations. Finally, the principle of proximity says that an emergency should be responded to at the lowest possible level in the society. Since societal emergencies often require that many different organizations and authorities take action, there is a need for coordinating these actions. Therefore, in addition to the sectoral responsibility, there also exists a *geographic area responsibility*. This responsibility exists at the local (the municipal government), the regional (the county administration board) and the national level (the national government). It is important to note that the geographical area responsibility *complements* the sectoral responsibility rather than supersedes it. More specifically, the geographic area responsibility consists of an obligation to coordinate the actions of various actors within the geographic area during an emergency (SFS, 2006:544, 2006:942). And what is more important for the present context, municipalities and county administration boards also must coordinate the emergency planning and preparedness activities within their geographic areas.

According to Swedish regulations, both authorities with a sectoral and a geographic area responsibility must conduct RVAs (SFS, 2006:544, 2006:942). In addition, some private actors, such as power distribution companies (SFS, 1997:857), are also obliged to conduct RVAs. Furthermore, the Governmental Bill (2005/06:133) "Coordination in case of emergencies – toward a safer society"[12] suggests that "*critical societal functions*" must be able to maintain a "basic level of security"

[11] Information about the Swedish emergency management system can be found on the website of the Swedish Civil Contingencies Agency (http://www.msb.se).
[12] Free translation from the Swedish title: "Samverkan vid kris – för ett säkrare samhälle".

during severe emergencies[13]. Critical societal function is a term used in the Swedish emergency management system to denote a function or service that must work in order to prevent or respond to societal emergencies. Critical societal functions include energy distribution, financial services, transportation, rescue services, emergency hospitals, business and industry[14]. As such, the term Critical Societal Functions corresponds well to the term "Critical Infrastructure Systems" which is frequently used internationally and in research literature, see e.g. Rinaldi et al. (2001) and Kröger (2006). Henceforth, the concept of critical infrastructure systems will therefore be used. Current work in Sweden concerns defining criteria for such basic functionality in various critical infrastructure systems. But in order to employ such criteria there must exist ways of analysing these systems from a risk and vulnerability perspective.

This thesis will address three types of risk and vulnerability analysis activities that are important from a societal perspective. These are *vulnerability analysis of technical infrastructure networks, post-event RVA of emergency response systems*, and *municipal risk and vulnerability analysis*. These three types of activities will be introduced below. Although the motivation for considering these activities stems from their relevance in a Swedish context, it is likely that they are relevant in an international context as well.

1.4.1 Vulnerability analysis of technical infrastructure networks

Technical infrastructure networks constitute a significant sub-category of the broader term Critical infrastructure systems. In fact, sometimes when the term *critical infrastructure systems* is used, one refers to the narrower term *technical infrastructure networks* (such as electric and water supply systems). This section will therefore first introduce the broader term critical infrastructure systems and then narrow it down to technical infrastructure networks, which is one focus in the thesis.

Critical infrastructure can broadly be defined as large-scale socio-technical systems providing services to the society that are essential for its proper functioning (de Bruijne and van Eeten, 2007), and they play important roles in the context of

[13] "Basic levels of security", Fact sheet, Swedish Emergency Management Agency, October 2007, http://www.krisberedskapsmyndigheten.se/upload/15500/faktablad_grundlaggande_sakerhetsnivaer_2007_engelsk.pdf , 2009-06-12.

[14] "Critical Societal Functions", Fact sheet, Swedish Emergency Management Agency, March 2007, http://www.krisberedskapsmyndigheten.se/upload/16351/Critical%20Societal%20Funktions.pdf, 2009-06-05.

societal emergencies. There are many accounts of what can be classified as critical infrastructure systems. The President's Commission on Critical Infrastructure Protection (PCCIP, 1997), conducted in the USA, which has been very influential in the area, suggests eight categories of systems: Information and Communications, Electrical Power Systems, Gas and Oil Transportation and Storage, Banking and Finance, Transportation, Water Supply Systems, Emergency Services and Government Services. Other conceptions of Critical Infrastructures are even wider, e.g. including systems such as food and agriculture, the health care industry, and the educational system (Rinaldi et al., 2001).

It is important to note that it is the *services* that the critical infrastructures provide that are the real value to people and society (Little, 2002). The societal consequences of critical infrastructure breakdowns thus depend not only on the extent and duration of the service disruption but also on how dependent the society is on these services. More specifically, critical infrastructures can have at least two crucial roles in an emergency. First, they can be seen as alleviating (if they continue to provide their services) or amplifying (if their services are disrupted) the consequences of an emergency caused by some phenomena affecting the society. Second, they can be seen as the originator or trigger of an emergency if their critical services are disrupted due to some infrastructure failures.

The critical infrastructures in the society have undergone, and are undergoing, considerable change. Zimmerman argues that "[t]echnological changes have improved the provision of services of transport, water, electricity, and communications, often transforming the way we live, while at the same time substantially increasing the fragility and vulnerability of these systems and the services they provide by making them more complex and interdependent" (Zimmerman, 2001, p. 99). Dependencies and interdependencies between the critical infrastructure systems mean that disruptions in one CI can cascade to other infrastructures, causing secondary, tertiary and even higher-order effects, and in addition, effects may cascade back to the system from where the disruption originated.

The complexity of the critical infrastructure systems and the interdependencies between them have consequences for how we can understand and analyse them. Haimes and Longstaff, for example, argue that it is not possible to understand cascading effects between infrastructures on an ad hoc basis or using brainstorming-like methods. Rather, they argue that "the complexity of the interdependencies among the nation's infrastructures and the various sectors of the economy require systemic and quantitative risk modelling, assessment, and management efforts" (Haimes and Longstaff, 2002, p. 439)

Several research projects have been initiated in the area of modelling and analysing critical infrastructure systems; see Pederson et al. (2006) for an overview of approaches. These suggestions all have different perspectives on the issues at hand; see e.g. Haimes and Jiang (2001) for an economic-mathematical model, Min et al. (2007) for an economic-system dynamics model, Brown et al. (2004) for an agent-based model, and Apostolakis and Lemon (2005) for a network modelling approach. It is argued that methods and models with different perspectives are needed since no single method/model can possibly capture everything of relevance regarding this complex "system of systems". This statement is in agreement with Eusgeld et al. who argue that "there is no single 'silver bullet solution' to the problems of analyzing the risks associated to critical infrastructures" (Eusgeld et al., 2009, p. 954) – the point being that there is a need for a diversity of methods. These arguments, along with the fact that several researchers point out that the research field is still very new and that the state-of-the-art is still quite rudimentary, e.g. Rinaldi (2004), and Pederson et al. (2006), suggest that research on method development in this area is highly relevant.

Although striving to formulate generic approaches to model and analyse risks and vulnerabilities in critical infrastructures would be highly interesting, such an endeavour is held to be too wide-ranging for a single thesis to attempt. Instead, this thesis will focus on those critical infrastructure systems that are "mainly" technical and possible to model as networks, henceforth referred to as technical infrastructure networks.

Technical infrastructure networks include systems such as electric power, fresh water distribution, transportation, telecommunications, etc. These systems have in common that they are geographically dispersed and consist of various *nodes*, e.g. generators and substations in power systems, intersections in a transportations system, and *edges*, e.g. power lines in power systems, communication links in telecommunication systems. Various types of commodities and services of high societal importance, e.g. electricity, fresh water and information, traverse these networks and disruptions can therefore cause large societal consequences, such as power disruptions leading to problems for heating of houses, business activities and much more. *This thesis will therefore address the question of developing methods for vulnerability analysis of technical infrastructure networks*.

1.4.2 Post-event RVA of emergency response systems

When an emergency occurs in some part of society, an array of actors (both professional responders and volunteers) and resources are mobilized with the purpose of satisfying the needs that arise and thus minimizing the damage in the

emergency. In this thesis such a system of actors and resources is referred to as an *emergency response system* (Uhr et al., 2008). The actions of this emergency response system definitely affect the risks and vulnerabilities in the society, which means that improving the emergency response system can reduce risks and vulnerabilities.

An essential input to activities aiming to improve emergency response systems is information and knowledge regarding the performance and function of such a system. Such information and knowledge can be generated by modelling, analysing and evaluating emergency response systems, either proactively with respect to future hypothetical scenarios or more reactively with respect to the actual response to events. Both the proactive and the reactive perspectives are important.

This thesis will primarily focus on the reactive perspective, which is important for at least two reasons. First, in the aftermath of an event many important lessons can be learned about how the emergency response systems functioned and how they can be redesigned in order to function even better. Second, in the aftermath of events, especially large-scale, a so-called "window-of-opportunity" often exists (McConnell and Drennan, 2006), which implies that it is easier to implement changes, for example due to increased awareness of weaknesses and increased political and public determination to implement changes, etc. It is important, though, that such an "after-the-event" analysis does not become too narrow, since that might lead to the phenomenon of preparing to "fight the last war" (Lagadec, 2006, p. 489). The next emergency always differs from the previous one (Quarantelli, 1998). Instead, one should utilize the response to an event as an information source for gaining more general and broader insights regarding the functioning of the emergency response system. Here, the term *post-event risk and vulnerability analysis* will be used to refer to an analysis that uses a past event as a point of departure but strives towards a broader picture of the functioning of the emergency response system. *The issue of post-event RVA will, therefore, be addressed in this thesis*.

1.4.3 Municipal risk and vulnerability analysis

As described in the previous section, certain actors have special responsibilities for emergency management in Sweden. When it comes to risk and vulnerability analyses, this means that municipalities are responsible to perform analyses at the local level[15] (SFS, 2006:544), and county administration boards are responsible for analyses at the regional level (SFS, 2006:942). In addition, The Swedish Civil Contingencies Agency (MSB) is responsible to perform an overall analysis of

[15] Some municipalities in Sweden also perform geographic RVA at the *municipality district* scale.

especially severe risks and vulnerabilities on the country level in cooperation with various actors in the society (SFS, 2008:1002) by using insights from other actors' risk and vulnerability analyses. The analyses performed at different societal levels can be seen from a systems perspective similar to the socio-technical systems view of risk management in an industrial context proposed by Rasmussen (1997). This model includes work, staff, management, company, regulator and government levels; and all levels taken together (including feedback between the levels) set the safety level in e.g. an industry. In the "RVA system" the different levels consist of local, regional and national levels. RVA analyses at lower levels should be used as input at higher levels in the RVA system (and to some extent also the other way around). With this view analyses should, therefore, be designed *not only* considering the specific level on which it is performed *but also* considering the RVA system as a whole. In addition, since analyses conducted at the municipal level are an important foundation for higher system levels, these are considered to be especially important.

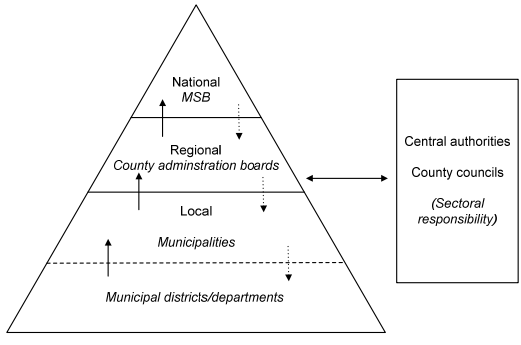


Figure 1-1. A systems view of the Swedish system of Risk and Vulnerability Analyses.

Although the legislation related to risk and vulnerability analysis by geographically responsible actors is relatively new, several activities are currently ongoing at both municipal, county and to some extent also the national level. However, since these activities are all in quite early phases, there are probably large potential for improvements. In addition there are some indications that improvements are actually needed (Hamrin and Strömgren, 2008; Nordström and Tonegran, 2008; SNAO, 2008; Abrahamsson and Tehler, 2009). Therefore, *this thesis will address the question of understanding and improving risk and vulnerability analysis practises in municipalities*.

1.5 A design research perspective

To a great extent, this thesis is concerned with designing and developing methods and frameworks that are useful in a risk and vulnerability analysis context, as well as improving existing practises. These two classes of problems, i.e. construction problems and improvement problems (van Aken, 2004), constitute *design research problems*. Since this research perspective differs somewhat from a natural science perspective (which is a more common subject in e.g. philosophy of science) it deserves some attention.

The overall purpose of natural science is to understand and gain knowledge about reality by employing systematic and scientific methods of inquiry – i.e. it is descriptive. This view is in accordance with Checkland, who states that "science is a way of acquiring publicly testable knowledge of the world" (Checkland, 1993, p. 50). Social and behavioural sciences have the same aim although focusing on other types of systems. In design research, on the other hand, the aim is to construct, design or develop different types of artefacts[16] that correspond to an "efficient accomplishment of some defined purpose" (Cook and Ferris, 2007, p. 173). Rather than the virtue of obtaining knowledge for the sake of the knowledge itself, which signifies natural science, design research is signified by the virtue of identifying and implementing the best, most efficient or at least satisfactory means of pursuing some predefined ends. As Bunge points out, whereas natural science elicits changes in order to know, technology (which is closely related to design) knows in order to elicit changes (Bunge, 2003). Design research thus has a *normative* feature – the concern "with how things ought to be" (Simon, 1996, p. 4), which descriptive sciences (e.g. natural science) lack.

Normally, design research concerns the development of *physical* artefacts of various types, e.g. technology for exhaust emission control, innovative medications, or improvement of building material properties. This thesis, on the other hand, is concerned with the design of methods and frameworks for risk and vulnerability analysis, which basically can be described as a set of interrelated thoughts and concepts that aim to help solve a problem of a specific kind in a specific context. The point, however, is that this is also a type of artefact, although of an *abstract* kind[17]. Developing methods thus concerns designing abstract systems, and many of the underlying principles that apply to the design of physical artefacts also apply to the design of abstract artefacts.

[16] Here, an artefact can be defined as a "thing" synthesised by humans to satisfy some human desire (Simon, 1996).
[17] Checkland (1993) uses the term designed abstract system.

Fundamentally, any designed system is developed for a certain *purpose*, or as Simon argues, design is concerned "with devising artefacts to attain goals" (Simon, 1996, p. 114). More specifically, Simon argues that design aims at adapting the "inner environment" (the artefact that is to be designed) to the "outer environment" (the world in which the artefact is used) so that the specified goals and purposes can be attained. One important step in the design process is the *evaluation* of a proposed artefact (Hevner et al., 2004). The evaluation phase concerns – using Simon's terminology – whether the inner environment actually is satisfactorily adapted to the outer environment, i.e. can the stated goals be adequately attained by using the artefact? Consequently, the evaluation of an artefact must be made "with respect to its specification" (Lewin, 1983, p. 130), since it is the goal specification that states what the artefact is made for.

The conclusion of this brief introduction to design research is that any design of artefacts, including the development of methods, must include *specification of design criteria*, corresponding to the purpose of the method, and *evaluation of the proposed design* with respect to those criteria. The problem is that these steps often seem to be made implicitly and non-systematically in the literature. But when the aim is a scientifically rigorous method development process, it is argued that these steps must be performed systematically and explicitly. In Section 4.1 these ideas will be further developed and formalised into a design research process.

1.5.1 A typology of abstract artefacts

Every design research activity must be directed at developing, producing or improving some type of artefact (Hevner et al., 2004). There are several types of abstract artefacts that are relevant here. More specifically, four types of abstract artefacts will be differentiated, namely *definitions*, *frameworks, methods* and *applications*, which draws on, but is not identical to, the classification proposed by March and Smith (1995), and Hevner et al. (2004)[18]. These four abstract artefacts can be related to each other on a scale expressing whether, or to what extent, the artefact is general or specific (see Figure 1-2).

[18] March and colleagues use the categories Constructs, Models, Methods and Instantiations. Constructs in their framework are equivalent to Definitions in this framework. Models, i.e. representations of how things are, on the other hand, have not been included explicitly here. However, in the present context, models are implicit in method and framework development. That is, in suggesting a method for analysing risk or vulnerability, one essential ingredient is to suggest how reality should be modelled (for example how critical infrastructure systems should be modelled).

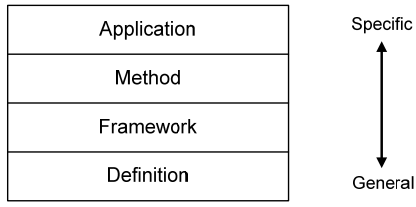


Figure 1-2. Four types of abstract artefacts on a scale from very general to very specific.

Definition is located at the bottom of the figure, i.e. it is very general in nature. In a definition one simply explains what is meant with a concept, such as risk or vulnerability. For example, risk is commonly defined as a combination of probability and negative consequences of unwanted events (Haimes, 1998). Although such a definition provides some insights about what risk *is*, it is too *theoretical* to be able to answer the question of what one must *do* in order to analyse risk. An *operational definition*, on the other hand, is a more concrete type of definition (Ennis, 1964). In this thesis the concept of operational definitions is used to denote definitions that provide guidance on what type of operations and procedures one must carry out in order to e.g. analyse the particular concept[19]. For example, the three risk questions (What can happen? How likely is it? What are the consequences?), from Kaplan and Garrick's definition of risk (Kaplan and Garrick, 1981; Kaplan et al., 2001), are of the operational type since they propose what questions need to be answered in order to analyse risk. This does not specify exactly *how* we should answer these questions. One reason for this is that a definition is meant to be applicable in a wide array of situations. Aven and Kristensen, in an attempt to bridge different areas of risk, argue for example that "there is no reason why these areas should have completely different perspectives on how to think when approaching risk and uncertainty, when the basic problem is the same – to reflect our knowledge and lack of knowledge about the world" (Aven and Kristensen, 2005, p. 1). However, to actually analyse or measure risk or vulnerability in different areas, such as structural engineering, business, transportation and medicine, will of course require rather different methods.

[19] In some areas, the concept of *operational definition* is used to denote a precise procedure to measure a theoretical concept. In operationalizing the theoretical definition one suggests one or several very concrete indicators (as well as how to measure them), which then are used to quantify/characterise the concept (Esaiasson et al., 2002). Note that the present thesis does not adopt this perspective on operational definitions, but rather regards an operational definition as expressing *what* questions need to be answered in order to analyse the concept — not exactly *how* since this will be different in different areas.

In order to be applicable to a practical problem, an operational definition must be concretised into a *framework* or a *method* that is adapted to the specific situation. Many assumptions are normally built in into frameworks and methods, and guidelines on how to conduct an analysis are usually explicated. The reason is to provide more specific guidance on *how* to answer the questions that need to be answered in order to analyse e.g. risk in a system. A game theory-based approach to characterise risk adapted to be of use in the context of terrorist threats (Bier, 2007) is one example of a method for risk analysis. The main difference between a framework and a method as it is being used here, is that a method is more specific than a framework; however, the principals are the same.

Applications constitute the practical utilization of definitions, frameworks and methods. A risk and vulnerability analysis conducted within some municipality constitutes an application of some underlying (implicit or explicit) method. The use of a newly proposed method or framework constitutes another application, and in a method development process, such an application demonstrates feasibility and effectiveness of the method (March and Smith, 1995).

In addition to the abstract artefacts mentioned, it is also worth pointing out the highly concrete implementation of methods in terms of *tools*. A tool can basically be seen as a product (in this context often computer software) that enables or facilitates the employment of a method. Monte Carlo simulation can be seen as one method for uncertainty analysis within risk analysis. A tool, then, is an implementation of a Monte Carlo-simulation method in a computer interface, e.g. @Risk, which is a user-friendly software, packaged together with a manual on how to use it.

It is important to note that the lower levels in Figure 1-2 should supersede the higher levels. That is, in order to develop a method, one should first start with clearly defining the concepts of interest. Of course, in principle it is possible to start directly to build a very specific method or concrete tool. However, if the method or tool is only *implicitly* or *vaguely* founded in some definition of the concept, the end result may not be very successful. Developing sound foundations, or appropriately using existing prevailing foundations, and making this explicit improves the scientific rigor of design research (Hevner et al., 2004). Here, this is for example addressed by clearly describing the conceptual points of departure for the most relevant concepts, i.e. risk and vulnerability; see Chapter 3.

1.6 Thesis publications

This section will present the six papers that are included in the thesis (the full-length papers can be found in the Appendices). Four of them have been published

in scientific journals, and two of them are currently in the peer-review process. Five of the six papers are outcomes of collaborations with one or two co-authors. In Chapter 5, when addressing the research questions, summaries of the author's contributions to each paper will be given. In addition, a number of related publications (e.g. conference proceedings and reports) are also presented below.

1.6.1 Appended papers

Paper I* Johansson, J., Jönsson, H. and Johansson, H. (2007), "Analysing the vulnerability of electric distribution systems: a step towards incorporating the societal consequences of disruptions", *International Journal of Emergency Management* **4**(1): 4-17.

Paper II* Jönsson, H., Johansson, J. and Johansson, H. (2008), "Identifying Critical Components in Technical Infrastructure Networks", *Journal of Risk and Reliability* **222**(2): 235-243.

Paper III Johansson, J. and Hassel, H. "An Approach for Modelling Interdependent Infrastructures in the Context of Vulnerability Analysis", submitted to *Reliability Engineering & System Safety*.

Paper IV Abrahamsson, M. Hassel, H. and Tehler, H. (2010), "Towards a systems-oriented framework for analysing and evaluating emergency response", *Journal of Contingencies and Crisis Management* **18**(1): 14-25.

Paper V Hassel, H., "Risk and Vulnerability Analysis in Practice: Evaluation of Analyses Conducted in Swedish Municipalities", submitted to *Natural Hazards*.

Paper VI Hassel, H., Tehler, H. and Abrahamsson, M. (2009), "Evaluating the Seriousness of Disasters: An Empirical Study of Preferences", *International Journal of Emergency Management* **6**(1): 33-54.

* Note that the author's previous surname was Jönsson.

1.6.2 Related publications

- Johansson, J. and Jönsson, H. (2008), "A Model for Vulnerability Analysis of Interdependent Infrastructure Networks", *Proceedings of ESREL 2008 and 17th SRA-Europe Conference*, Valencia, Spain.

- Abrahamsson, M., Jönsson, H. and Johansson, H. (2008), "Analyzing emergency response using a systems perspective", *Proceedings of PSAM9*, Hong Kong, China.

- Jönsson, H., Abrahamsson, M. and Johansson, H. (2007), "An Operational Definition of Emergency Response Capabilities", *Proceedings of 14th TIEMS Annual Conference 2007*, 350-359, Trogir, Croatia.

- Jönsson, H. (2007), "Risk and Vulnerability Analysis of Complex Systems: a basis for proactive emergency management", Licentiate Thesis, Department of Fire Safety Engineering and Systems Safety, Lund University, Lund.

- Jönsson, H., Johansson, J. and Johansson, H. (2007), "Identifying Critical Components of Electric Power Systems: A Network Analytic Approach", *Proceedings of the ESREL 2007,* 1:889-896, Stavanger, Norway.

- Johansson, H. and Jönsson, H. (2007), "Metoder för risk och sårbarhetsanalys ur ett systemperspektiv", LUCRAM report 1010, Lund University, Lund. (In Swedish.)

- Johansson, H., Jönsson, H. and Johansson, J. (2007), "Analys av sårbarhet med hjälp av nätverksmodeller", LUCRAM report 1011, Lund University, Lund. (In Swedish.)

- Johansson, J., Jönsson, H. and Johansson, H. (2006) "Analysing Societal Vulnerability to Perturbations in Electric Distribution Systems", *Proceedings of the CNIP 2006*, Rome, Italy.

2 Aims and research questions

The previous chapter has established the focus areas of the thesis, and also motivated the need for research in these areas. In this chapter these will be further broken down, first into an overarching, general aim of the thesis and then into a couple of more specific aims. Finally, these aims are narrowed down into a number of concrete research questions.

2.1 Aims

The general aim of this thesis is *to improve the analysis of risk and vulnerability in society's proactive emergency management*. As such, the thesis primarily constitutes design research. Admittedly this aim is very general, but it has served as the overall guidebook for the research conducted over the past five years in this doctoral project. Although most research activities in the field are directed at some specific types of systems (including the present thesis), many of the lessons learnt can likely be generalised to other fields of application; hence, this makes the above general aim reasonable. The general aim, stated above, will be addressed in two different ways. First, by *developing methods and frameworks that can be useful in analysing risks and vulnerabilities in society's proactive emergency management.* Second, *by understanding practises related to Risk and Vulnerability Analysis and suggesting how they can be improved*.

2.2 Research questions

Several of the research questions below concerns the development of methods or frameworks in the context of risk and vulnerability analysis. Some ideas about design research were presented in the Introduction, and it was emphasised that the *specification of design criteria* in relation to a method/framework development activity is essential since that guides the method development process and determines whether the proposed method design is satisfactory or not. It is important to realise that the specification of design criteria is an important part of the research process, they do not exist beforehand (this will be further explained in Chapter 4.1). When presenting the research questions, below, the design criteria related to each method/framework development activity will be specified. However, since the specification of design criteria is a part of the research process and result of the research, the *justification for the design criteria will be given in Chapter 5*. Therefore, in order to properly understand the design criteria and the context of the specification the reader is directed to Chapter 5.

2.2.1 Research question 1-2 – Method development

Vulnerability analysis of technical infrastructure networks

The introductory chapter established the societal importance of technical infrastructure networks and the need for developing methods that are able to model and analyse these systems. The ultimate objective of such an endeavour is definitely to be able to model multiple interdependent infrastructures. However, before doing that one must first be able to model and analyse single infrastructures with an approach that can be expanded into analysis of multiple interdependent infrastructures.

Traditional methods for risk and reliability analysis, such as fault and events trees, may be applied to analysis of critical infrastructure systems. However, there is growing recognition that these methods have limitations, especially related to handling the complexities of critical infrastructure systems (IRGC, 2006; Zio, 2007; Kröger, 2008; Eusgeld et al., 2009). In addition, traditional methods have particular difficulties in handling large-scale perturbation since, normally, failure independence and generic failure probabilities have to be assumed, leading to very small probabilities (and potential neglect) of multiple failures. However, failures stemming from common origins (malicious acts, natural hazards, etc.) and cascading failures are possible[20], which would lead to much higher probability of multiple failure than if the failures had been independent (Mili et al., 2004). Furthermore, the "N-1" design criterion[21] extensively used in practise (Mili et al., 2004; IRGC, 2006) also leads to little incentive to look beyond small-scale perturbations; however, here it is argued that large-scale perturbations should also be addressed. Therefore, the thesis will focus on *vulnerability analysis*, which, in the present context, means that the probabilities of the perturbations are not explicitly considered. Instead the focus is on how well the systems can withstand the occurrence of the perturbation, i.e. what are the negative consequences due to the perturbation? In order to subsequently make decisions regarding whether to reduce these vulnerabilities, one of course needs to consider whether any plausible perturbations or hazards exist that can exploit these vulnerabilities[22] – thus basically

[20] Several recent events have illustrated this, e.g. the power disruption in Auckland (Newlove et al., 2000).

[21] The N-1 criterion says that "any probable single event leading to a loss of a power system element should not endanger the security of the interconnected operation, that is, trigger a cascade of trippings or the loss of a significant amount of consumption" (Kröger, 2008, p. 1782).

[22] Note also that even though an analyst may not be able to imagine a plausible hazard that exploit the vulnerability, there *may* be reasons for reducing that vulnerability. Hansson, for example, argues that "safety does not mean measures only against those hazards that are

expanding the vulnerability analysis to a risk analysis (see Chapter 3 for definitions of risk and vulnerability). But it is argued that by *first* considering the system's vulnerability and *then* considering plausible hazards, threats and perturbation, a more unbiased mindset regarding what can happen in the future can be achieved. Based on the discussion above, the following two research questions can be expressed:

1a) How should a method for analysing the vulnerability of <u>single</u> technical infrastructure networks be designed, in order to satisfy the following design criteria:

- *i. The method should be based on the operational definition of vulnerability presented in Chapter 3.*
- *ii. Both analyses of global vulnerability and of critical components should be included in the method.*
- *iii. The method should be able to comprehensively analyse the vulnerability of technical infrastructures to large-scale perturbations, without leading to impractical computational times.*
- *iv. The method should be flexible enough to accommodate any type of technical infrastructure network.*
- *v. The method should more extensively account for functional properties of the technical infrastructure networks than the prevailing methods do.*
- *vi. The method should focus on the degradation in the services provided by the infrastructures to society rather than only technical aspects of the system.*
- *vii. Aggregate metrics for expressing global vulnerability should be included in the method.*
- *viii. A strategy for screening among possible combinations of failures in order to identify especially interesting ones should be included in the method.*

1b) How should a method for analysing the vulnerability of <u>multiple interdependent</u> technical infrastructure networks be designed in order to satisfy the following design criteria (in addition to the design criteria stated above):

- *i. The method should be able to account for functional and geographic dependencies.*
- *ii. The method should be able to analyse critical geographic locations.*

known and quantified, but also as far as possible against those that are unknown and unexpected" (Hansson, 2005).

Post-event RVA of Emergency Response Systems

Being able to model and analyse emergency response systems from a risk and vulnerability perspective is highly relevant for society's emergency management. This can be done in essentially two major ways. First, one can look backwards in time and consider the actual response to an emergency and perform a post-event RVA. The purpose of such an endeavour would basically be to create an understanding of the response to an event, as well as what the response to similar but hypothetical events would have been, in order to learn from it and improve future practices. This is referred to as an RVA since it strives to be broader than just a narrow analysis of the particular event. Second, one can look forward in time and consider future hypothetical scenarios, and model the emergency response in order to proactively identify weaknesses and possibilities for improvement. Such a perspective would be relevant for a "predictive" RVA. However, independent of whether the purpose is backward-looking or forward-looking, one must be able to appropriately model these systems. It is argued that the same basic modelling approach can be utilized in both instances, which is very similar to the relation between risk analysis and accident analysis, where the same underlying models and methods are often used for both purposes, see e.g. Hollnagel (2004) and Leveson (2004). This thesis will focus on the backwards-looking perspective. The research question can then be stated as follows:

2) *How should a framework for post-event risk and vulnerability analysis and evaluation of emergency response systems be designed in order to satisfy the following design criteria?*
    i. *The framework should address issues related to the values governing the evaluation*
    ii. *The framework should address issues related to the complexity of the systems involved*
    iii. *The framework should address issues related to the validity of the information on which the analysis and evaluation is based*
    iv. *The framework should address issues related to the limiting conditions under which the emergency response system operated*
    v. *The framework should aid in broadening the scope of the possible conclusions that can be drawn, i.e. enable conclusions to be drawn regarding other events than the one from which the analysis commenced.*

2.2.2 Research question 3-4 – Improve practises

Municipal Risk and Vulnerability Analysis

This question focuses on RVA practises in Swedish municipalities. Municipalities have the geographic area responsibility at the local level, and are therefore argued to be of special importance when it comes to the performance of risk and vulnerability analysis. The research questions can be stated as follows:

3a) How are risk and vulnerability analyses carried out in Swedish municipalities?

3b) How should the risk and vulnerability analysis processes[23] (studied in question 3a) be changed in order to satisfy the following design criteria?

i. The proposed changes should lead to improved fulfilment of some purposes stipulated by Swedish legislation.

ii. The proposed changes should be feasible given constraints that exist in the practical context of municipal RVA.

Value and preference elicitation

Another way of improving RVA practises in the society's emergency management is to pinpoint the second core dimension of risk and vulnerability analysis (see section 1.3). That is, to increase the knowledge about what values and preferences people have in relation to negative outcomes. The dimension of values is often not addressed sufficiently in research or practise, which means that studies of preferences are highly interesting. Although the ultimate goal related to this research question is to improve practises, the research question itself is primarily *descriptive* in nature.

Value elicitations can be performed in different ways, focusing on different aspects. One way is to perform broad, overall value elicitation with decision-makers and stakeholders in order to derive a set of values or valuable objects that are worth protecting; see e.g. Hallin et al. (2004). Another way of performing value elicitations is to make in-depth studies of how willing people are to make trade-offs between some specific attributes. The latter approach is the one adopted here. Four key characteristics of disasters will be used to study how important they are for people's judgment of disaster seriousness. Three of the characteristics constitute *consequences dimensions*[24] (number of fatalities, number of serious injuries and economic loss) whereas the fourth constitutes the *disaster cause*. Most approaches to

[23] Note that the municipal RVA can be seen as an application according to Chapter 1.5.1.

[24] The three consequence types were chosen since they are argued to among the most important ones in a disaster context.

risk analysis and evaluation only consider the consequences of the disaster, but if the cause also affects the judged seriousness of disasters, then perhaps the approaches to risk analysis and evaluation need to be reconsidered. This leads to the following research question:

4) *How are peoples' judgments of disaster seriousness affected by the following disaster characteristics:*
   - *number of fatalities in the disaster,*
   - *number of serious injuries in the disaster,*
   - *economic losses in the disaster,*
   - *cause of the disaster.*

2.3 Normative and descriptive research

Figure 2-1 shows an overview of the research activities that have been conducted as well as the relations between different activities. A distinction is made between which activities can be seen as *normative* (addressing question regarding how things ought to be) and *descriptive* (addressing questions regarding how things are)[25]. In design research, normative and descriptive questions interact iteratively. First, we need descriptive research to understand the nature and characteristics of the problems we set out to solve. Second, we need normative research to suggest how we should solve them. Third, we need descriptive research to gain insights regarding whether or to what extent we have actually solved the problems at hand. Fourth, we need normative research to further improve our problem-solving capability, since there will always exist better ways of solving complex problems (such as analysing risks and vulnerabilities of complex systems). Even primarily descriptive research, such as research question 4, approaches the normative realm when drawing on what implications the empirical findings have for risk and vulnerability analysis practise.

[25] This dichotomy is for example described by March and Smith (1995) and Brehmer (2008), and is very similar to the episteme–techné distinction once proposed by Aristotle (Hansson, 2003).

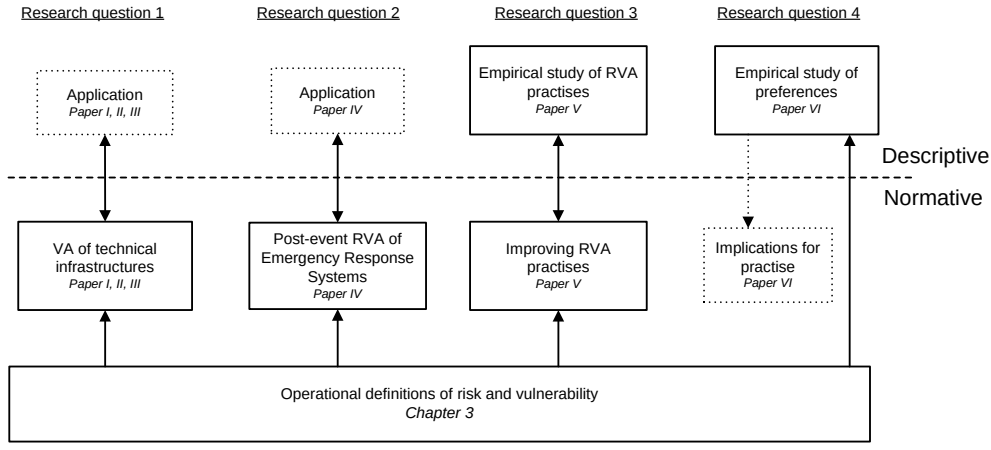


Figure 2-1. Overview of and relations between the research questions and where the research questions are answered. The broken lines indicate that these activities are not the primary research questions. For example in the case of vulnerability analysis of infrastructures, the interest is not primarily to gain empirical insight about the systems studied. Instead, the applications are carried out to test and evaluate the suggested methods.

As was described in section 1.5.1, in order to be able to develop and suggest a method for risk and vulnerability analysis there must exist a good foundation. Therefore, the next chapter will present such a foundation in terms of operational definitions of the risk and vulnerability.

3 Conceptual points of departure

Method development (and many other activities) should be founded in an explicit definition of the particular concept of interest (see 1.5.1). This foundation will therefore be briefly presented in this chapter along with some arguments regarding the plausibility of the suggested definitions. For a more extensive presentation of the concept definitions employed in the present thesis, the reader is referred to a previous work by the author (Jönsson, 2007).

3.1 Operational definition of risk

In the early 1980s, Stanley Kaplan and John Garrick published their view of how to define risk (Kaplan and Garrick, 1981), which has been very widely used in the risk analysis field. The original definition was later somewhat modified and refined (Kaplan, 1997; Kaplan et al., 1999; Kaplan et al., 2001). The definition was referred to as "the quantitative definition of risk"; however, that term makes the definition unnecessarily narrow since one actually does not have to quantify risk in order to adopt the definition. Therefore, the present thesis will refer to an operational definition[26].

Central to this definition of risk is the notion of *scenarios*. A scenario expresses a possible way that a system can behave in the future, and it can be viewed as a "trajectory in the state space of a system" (Kaplan, 1997, p. 416), see Figure 3-1. A scenario can be described as a succession of system states, U_j, over time, i.e. U_1, U_2…, U_k. Since there are always *uncertainties* regarding the future behaviour of the systems of interest in risk analyses, there always exist many possible scenarios. The type of scenarios of interest in risk analyses is referred to as *risk scenarios*, S_i. A risk scenario is a scenario that deviates from the "success scenario", S_0, which defines the behaviour of the system when everything works according to "the plan".

[26] Note that in the present thesis a distinction is made between a method for measuring risk or vulnerability and an operational definition, in that the operational definition provides a general way of characterising a concept, i.e. should be applicable in a wide array of contexts, whereas a method provides a practical way of complying with the operational definition in a specific context. The operational definition of risk thus addresses *what* needs to be answered in order to analyse risk, and a method answers the question of *how* to do it in a particular context.

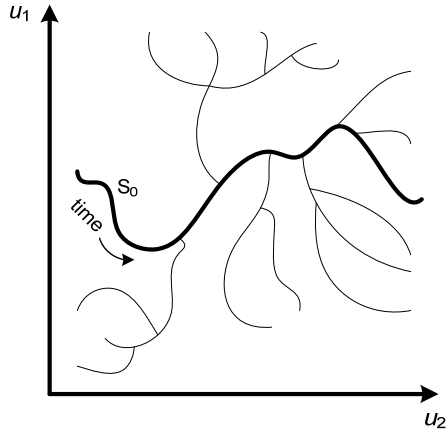


Figure 3-1. An illustration of risk scenarios (deviations from the success scenario) by using a geometrical state space representation of a system (in this case a system with only two state variables: u_1, u_2).

Significant for risk scenarios are that they lead to negative consequences, X_i. As has been noted earlier, a negative consequence is something that harms what is considered of *value* in the system of interest. Usually several dimensions of negative consequences are relevant to accurately capture the adverse effects of a potential event. This can be expressed as a vector composed of different consequence attributes (X_1, X_2….X_n), e.g. number of fatalities, number of serious injuries, number of minor injuries. In addition to the negative consequences, each scenario is also characterized by a probability, L_i, of occurrence. Probability is used to express that we are uncertain about what will happen in the future.[27]

The basic concepts of risk discussed above can be summarised in three questions that must be answered in order to analyse risk:

1. What can go wrong? (i.e. what risk scenarios can occur?)
2. How likely is it?
3. If it does happen, what are the consequences?

[27] Note that a more lengthy discussion about how to interpret the probability dimension of risk is certainly possible, but will not be pursued here. The reader is referred to Kaplan and Garrick (1981) and Aven and Kristensen (2005) for discussion of different interpretation of probability, e.g. frequency, probability of frequency and predictive Bayesian interpretations.

Since there are uncertainties regarding the future system behaviour, there are many answers to these questions. Risk can then be defined as a set of scenarios and their likelihood and negative consequence (see equation 1).

$$R = \{< S_i, L_i, X_i >\}, \quad (1)$$

There are three essential requirements for the definition of risk stated above. First, for practical reasons the set of scenarios should be *finite*. Second, the set of scenarios should be *disjoint*, i.e. no overlap may exist in the sense that several identified scenarios cover the same underlying scenarios. Third, the set of scenarios must be *complete*. The criterion of completeness means that the set of identified risk scenarios S_i must *cover everything* that may happen in the system. It is important to note that "covering all possible risk scenarios" does not mean that all possible risk scenarios must be described in detail in the risk analysis, only that all possible scenarios must be *represented* by some scenario description, S_i. The latter requirement should be seen as an ideal, since it is impossible in practise to really know whether everything of relevance is actually covered or not (Pidgeon, 1998; Stirling, 1999). This fact introduces what is sometimes referred to as *completeness uncertainties* (Vesely and Rasmuson, 1984), which could be seen as *constraints* on the risk analyses, since the result of the analyses only represents the risk scenarios that have been captured.

How to properly identify the risk scenarios so that the criterion of completeness (or near completeness) is achieved is to a large extent what constitutes the science and art of conducting risk analyses. A similar view is proposed by Kaplan and colleagues who argue that "[f]or any real-world situation the set of possible failure scenarios can be very large. In practice, the challenge is to manage this set – to organize and structure it so that the important scenarios are explicitly identified, and the less important ones grouped into a finite number of categories" (Kaplan et al., 1999, p. 8).

Note that the list of risk scenarios (along with their probabilities and consequences) generated in a risk analysis *is* the risk in the system. As Kaplan notes, risk defined in this way is "not a number, nor is it a curve, nor a vector, etc. None of these mathematical concepts is "big" enough in general to capture the idea of risk" (Kaplan, 1997, p. 409).

Summary and reflections on the operational definition of risk

The short version of the operational definition of risk is that risk *is* the answer to three basic questions: what can go wrong, how likely is it, and what are the

consequences? The answer to these questions is a list of risk scenarios, their likelihood and negative consequences.

All definitions of and approaches to risk somehow address unwanted events that may happen in the future and that entail negative consequences. In the terms used in the definition presented above, these events and the dynamic developments leading up to the negative consequences are referred to as *risk scenarios*. All definitions must therefore somehow address risk scenarios (although this term of course need not be used). Two general approaches can be identified in relation to this: scenario and index approaches. The definition presented above is a scenario approach since it *explicitly* addresses potential future events. Index approaches to risk, on the other hand, rather than focusing on future courses of events, focus on indicators that correlate or are assumed to correlate with risk (Davidson, 1997; Khan et al., 2003). Similarly, there are also index approaches to vulnerability, e.g. Morrow (1999) and Cutter et al. (2003). The underlying idea is that the indicators contribute to the occurrence of risk scenarios, e.g. the indicator "quantity of hazardous material at a facility" contributes to both the probability and severity of risk scenarios; however, risk scenarios are *not* explicitly addressed. Usually, many indicators are relevant and these are then combined into a composite risk index using mathematical weighting techniques. Index approaches, however, have a number of limitations which make them less useful for the present thesis. First, an index approach presumes that the risk in the system can be reduced to a set of indicator variables that are able to capture the relevant factors that affect risk. In the case of complex systems, this is not a straightforward task. Second, since the systems of interest here are constantly changing, the underlying index method (that is used for the analysis) must also constantly change (i.e. new indicators may become relevant). Although this is possible theoretically it is likely to be problematic in practise. Third, performing analyses using an index approach would consist of investigating how the system of interest "scores" against the indicators rather than focusing on the future negative events that may occur. In directing the attention of the analysis away from what may happen in the future, many of the process benefits of performing risk analyses may be missed (e.g. creating risk awareness and making people reflect on what may happen in the future). Fourth, in order to develop an index approach the developer has to assume what values should be used as a basis for the approach (e.g. what are the relevant dimensions of negative consequences). Hence, in order to make use of the index approach, the analyst's values must correspond to the values used as a basis for the index approach (usually those of the developer). But since values are subjective, this is not always the case; instead, it is argued that it must be up to the individual analyses to establish the value basis.

From the arguments above it is concluded that a scenario approach is more suitable for the present thesis; and the definition, presented above, is argued to include the essential building blocks (scenarios, probabilities and consequences) of such an approach. Without scenarios we have no description of the potential course of events that lead to negative outcomes, i.e. we do not attempt to anticipate what may happen in the system. Not considering scenarios would also lead to great difficulties in knowing how to prevent a risk or how to prepare for it, since we have no knowledge about what aspects, features, etc. of the system affect the courses of negative events.

Without probability we cannot say anything about how likely or how often a particular scenario may occur. If we are only interested in drawing a broad and rough picture of what may happen in the future, then perhaps we do not need to use probabilities. However, most often we need to be able to screen (e.g. what scenarios to include in the analysis) and prioritise (e.g. regarding what to do with respect to future potential events), and then we must consider what future potential events are more or less likely. A comet *may* collide with the earth in the coming 10 years, but perhaps we should not spend all our resources in preventing it since the probability is likely to be small.

Without negative consequences there is no relation to what system states we want to avoid. In the same way as we need probabilities to screen and prioritise, we also need negative consequences. Perhaps it is likely that a spruce cone will fall to the ground very soon, but it is not likely to be a negative consequence of relevance to the industry lying close to the spruce. In relation to the negative consequences, it is also necessary to explicate the value dimension of risk, since the values used as a basis for the analysis determine which system states constitute the negative consequences.

3.2 Operational definition of vulnerability

The application of the concept of vulnerability in the context of risk and emergency management began in the 1970s as a reaction to the prevailing paradigm that was seen as overly "hazard-centric" (Dilley and Boudreau, 2001), which was also reflected in how risks were managed (Weichselgartner, 2001; McEntire, 2005). Instead of investigating the internal characteristics of systems (such as a municipalities or a geographic region), the focus was on studying the external hazards and threats with the potential of damaging these systems. In the research literature it is possible to distinguish two subtly different but interrelated ways of interpreting the concept of vulnerability: vulnerability as a *property of the system as a whole* and vulnerability as a *feature or aspect of a system*.

The first of these views treats vulnerability as an emergent system property that determines the effect a specific hazardous event or perturbation has on the system – i.e. the magnitude of the of the negative consequences *given* the occurrence of a particular stress (Aven and Renn, 2009b). As such, "vulnerability is the crucial modifier of consequences" (Salter, 1997, p. 60). In this view, then, the "relationship between the hazards to which [the systems] are exposed and their vulnerability to those specific hazards is what creates risks of a specified negative outcome" (Dilley and Boudreau, 2001, p. 232), a view in accordance with the views proposed by several other scholars in the field, e.g. Salter (1997), Brooks (2003), Cardona (2003), Winser et al. (2004), Haimes (2006), and Aven (2007). In order to be able to talk about the vulnerability of a system, the vulnerability thus has to be related to specific perturbations.

The view that treats vulnerability as features or aspects of systems is for example proposed by Einarsson and Rausand (1998), Winser et al. (2004), Apostolakis and Lemon (2005), Haimes (2006), and Aven (2007). Instead of talking about vulnerability as a system property, they talk about *vulnerabilities* as features, weaknesses, or states that *contribute* to an increased susceptibility to perturbations, i.e. contribute to an increased vulnerability (when the term is interpreted as a system property). Aven, for example argues that "vulnerability is an aspect or a feature of the system that is judged to give a high vulnerability" (Aven, 2007, p. 747). In this phrase Aven thus uses vulnerability to refer to both types of interpretations of the concept. First he talks about *a* vulnerability and he exemplifies it with lack of redundancy in a system; then he uses vulnerability to refer to the overall susceptibility of the system to which the lack of redundancy is a contributing factor.

This thesis acknowledges that both these perspectives may generate important insights in a vulnerability analysis. However, for the sake of clarity two different concepts will be used for the perspective: when talking about the system's overall susceptibility to a perturbation the concept of "global vulnerability" is used, since it refers to a global property of a system; and when talking about features of a system the terms "critical components" or "critical locations" will be used, which are local properties.

Due to the similarities between risk and vulnerability, the framework provided by the operational definition of risk, presented previously, can be used to define vulnerability as well[28]. What is interesting in the vulnerability case is how the

[28] The operational definition of vulnerability that is suggested in the present thesis is to a large extent based on the report "Metoder för risk- och sårbarhetsanalys ur ett

system withstands the perturbation, or recovers from it given that the system has been damaged. Of interest is thus what risk scenarios may occur *given* the realisation of a hazard. So instead of the traditional three questions that need to be answered in conducting a risk analysis, the three questions to be answered in a vulnerability analysis are:

1. What can happen, given a specific perturbation? (i.e. which risk scenarios can occur?)
2. How likely is it, given that perturbation?
3. If it does happen, what are the consequences?

The vulnerability of a system to the specific perturbation will affect which risk scenarios can occur, and their respective probability and consequence. If it is likely that the consequences due to the perturbation will be large, the system is said to be vulnerable, whereas it is less vulnerable if the consequences are likely to be small.

The perturbation in itself can be of very short duration, such as an earthquake, but more often it represents a dynamic process that is stretched out in time, such as a hurricane. In defining the perturbation, using the concept from the definition of risk, it is not sufficient to define it as a single state; it must rather be a succession of states over time, i.e. a scenario. The perturbation, however, will only *constrain* or *determine* the state of some specific state variables in the system of interest or in its environment. For example, the perturbation "a hurricane" will only constrain the state of the variable "wind speed"[29]. How the other state variables in the system will be affected by the perturbation will depend on the system's internal characteristics, and how the state variables that are related to the underlying *value system* (such as those related to life and health, the environment etc.) are affected depends on the system's vulnerability to the specific perturbation. Thus, the perturbation is not defined as a completely determined risk scenario; instead it is defined as a *partially*

systemperspektiv" (Methods for risk and vulnerability analysis from a systems perspective) (Johansson and Jönsson, 2007). The report is a result of the research conducted in the research programme of which the author is a part.

[29] Here of course it is crucial how the perturbation is specified. The perturbation "a hurricane" will *constrain* the state of "wind speed", since this is what actually defines a hurricane. The state of the "levee integrity" will for example not be constrained by the hurricane. Of course, the levees may very well be damaged as a consequence of the perturbation; however, whether this will be the case also depends on the robustness of the levees. If instead the perturbation was specified as "a hurricane that breaks the levees" the levees would have been assumed to be damaged, since this is what defines the specified perturbation, i.e. the perturbation constrains the state of the "levee integrity" so it is in a damaged state.

determined risk scenario, which constitutes a deviation from the success scenario S_0. More specifically, the partially determined risk scenario that represents a perturbation, S_p, consists of a succession of *partially determined states of the system*:

$$S_p = \left(U_{p,1}, U_{p,2} \ldots U_{p,n}\right). \quad (2)$$

Each partially determined state of the system, in turn, consists of two types of state variables, the ones determined by the perturbation, and the ones *not* determined or constrained by the perturbation. The latter type of state variables is denoted $\#_1$, $\#_2 \ldots \#_j$, whereas the former type is denoted $u_{p,1}$, $u_{p,2} \ldots u_{p,k}$.[30] A partially determined state of the system, U_p, that correspond to the perturbation can then be defined as:

$$U_p = \left(u_{p,1}, u_{p,2} \ldots u_{p,k}, \#_1, \#_2 \ldots \#_j\right), \quad (3)$$

where $k>0$ and $j \geq 0$. Note also that k and j can vary for different $U_{p,1}$, $U_{p,2} \ldots U_{p,n}$.

The states of the #-variables are *not* determined by the perturbation (but may can be affected by the perturbation). S_p can therefore be thought of as corresponding to a set of risk scenarios that covers a constrained area of the state space of the system, see Figure 3-2.

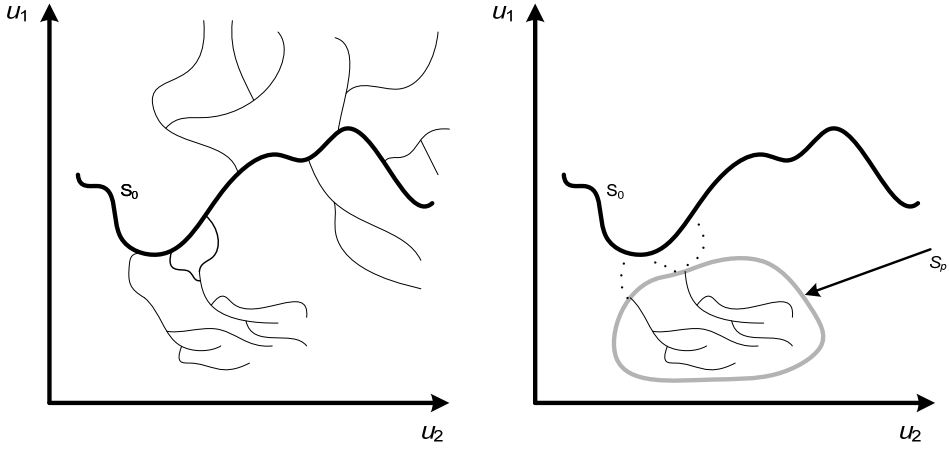


Figure 3-2. The difference between risk (to the left) and vulnerability (to the right) by use of state space representation.

[30] The notation chosen here is influenced by the notation used by Holland (1995) in his book *Hidden Order*.

The conceptual differences between vulnerability and risk can now be applied to Equation 1 to adapt it to define vulnerability in an analogous manner as risk, i.e. as a set of triplets. The only modification that has to be made stems from the fact that in a vulnerability analysis it is only interesting to study the risk scenarios that can occur *given* that a specific perturbation occurs. The perturbation is defined by specifying a partially determined risk scenario $S_{p,}$ and all identified risk scenarios must be consistent with this scenario, i.e. they must be members of the set S_p. These modifications are presented in Equation 4 below.

$$V_P = \{< S_i, L_i, X_i >\}_P : S_i \in S_p \quad (4)$$

Summary and reflections on the operational definition of vulnerability

The short version of the operational definition of vulnerability is that vulnerability *is* the answer to three basic questions: what can go wrong, given the occurrence of some perturbation, how likely is it given the occurrence of the perturbation, and what are the consequences? The answer to these questions is a list of risk scenarios, their likelihood and negative consequences, contingent on the occurrence of the specified perturbation (which must be well-defined).

Based on the view that vulnerability is a system's susceptibility to a specific perturbation, and the relation between the concepts of risk and vulnerability, the operational definition of risk can rather straightforwardly be adapted to vulnerability. The crucial difference between analysing risk and analysing vulnerability is that the perturbation which the analysis is conducted with regards to must be clearly and explicitly described. The plausibility of the operational definition of vulnerability thus depends on whether the operational definition of risk and the relation between risk and vulnerability is plausible – which has been argued for above.

In this thesis the phrase risk and vulnerability analysis is used. This term is frequently used in the Swedish emergency management system and sometimes also in the research literature. The Swedish Civil Contingencies Agency (MSB)[31] uses the phrase in order to put an increased emphasis on the consequence dimension of risk, especially the long-term consequences and the capability to respond to emergencies (KBM, 2006a). A risk and vulnerability analysis, according to MSB, starts with a rather coarse risk analysis (similar to a preliminary hazards analysis)

[31] In 2009 the Swedish Emergency Management Agency (SEMA) ceased to exist. Instead the Swedish Civil Contingencies Agency (MSB) was created and assumed the responsibilities of SEMA.

including semi-quantitative estimations of probabilities and consequences of different scenarios, followed by an in-depth analysis of a small number of scenarios with respect to different actors' capabilities to respond to the scenarios on.

As the concepts are used here, it is clear that vulnerability is part of risk. But when using the phrase risk and vulnerability analysis, instead of only risk analysis, one emphasises the vulnerability dimension of risk. This view is suggested by Aven who argues that "[a]s vulnerability is part of risk, a vulnerability analysis is part of the risk analysis……To emphasis that we specifically address vulnerability, we write risk and vulnerability analysis" (Aven, 2007, p. 748). Similar to Aven, Wisner argues that vulnerability is part of risk, meaning "potential for disruption or harm" (Wisner, 2001). He further argues that if "there is sufficient probabilistic, process knowledge of the particular hazards, statements about risk as the probability (not simply potential) for disruption or harm can result" (Wisner, 2001, p. 1).

In expanding an analysis from *potential* for harm to *probability* of harm, more interesting conclusions can generally be drawn, and the possibilities for suggesting rational strategies for risk reductions are enhanced. Intuitively, therefore, it could be argued that one should always strive to expand a vulnerability analysis into a risk analysis. But sometimes it can be very difficult to determine the probability of a perturbation accurately due to lack of knowledge and data regarding the phenomena – for instance the threat of terrorism and cases of multiple simultaneous failures in infrastructures. On such occasions, a vulnerability analysis is a good starting point to gain knowledge of how well a system can withstand and recover from certain perturbations, without having to consider the probability of the perturbation explicitly. Thus, vulnerability analyses can be used as a first step in a broader risk analysis to point out critical components in the system that merit deeper analysis in terms of how well protected they are, how likely they are to fail and so on.

4 Research method

Selecting and designing appropriate methods for the research problems at hand is the main way for a researcher to ensure a result of high scientific quality. The present chapter, therefore, will describe the methods used for answering the various research questions stated in Chapter 2. Primarily, it will focus on more general and overall aspects of the methods used here, rather than go into very specific details of the methods used in the individual papers. For these specific details the reader is referred to the appended papers.

This thesis employs two approaches to creating good preconditions for improving society's proactive management of emergencies: method and framework development, and understanding RVA practises and subsequently suggesting improvements. In spite of the apparent differences between these two ways of improvement, they share one characteristic – they constitute *design research problems*. In the case of method/framework development, the problem concerns how to design the method to fulfil certain specified criteria. In the case of RVA practise, the problem concerns how to change an RVA process in e.g. a municipality so that the RVA process is improved. The next section will present the design research process developed and used in the present thesis. After that, a number of additional methods, e.g. data collection methods, which have been used throughout the research, will be presented. Finally, an overview of the methods employed for answering the various research questions and in the various papers will be given.

4.1 Design research

The ideas on design research presented in this section and adopted in this thesis are highly influenced by Herbert Simon's (Simon, 1996) ideas about design, Peter Checkland's (Checkland, 1993) ideas on methodology development, the ideas about design science proposed by March and Smith (1995) and Hevner et al. (2004)[32] and the design logic framework suggested by Brehmer (2008) – which in turn is based on work by Rasmussen (1985).

4.1.1 General approach

Developing methods (and other abstract artefacts) for some specific purpose can be done in an infinite number of ways. In such a situation it is of course impossible to

[32] Some previous ideas on engineering design research have been presented by the author in Jönsson (2007).

identify *all* possible alternatives (Hevner et al., 2004), which means that one cannot have the ambition of developing the optimal method. Instead, one has to strive to develop a method that is *satisfactory*, that is, it satisfies the design criteria that have been set up for the method (Simon, 1996). Note that there are always many solutions to a design problem, i.e. there are always many methods that meet the design criteria (Poser, 1998). Another consequence of the fact that the number of alternatives is infinite is that the method development process can go on for ever, striving to continually improve the method by successively implementing changes to improve the method. Therefore, method development should be seen as a "living process", which in principle can continue perpetually (Lewin, 1983). Commonly, though, it is likely that a method of a specific type is eventually abandoned in favour of a method of a totally different type, for example using a totally different methodological approach[33].

When the ambition of finding the optimal method has been abandoned, there are (at least) two possibilities of proceeding (see Figure 4-1 for an illustration of these two approaches). The first is in analogy with the systems engineering process, which can be described chronologically as choice of objectives (design criteria), creation of a finite number of alternatives, evaluation of alternatives and finally choice of the best alternative – the one that scores the best on the objectives (Lewin, 1983; Leveson, 2002). This would essentially entail one choice – i.e. the choice between the alternative methods. The second way forward is to view the method development process in a much more incremental way which entails a number of consecutive method choices. First, larger paradigmatic or methodological choices are made, e.g. regarding whether the method should be qualitative or quantitative, or whether an analytical or numerical approach should be used, etc. As the process continues, more and more specific method choices are made, *given* all the previous choices that have already been made. It is important to note that over time in the method development process, more and more knowledge and information is gained that may lead to a situation where a previously made method choice no longer seems to have been the best one possible. If possible, then the choice should be revised; however, sometimes a method choice

[33] There is a rather straightforward analogy to the theory of scientific revolutions proposed by Thomas Kuhn (Kuhn, 1962). Kuhn argues that most activities in a specific scientific field are conducted within a *scientific paradigm* corresponding to what is referred to as *normal science*. Knowledge is generated, problems are solved and phenomena are explained by using methods and scientific theories that are accepted within the paradigm. However, over time questions and doubt arise in relation to problems and phenomena that cannot be explained within the paradigm. Eventually, an alternative paradigm arises, which is able to explain some of the phenomena that the old paradigm did not explain, and replaces the old paradigm – causing what is referred to as a *scientific revolution*.

may be difficult to revise, which means that one has to accept the choices and their implications although one has become wiser in hindsight.

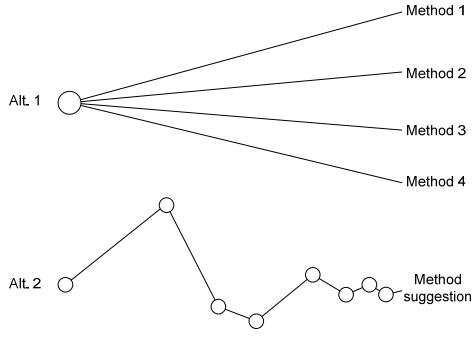


Figure 4-1. An illustration of two different ways of developing methods. The nodes represent a choice. The first alternative thus only considers a single choice between a number of candidate methods. The second alternative (which is adopted in the present thesis) concerns an array of choices concerning method characteristics. In the beginning choices with large consequences for the method properties are made, and towards the end the choices will have small effects on the method properties.

The present thesis will adopt the second way of developing methods (described above). It is argued that this approach is more feasible for method development at a "micro level", i.e. when a researcher or a research group develops a method, since they most likely have resource constraints making alternative 1 unpractical. Alternative 1 is argued to be more applicable in a situation when an analyst addresses a specific problem and where several *existing* methods to address the problem exist. Then choosing one of these methods, depending on how they score on the design criteria for the particular problem situation, seems reasonable; see Ford et al. (1979) for an example of such an approach.

One consequence of choosing alternative 2 is that there is an iterative relationship between research question and design criteria. Early in the research process, when few criteria have been specified, the research question is rather vaguely formulated. But as additional design criteria are specified and method choices are made, the research question becomes more specific and narrow. It is essentially the end product of this iterative process that is depicted in the research question in Chapter 2.

4.1.2 The method development process

An overview of the research process used to develop methods, which draws on design research, is presented in Figure 4-2. The various steps in the process will be described and discussed in turn below.

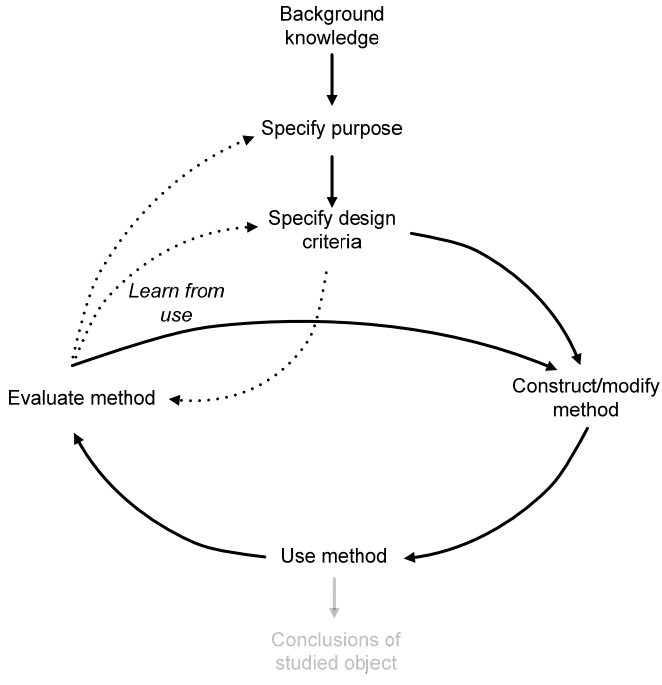


Figure 4-2. The research process used to develop methods in the context of risk and vulnerability analysis.

Background knowledge

The first step, which concerns background knowledge, is perhaps an obvious but at the same time important one for addressing design problems. The assumption is of course that we cannot start to think about a design problem, such as method development, without having some background knowledge. In the present context, this first of all concerns *domain knowledge*. That is, if the research interest is methods for analysing risk and vulnerabilities in society, we need to have an understanding of the activities that are ongoing in society on risk and vulnerability issues; we need to understand what the challenges in the particular areas are, etc. If the interest is in methods in the critical infrastructure area, then one has to have a good understanding of what characterizes these systems and what the challenges are

in analyzing them. Second, we also need to have knowledge of the *needs* in relation to the method development – i.e. is the research relevant (Hevner et al., 2004)? With a design perspective comes the requirement of usefulness (Nordin, 1988; Kroes, 2002), i.e. the artefacts that are developed must be useful for some actors. Therefore, in method development it is important to understand what is needed in practice. Third, we need to have knowledge about *existing methods and their limitations*. This is because the goal of design must be to improve or complement existing methods[34].

Specify purpose

As has been argued previously, in the centre of any design problem is a purpose (or several); and it is important that this purpose is expressed clearly, since every step of the design process is directed at the pursuit of constructing an artefact that is able to fulfil that purpose. The specification of purpose can sometimes be derived from legislation (if there are any requirements expressed in the legislation e.g. regarding performance of RVA). Another way of deriving the purpose is from the needs of potential users, since research in the design area should be directed towards developing *useful* artefacts.

Specify design criteria

The purpose of an artefact is expressed in very general and abstract terms, which means that it is important to specify more concrete *design criteria*[35]. The design criteria basically state what functions and characteristics the artefact needs in order to be able to fulfil the specified purpose (Brehmer, 2008), and in order to do that the designer must make an array of *normative assumptions*[36]. It is very important that these normative assumptions are properly justified[37] (e.g. based on empirical

[34] The analogy to natural science is straightforward again. There the goal is to improve the prevailing scientific theories; and in order to do that one must of course understand what their limitations are.

[35] Other terms sometimes used with a similar meaning are constraints and requirements (Simon, 1996; Hevner et al., 2004).

[36] A normative assumption, in this context, can be seen as a proposition regarding some aspect of a method that makes the method better than if we do not make the assumption (or make other assumptions regarding that particular aspect). For example, one normative assumption used in this thesis is that the values underlying the analysis must be identified and described early in the risk analysis. If the value basis is not addressed or made explicit, the quality of risk analysis will be poorer. Rational argumentation has been used to support this proposition (see e.g. section 1.3).

[37] The term justify stems from the article on design written by March and Smith (1995), March and Smith, however, use the term to refer to an activity in descriptive research that concerns finding evidence in favour of a proposed hypothesis (e.g. conducting

evidence, research literature or some type of rational or logical reasoning) because this affects the scientific rigor of the design. In addition, it is important that these arguments are made transparent to enable external actors to scrutinize the work. First, scrutiny can be performed by the research community in order to investigate the scientific quality of the work. Second, scrutiny can be performed by potential users when considering whether to use a proposed method or not, which largely depends on whether he/she believes the assumptions are valid in the particular context of interest.

It is likely that all method development activities, e.g. in the risk and vulnerability analysis field, have some design criteria that guide the development. However, most often these are kept *implicit* or are only *vaguely* formulated. This is unfortunate because it becomes very difficult to say anything about the quality and applicability of the method due to the fact that peers/users have to assume what design criteria were used.

Construct method

The next step is to actually construct the method[38]. As has been described previously, the goal of this step is not to identify the optimal method but to construct a method that satisfies the specified design criteria. Optimization is simply impossible since it is impossible to identify all possible alternatives (Simon, 1996; Hevner et al., 2004). Note that several possible methods that satisfy the design criteria will always exist. In Brehmer's framework this would correspond to the fact that there are many *forms* (i.e. concrete configurations) of an artefact that fulfil the functions and characteristics stipulated by the design criteria (Brehmer, 2008). Of course, this is true for any type of artefact; take a building for example. Several design criteria are likely to be relevant. E.g. it should be multi-story, it should be a residential building for between 20 and 30 families, it should withstand a magnitude 7.5 earthquake, and its aesthetic characteristics should harmonise with the surrounding buildings, etc. But, even though a wide array of design criteria is specified, there will still be many alternative buildings that satisfy these criteria – i.e. different building materials, different sizes on the apartments, different colour on the façade, etc.

The process of creating the method is a creative and explorative process that e.g. includes making thought experiments regarding what consequences various

experiments). However, the same basic activity is argued to also exist in design research when a researcher strives to find support for normative assumptions.

[38] The analogy in natural science is to construct a falsifiable hypothesis regarding some natural phenomenon.

method choices will have for the design criteria (see Alt. 2 in Figure 4-1 for an illustration of the explorative process). Throughout this explorative process the design criteria are used as a guide-post for the method choices. It is also important that the method choices are justified, since as March and Smith argue, the research contribution (in addition to being novel) "lies in the persuasiveness of the claims that the artefact is effective" (March and Smith, 1995, p. 260).

Note that it is very common that method development does not start from scratch but rather departs from an existing method and tries to improve some aspects of that method or modify it so that it is applicable in another area[39].

Use method

After the method has been constructed it should be used in order to get a sense of its applicability and feasibility[40]. This can be done in either a *small-scale* (which is commonly an initial step in a method development process) or a *full-scale* application. It can be done on *hypothetical* (but realistic systems) or *real systems* using data from the actual context. Of course, applying the method on a real system using actual data as input is generally preferable although sometimes it is not "cost-effective" in the sense that some issues related to the method can be highlighted without having to spend resources on collecting the data of the real system. Naturally, small-scale testing on hypothetical systems is common in the early phases of the method development process, whereas full-scale applications on real systems are more common later in this process.

The application of a method can also provide important insights about the systems on which it is applied (March and Smith, 1995). This is of course the main goal when ultimately using a method for RVA in practise. However, in the method development process, the details of those insights are not essential since it is the applicability, feasibility, effectiveness, etc. of the method that constitute the primary interest.

[39] The analogy in natural science is yet again straightforward: in natural science, researchers often depart from existing theories and try to alter some aspects of those theories so that they become better at predicting some phenomena, or is able to explain some additional phenomena which the original theory did not explain.

[40] This step is similar to the phase in natural science where the researcher makes observations or conducts experiments.

Evaluate method

As has been described previously, an important phase of the method development process is the evaluation of the proposed method[41] (Lewin, 1983; Hevner et al., 2004). From an evaluation one can e.g. draw conclusions regarding what worked well and what did not work so well in practise – which is an important input to the continuous process of improving the proposed method.

Note that evaluation can be done either *internally*, i.e. by the ones that developed the method, or *externally*, i.e. by researchers who are independent of those who developed the method (e.g. through peer review in scientific journals). These two ways of evaluation are similar to the α-tests (tests and evaluations by the originators) and β-tests (tests and evaluations by third parties) performed in the software development field (van Aken, 2004). The main point of β-testing, according to van Aken is to counteract the "unrecognised defences" of the originator of the rule, which may blind him or her to possible flaws in its use. As such, both internal and external evaluations are important to ensure the scientific quality of the method development[42]. However, β-testing is usually outside the scope and control of the originator.

Note that when evaluating methods it is important to appreciate the difficulty of distinguishing between deficiencies/limitations in *the method itself* and deficiencies in the *application* of the method, i.e. deficiencies introduced when the method is applied in practise. This can for example stem from practical constraints or the fact that the method was not used as it was intended by the method developers.

Learn from use

The point of the method evaluation phase is to learn from the application. E.g. is it possible to modify it in order to better meet the design criteria (Checkland, 1993), or can it be simplified and made more efficient without violating the design criteria? As Hevner et al. (2004) argue, in design science it is common that several iterations in the "construct-evaluate loop" are made before a design is finalised. If proper modifications of the method are difficult to introduce, then an alternative would be to document that the method has limitations in some context. These

[41] The analogy to evaluating a method in the natural sciences is the interpretation of performed experiments/observations with subsequent corroboration/falsification of the hypothesis.

[42] In natural science the analogy would be that the scientists proposing a hypothesis should perform experiments and collect data that supports the hypothesis (internal evaluation). But in order to really become an accepted scientific theory, external, independent research groups must also conduct experiments that corroborate the hypothesis.

must then be communicated to the users so that they can employ the method appropriately.

It is important to note that the evaluation phase may also lead to the fact that some design criteria should be added, deleted or modified. This is because the empirical studies made during the method application and the subsequent evaluation may lead to new insights that call for changes regarding the normative assumptions that underlie the design criteria. Thus, the specified design criteria should not be fixed but open to revisions if good reasons can be presented (such as empirical evidence or other convincing arguments). In addition, even the overarching purpose of the method may need to be revised in the light of new knowledge gained in the method development process.

4.1.3 Summary and reflections on the design process

The method development process, as depicted and described above, is somewhat simplified as compared to when it is actually implemented. What is not really captured in Figure 4-2 (for clarity reasons) is the *iterations* between the various steps of the process. Especially important are the iterations between the specification of design criteria and the other steps. The figure *could* be interpreted in the sense that an exhaustive and fixed list of design criteria is first specified, followed by the method construction in accordance with these criteria. However, these steps are more intertwined, since while constructing the method, given an initial set of criteria, insights and new knowledge may lead to additional criteria or revisions of existing criteria.

In principle, an extremely large set of design criteria could be specified. In general, though, the design criteria specified first will have a large influence on the method characteristics. But as more design criteria are specified they will have lesser impact, thereby putting an upper limit on the number of design criteria that are sufficient, since additional criteria would only have marginal effects on the method characteristics. Of course, in principle, the method development process could go on perpetually, continually refining and adding design criteria, and improving the method.

In summary, the proposed design process aims to increase the scientific rigor of the method development. This is acheived by approaching the design problem systematically and using a transparent process where normative assumptions (purpose and design criteria) are clearly stated and the method choices directed by those assumptions are justified using a logical line of reasoning.

4.2 Interviews

Interviews have been performed within several of the papers. The purpose of the interviews has varied between the papers and between different phases of the research. The aim of some of the interviews, especially related to the research questions about technical infrastructure networks, has been to gain rather general background knowledge of some activities or systems of interest. These interviews can be termed *explorative* (Kvale, 1997), and have sometimes been combined with the author's introducing the research project and inquiring whether data about some existing infrastructure system (e.g. the electric distribution systems analysed in papers I and II) is available. The explorative interviews have been rather loosely structured and documented by taking notes.

The aim of some other interviews, especially those performed within paper V related to evaluating municipal RVAs, has been to gain deeper understanding of some activity or aspects of an activity. These interviews can be termed semi-structured (Dunn, 2005), since a rather detailed interview protocol has been used to ensure that all relevant topics are covered. At the same time, the interview design has allowed for some flexibility in the ordering of the questions, follow-up questions, etc.

4.3 Document studies

Document studies have been performed, more or less, in all but one paper. In papers I-III (related to technical infrastructures), it is primarily documentation from the infrastructure owner regarding the systems' functioning and structure. No specific structured text analysis method has been necessary, since in the cases where large documents have been studied it has only been a small part of these that have contained information of interest. Paper V, on the other hand, used content analysis (Weber, 1990) to study the documentation from a number of analyses performed by Swedish municipalities as well as when deriving the purpose of these from legislative texts. The general approach has been to define a number of categories or themes of interest (e.g. *purpose of the analysis*). For each theme a number of relevant key words (*purpose, goal, aim, intention, objective, etc.*) were used to identify segments of the text that may address the theme of interest. The identified text segments were then used to interpret and draw conclusions regarding how the documentation addressed the particular theme studied.

4.4 Survey

The empirical study in Paper VI used a survey to elicit the preferences expressed by participants. Two different elicitation procedures were used in order to gain

insights about e.g. uncertainty of the elicited weights. The details of the elicitation procedures, e.g. how they were designed to address validity and reliability issues, are described in Paper VI. In order to facilitate both the data collection and the subsequent statistical data analysis, the survey was implemented in computer software that could then be accessed online. The elicitations were carried out in a classroom setting where each participant had a computer on which the online survey could be accessed. Before initiating the elicitation, the tasks to be completed by the participants were presented and explained. During the whole elicitation process, facilitators were present to answer any questions that arose, and at the end of the survey, the participants were asked to reflect on the elicitation procedures.

4.5 Evaluation seminars

In paper IV the proposed framework for analysing emergency response systems was applied in a pilot case study where the authors acted as analysis coordinators for a group of municipal actors. The framework was applied during a number of seminars where the municipal actors received extensive guidance in using the framework. Since the main purpose of the pilot case study was to evaluate whether the framework could be applied in its intended context, as well as to gain insights regarding perceived benefits and difficulties related to the framework application, these seminars are referred to as evaluation seminars.

4.6 Computer programming and simulation

Computer programming and simulation has been used extensively in several of the papers. In papers I-III, Matlab and Microsoft Visual Studios have been used to enable the application of the methods for vulnerability analysis of technical infrastructure networks. This has been necessary because the amount of data that must be handled is vast, both in terms of input to the analysis and in terms of the output from it. Microsoft Visual Studios has also been used to create an interface for the framework for analysing emergency response systems (Paper IV) in order to facilitate execution and visualisation, and to design and manage the surveys in the study of preferences (Paper VI). Matlab was then also used to perform the statistical analyses of the results from the surveys.

4.7 Summary of methods for each paper and research question

Different methods described above have been employed in different papers and research questions. In Table 4-1 an overview of methods used in the different papers is presented. Below the methods used to answer each of the four research

questions will also be briefly summarised, which of course is closely related to the papers.

Table 4-1. Summary of methods employed in the six papers*.

Research question	Paper	Design process	Interviews	Evaluation seminars	Document studies	Survey	Computer programming/ simulation
	I	X	x		x		X
1	II	X	x		x		X
	III	X	X		x		X
2	IV	X		X	x		x
3	V	X	X		X		
4	VI					X	x

* X means that the method has been used extensively, x means that the method has been used but to less extent in the paper.

Research question 1 – Vulnerability analysis of technical infrastructure networks

Since this research question is about method development, the process described in Figure 4-2 has been employed. In this process both interviews and document studies have been used both to gain knowledge about how the systems of interest function and to elicit data about the structure of the systems in some specific area of interest. Computer programming and simulation has also been used extensively to implement the ideas from suggested methods and analytic measures so that the applications, demonstrating feasibility, become practically possible.

Research question 2 – Post-event RVA of emergency response

Similar to research question 1, answering this question has also been addressed by employing the method development process presented in Figure 4-2. Computer programming has been used to create a computer interface that facilitates the employment of the suggested framework for post-event RVA. Document studies were used to gain initial information about the emergency and response to the emergency in the application of the framework. The framework was then applied during a number of seminars where the participants were people with central roles in the response. The aim of the seminars was to perform an initial evaluation of the framework and have the participants reflect on the analysis processes.

Research question 3 – Municipal risk and vulnerability analyses

This question has both a normative and a descriptive part. The normative part concerns evaluating a number of municipal RVAs and suggesting how they can be improved. Since this essentially is a design problem, the main ideas of the design

process presented in Figure 4-2 were used, which essentially constitutes specifying the purpose/purposes of municipal RVA against which the evaluation will be performed and specifying concrete characteristics and functions that the municipal RVA should have in order to fulfil the specified purposes. Empirical studies of a number of municipal RVAs have then been performed to gain insights regarding the practises of municipal RVAs, which constitute the descriptive aim of the research question. Document studies and interviews have been used for data collection. The empirical studies have then been used as the input to the evaluation, where the characteristics of the studied RVAs and the characteristics argued to be desirable have been compared. The comparison was finally used as a basis for considering improvements.

Research question 4 – Empirical study of preferences

The empirical study of preferences used two preference elicitation procedures that were implemented in a computer-based survey. The computed-based survey aimed to facilitate the data collection and the subsequent analyses. Statistical regression analysis techniques were used to draw conclusions regarding the importance of different attributes. The survey also included a small questionnaire where the participants were asked to describe how they had reasoned when completing the survey. Insights from these answers were also used to draw conclusions regarding the studied attributes.

4.8 Demarcations

There are obviously many strategies for improving society's emergency management. The strategy chosen in this thesis is through the performance of risk and vulnerability analysis. However, this choice is not made based on an analysis of the relative effectiveness of different strategies. The choice is rather based on an assumption that efforts related to RVA can have a high impact on society's emergency management. This can be seen as a limitation of the present thesis.

To a large extent, the thesis departs from and focuses on a Swedish context, and few efforts have been devoted to explicitly consider the relevance of the research for other parts of the world. However, due to the extensive similarities between many aspects of western societies it is likely that many principles and findings of the present thesis can be generalised to other western countries as well.

One of the aims of the thesis is method development, but to a large extent the method development is still in a rather early stage. This means that they have not been formalised to the extent that enable easy applications by external actors. What is needed to facilitate applications by practitioners is better method support in terms of e.g. guidelines, computer-based software and the like. This essentially

constitutes work aiming at developing the suggested methods into tools, but is outside the scope of the present thesis.

Another consequence of the early stages of the method development is that only a single or a few loops in the method development process have been carried out (see Figure 4-2). Although additional method applications would contribute to the development of the method (in terms of quality and substantiation), it is outside the scope of this thesis.

5 Results and research contributions

This chapter will present the main results and research contributions of the thesis. First, brief overviews of the appended papers will be given, which highlight the themes of the papers and the most important findings. Then, each research question posed in Chapter 2 will be addressed in more detail. For publications that are co-authored short summaries of the author's contributions are given. This is done by stating whether the author's contribution is *major* (more than 2/3), *medium* (1/3-2/3) or *minor* (less than 1/3) for different aspects of the work.

5.1 Brief summaries of papers

5.1.1 Paper I[43]

Johansson, J., Jönsson, H. and Johansson, H. (2007), "Analysing the vulnerability of electric distribution systems: a step towards incorporating the societal consequences of disruptions", *International Journal of Emergency Management* **4**(1): 4-17.

In paper I a method for analysing the global vulnerability of electric distribution systems is presented. The field of network analysis was used as a point of departure in developing the method. However, since network analysis mainly uses topological measures of system performance, efforts were made to develop measures to provide greater account of the functional characteristics of the systems. In addition, in evaluating consequences of failures, network studies of infrastructures have mainly focussed on the technical aspects of the system. In this paper it is argued that if analyses are to be useful in a societal context, societal aspects of the consequences must also be depicted. The suggested method is used for analysing two electric distribution systems located in two Swedish municipalities. The conclusion is that the proposed method is useful especially when the purpose is to perform an overall analysis of an electric power system, and it increases the value of using network analysis in this context. Although the method was adapted to electric distribution systems, the ideas can be extended to other levels of electric power systems, as well as to other technical infrastructure networks.

The author's contribution: The author played a *medium role* in planning the study, deigning the method, collecting the data about the system to which the method

[43] Paper I is an updated and extended version of a conference paper presented at CNIP 2006 (Johansson et al., 2006a).

was applied, performing the simulations and writing the paper; and a *minor role* in the implementation of the computer code.

5.1.2 Paper II[44]

Jönsson, H., Johansson, J. and Johansson, H. (2008), "Identifying Critical Components in Technical Infrastructure Networks", *Journal of Risk and Reliability* **222**(2): 235-243.

In paper II a method for analysing critical components of a technical infrastructure network is presented. Here, the criticality of a component, or set of components, is defined as the vulnerability of a system to failure in the component/set of components. More specifically, the criticality of a component or set of components is estimated in terms of the magnitude of the negative consequences given failure. Similar to paper I, the method suggested in paper II departs from network analysis but makes an effort to account for functional characteristics of the system of interest. The purpose of the method is to be able to perform analyses of large technical infrastructure networks. In addition, the interest is in being able to analyse several simultaneous failures. One difficulty that arises is that the number of combinations of failures may be vast. Therefore, a procedure for screening among sets of failures is suggested in the method. The method is applied in analysis of both a fictive and a real electric distribution system in a Swedish municipality. Although the application was made in the context of electric distribution systems, the ideas are relevant for other technical infrastructures as well. The conclusion is that the proposed method facilitates the identification of critical components and sets of components in large-scale technical infrastructures.

The author's contribution: The author played a *medium role* in planning the study, designing the method, collecting the data about the system to which the method was applied, performing the simulations and writing the paper, and in implementing the computer code.

[44] Paper II is an updated and extended version of a conference paper presented at ESREL 2007 (Jönsson et al., 2007b).

5.1.3 Paper III[45]

Johansson, J. and Hassel, H., "An Approach for Modelling Interdependent Infrastructures in the Context of Vulnerability Analysis", submitted to *Reliability Engineering & System Safety*.

In paper III an approach for modelling interdependent infrastructure systems, with the purpose of using it for analysing vulnerability, is presented. In the approach the systems of interest are modelled in terms of a structural model, similar to what is done in network analysis, and in terms of a functional model, aiming to capture the most important functional aspects of the systems. In addition, in the approach both functional and geographic dependencies between the infrastructure systems are captured. Furthermore, in order to gain as complete a picture of the vulnerability of the systems as possible, the vulnerability is analysed from three perspectives: global vulnerability, critical components and critical geographic locations. The suggested approach is then applied by modelling and analysing the railway system in southern Sweden, which consists of five systems and interdependencies among them. Although some of the data on the railway system are fictional, it is shown that the modelling approach can be used for vulnerability analysis of interdependent infrastructures.

The author's contribution: The author played a *medium role* in planning the study, collecting the data about the system to which the method was applied, in designing the method, performing the simulations and writing the paper, and a *minor role* in the implementation of the computer code.

5.1.4 Paper IV[46]

Abrahamsson, M. Hassel, H. and Tehler, H. (2010), "Towards a systems-oriented framework for analysing and evaluating emergency response", *Journal of Contingencies and Crises Management*, **18**(1): 14-25.

In paper IV a framework for analysing and evaluating the emergency response in past emergencies is presented. The aim of the framework is to enable the analysis and evaluation of emergency response that included several sectors and

[45] Paper III updated and extended version of a conference paper presented at the joint ESREL 2008 and 17th SRA-Europe Conference (Johansson and Jönsson, 2008). This paper was invited for possible publication in the Special Issue "Selected papers from ESREL 2008".

[46] Paper IV is an updated and extended version of a conference paper presented at PSAM9 (Abrahamsson et al., 2008) and to lesser extent also on a paper presented at the 14th TIEMS annual conference (Jönsson et al., 2007a).

organizations. The framework development was guided by four key challenges that are argued must be addressed in this context: 1) issues related to the values governing the evaluation, 2) issues related to the complexity of the systems involved, 3) issues related to the validity of the information on which the analysis and evaluation are based, and 4) issues related to the limiting conditions under which the emergency response system operated. A key characteristic of the framework is that an explicit system model of the emergency response is generated based on the views and perceptions of the involved actors. The main benefit of the model is that it increases the actors' understanding of the emergency response as a whole. Furthermore, the model is also used as a basis for analysing counterfactual scenarios, i.e. scenarios that did not occur but could have had any circumstances been different. It is argued that analysis of counterfactual scenarios makes it possible to draw more extensive conclusions about the emergency response. The main conclusion of the paper is that the proposed framework can provide important insights and information that are highly useful as a basis for preparing for future emergencies.

The author's contribution: The author played a *medium role* in designing the framework, in planning the study and in writing the paper and a *minor role* in applying the framework in the case study and in developing the computerized interface used during the pilot case study.

5.1.5 Paper V

Hassel, H. "Risk and Vulnerability Analysis in Practice: Evaluation of Analyses Conducted in Swedish Municipalities", submitted to *Natural Hazards.*

In paper V an empirical evaluation of a number of Swedish municipal risk and vulnerability analyses is carried out, and based on the evaluation a number of suggestions for improvements are given. A design science approach is used for the evaluation in which the purpose, or purposes, of the RVA must first be specified. In the paper, two different purposes for the municipal RVAs were derived from Swedish legislation: using the RVA as a basis for risk-related decisions, and that the RVA process itself should contribute to reduced risk and vulnerability. From these purposes a number of characteristics and functions considered as being *desirable* for the particular purpose were explicitly specified and justified. The specified desirable characteristics were then compared with the characteristics and functions of the analyses studied. Both interviews and documentations were used as a source of information for the evaluation. The conclusion was that the analyses studied have several characteristics and functions that can be considered desirable, but that there is also potential for improvements. One interesting finding is that the most emphasized purpose, according to the interviewees, is that the processes themselves

should contribute to reduced risk and vulnerability rather than using the analyses as input to decisions, which is the most commonly expressed purpose of risk and vulnerability analyses in the research literature.

5.1.6 Paper VI

Hassel, H., Tehler, H. and Abrahamsson, M. (2009), "Evaluating the Seriousness of Disasters: An Empirical Study of Preferences", *International Journal of Emergency Management* **6**(1): 33-54.

In paper VI an empirical study of people's preferences for different disaster characteristics is presented. A total of 81 persons (students) evaluated the seriousness of disasters described in terms of four basic attributes (and their ranges): number of fatalities (0–1000), number of serious injuries (0–4000), economic loss (SEK 0–40 billion) and cause of the disaster (natural, accidental, terrorism). Since it is impossible to eliminate all biases in value elicitations, two fundamentally different methods were used to gain insights into how important the attributes are relative to each other. In the study, the results from the two methods differed somewhat, but the ordinal relation between the attributes was generally the same. Most participants regarded the attributes related to physical harm (especially the number of fatalities) as most important, a finding that must be seen in relation to the ranges of the attributes. Interestingly, although generally being the least important attribute, the cause of a disaster actually seemed to affect many of the participants' judgements of its seriousness. The results may be of use in the context of risk analysis and risk-related decisions, especially when value elicitations are not carried out on those stakeholders who are relevant in the specific situation.

The author's contribution: The author played a *major role* in planning and designing the study, in collecting and analysing the data and in writing the paper, and a *minor role* in implementing the questionnaire in the web-based interface.

5.2 Addressing the research questions

Comments on the structure of the answers to the design research questions

Questions 1a, 1b and 2 deal with method development, and the general research strategy used to answer these questions has therefore been the suggested method development process. The model described in Figure 4-2 will therefore be used to structure the answer to these questions. First, the *purpose* of the design will be described. Second, the *method construction process* will be described. This includes the steps "specify design criteria" and "construct method" (from Figure 4-2). These

two steps will be described in parallel since they interact iteratively. More specifically, initially one or several *general design criteria* (DC) will be presented and *justified*. Then the *implications* of these design criteria regarding desirable method characteristics will be described, as well as any method choices made. *Given* these implications and method choices, more specific design criteria can be described which leads to new implications and choices. This process can then continue a number of cycles before a final method proposal can be summarized. An illustration of the method construction process is given in Figure 5-1. Third, a short description of how the methods have been used is given. Finally, insights gained from these applications will be highlighted when evaluating and learning from their use.

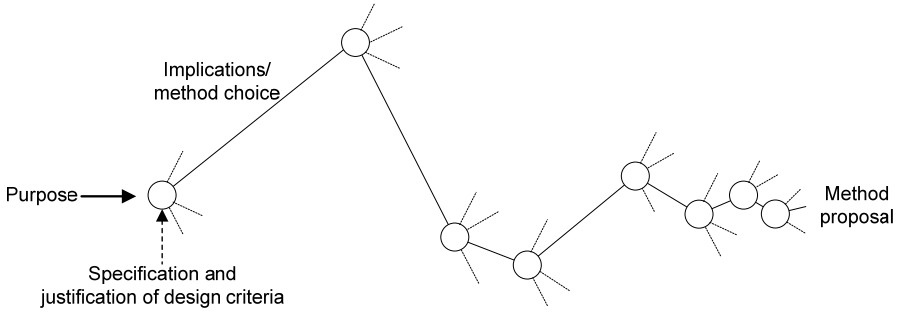


Figure 5-1. An illustration of the method construction process. Dashed lines symbolize choices regarding method characteristics that *could* potentially have been made. The purpose of making these explicit is to emphasise that method choices made early in the process significantly affect those made later in the process.

5.2.1 Research question 1a

Paper I (global vulnerability analysis) and Paper II (critical components) comprise the basis for answering research question 1a, which is: *how should a method for analysing the vulnerability of single technical infrastructure networks be designed?*

Purpose of the method

Based on the discussions in Chapter 1.4.1 and 2.2, the following purpose can be stated for the method:

> *The purpose of the method is to comprehensively analyse the vulnerability of technical infrastructure networks, especially accounting for large-scale perturbations, which can be used in practise as a basis for societal decisions regarding how to reduce the vulnerabilities of these systems.*

The method construction process

DC 1: The method should be based on the operational definition of vulnerability presented in Chapter 3.

Justification 1: All methods for vulnerability analysis must be based on some underlying definition of the concept. In many method suggestions, however, the conceptual foundation is rather vague or at least implicit, which reduces the scientific rigor of the approach. The operational definition of vulnerability presented includes the essential elements of a definition of vulnerability and is applicable to essentially any type of system (see Chapter 3.2 for arguments on the feasibility of the definition).

Implication #1: The implication of using the operational definition of vulnerability as a point of departure is that the method for vulnerability analysis should aim to assist in answering the following questions: What can happen, given a specific perturbation? How likely is it, given that perturbation? What are the negative consequences? The process of answering these questions thus constitutes the generation of risk scenarios, and the end product is basically a list of scenarios with their consequences and probabilities (contingent on the perturbation), and this list of scenarios should be complete and disjoint.

DC 2a: Both analysis of global vulnerability and critical components should be included in the method.

Justification 2a: As was described in Chapter 3.2 there are two slightly different perspectives on vulnerability: one where the interest is in a *system*'s vulnerability to various types of perturbations (a global property here termed "global vulnerability"), and another where the focus is on components within the system that are critical for the functioning of the system (a local property termed "critical components"). In a vulnerability analysis, it is important to capture both these perspectives. Looking at the system as a whole provides an overall view of the system's susceptibility to various perturbations. However, it does not necessarily yield any direct indications of what components contribute significantly to the overall susceptibility. This latter information is essential, though, when the goal is to use the analysis in practise as a basis for decisions regarding vulnerability reductions, which is one of the goals of the present method development.

DC 2b: The method should be able to comprehensively analyse the vulnerability of technical infrastructures to large-scale perturbations, without leading to impractical computational times.

Justification 2b: The purpose of the method stated that it should be able to analyse large-scale perturbations and at the same time be applicable in practise. This means that computational time, given the practical constraints regarding computer power, must be practically feasible. Access to some "supercomputers", e.g. similar to the ones used for simulations at Sandia or Los Alamos National Laboratories, should thus not be a prerequisite for being able to use the method. Computational time is a big issue when it comes to multiple simultaneous failure, and it often leads to analyses that are limited in scope in terms of only considering single failures, e.g. the one performed by Koonce et al. (2008), or that the method "is implemented not via an exhaustive search but rather via a partial assessment" (Mili et al., 2004, p. 40). However, only addressing single failures or conducting excessively partial analyses may fail to capture many important insights regarding the vulnerability – especially unexpected and concealed vulnerabilities.

Another common way of reducing computational times and making analyses more practical is to consider only very small portions of a technical infrastructure at a time. Of course, there will always be a trade-off between the level of detail in the modelling and how comprehensive a portion of a system can be included. Both extremely detailed but very narrow methods and rougher but more comprehensive methods are definitely needed. In the present thesis, the focus will be on the latter, i.e. striving to make appropriate abstractions in order to be able to capture the broad picture.

DC 2c: The method should be flexible enough to accommodate any type of technical infrastructure network.

Justification 2c: One purpose of the method is to be able to analyse any technical infrastructure network (electrical power, water distribution, transportation, information systems, etc.). Luckily, there are many commonalities between technical infrastructure networks, e.g. they are built in geographically distributed networks, they provide vital services to society, various commodities traverse the networks, they are vulnerable to internal (component failures) and external (natural hazards, malicious acts) events. These commonalities can be exploited to construct a method that is applicable to all these systems (or at least a wide array of them). Since there are differences between the systems, the method must be flexible to allow accounting for these differences. In addition, since the method is used as an input to research question 1b (the modelling of interdependent systems), the approach should be designed so that it is easily expandable.

Implication #2: The four design criteria described thus far are essentially about choosing or developing an appropriate modelling approach. Of course, several

modelling approaches that satisfy the criteria may exist. The approach that was judged to be most appropriate for the present method was network theory (see Albert and Barabási (2002), and Newman (2003) for overviews of this paradigm). The benefits of network theory are that it is very generally applicable to systems that are structured in network formations[47], it requires relatively little computational time (Eusgeld et al., 2009), and has been applied several times in the study of robustness and vulnerability of complex networked systems – focusing on both global and local properties of networks, see e.g. Albert et al. (2000), Holme et al. (2002), Albert et al. (2004), Crucitti et al. (2004a), and Holmgren (2006).

In network theory a system is represented as a network composed of nodes and edges. The main reason for studying the network representation of a complex system is that "structure always affects function" (Strogatz, 2001, p. 268). So by studying networks, it is possible "to understand and explain the workings of systems built up on those networks" (Newman, 2003, p. 224). A wide range of analytic metrics have been developed in this field describing different system characteristics; of course, different characteristics are relevant for different systems and interests. Since it is primarily the structure (topology) of the network that is studied in network theory, much of the functional and physical details of the infrastructure systems are abstracted away. The point of this is to enable a very broad and comprehensive approach rather than in-depth studies of single scenarios. If the network-theoretical analysis identifies vulnerabilities or criticalities, then other methods can be used for more in-depth studies (which will not be addressed in the present thesis). The use of several complementing methods for vulnerability analysis of technical infrastructure networks is in line with both the framework proposed by Eusgeld et al. (2009) and the multi-method approach suggested by Murray et al. (2008).

Most network analytic approaches to vulnerability analysis focus on global vulnerability, e.g. Albert et al. (2004), Crucitti et al. (2004c) and Holmgren (2006). This is done by successively removing components (nodes and/or edges) from the network while studying the degradation in the network performance (i.e. the negative consequences). If the performance is degraded "quickly" (i.e. very few removals are required to severely reduce the performance), the system is said to be vulnerable. Different ways of removing components from the network can be employed. These are referred to as *attack strategies* and represent different types of perturbations. The most commonly employed ones are random removal and

[47] Newman (2003) for example shows a wide array of applications in social, information, technological and biological systems.

directed removal, such as removing components in descending order of some measure of centrality that could represent some type of malicious act. The choice of what attack strategies to expose a system to depends on what types of perturbations are relevant in the particular context[48].

Some network-analytic approaches to vulnerability analysis also focus on local properties, e.g. component criticality or importance, e.g. Gorman et al. (2004), Apostolakis and Lemon (2005), Crucitti et al. (2005), and Jenelius et al. (2006). These and other approaches differ in one important sense: whether the probabilities of failures are included in the criticality measure or not (Aven, 2009). As *criticality* is defined in this thesis, probabilities are *not* included, i.e. a component's criticality is only related to the negative consequences *given* a failure. Excluding the probabilities when addressing criticality, however, is *not* meant to say that probabilities are irrelevant when making *decisions* regarding vulnerability reducing measures. They are highly relevant. But it may often be very difficult to properly estimate the probability or frequency of failures, especially when it comes to several simultaneous ones. Often one has to make assumptions, such as using generic failure frequencies or assume failure independences, which are not always valid (e.g. in the case of external perturbations, storms, malicious acts and common cause failures). As such, uncertainties are large and the assumptions may lead to large underestimations. The consequences of a given failure, on the other hand, may be rather straightforward to estimate. The suggestion is therefore here to first identify components that would give rise to large consequences if they fail. These are the components that must be especially robust, well-protected, reliable, etc. so that the failure probabilities are kept low. If this is not the case, measures should be taken. Thus, in order to make decisions about measures, the probability dimension should also be considered, but here it is not quantitatively integrated in the criticality measure.

The main reason for using network analysis is that it assists in answering the questions stipulated by the operational definition of vulnerability (see section 3.2). According to this definition vulnerability *is* a list of risk scenarios and their corresponding probabilities and negative consequences, *given a specific perturbation*. In the case of global vulnerability analysis, a specific perturbation is described by an attack strategy *and* a fraction (or number) of removed components. An example of

[48] It is also possible to combine purely random and directed removal. For example, if the interest is to study the vulnerability of an electric distribution system to storms, some edges may have a higher relative probability of failing (long overhead lines) than others (very short overhead lines or underground cables). This is rather easy to account for in the simulation and has been demonstrated in a Master's thesis (Nykvist and Ohlson, 2007).

such a perturbation is *1% randomly removed nodes*. Since these nodes are removed in a purely random fashion, any combination of 1% removed nodes constitutes a perturbation to the system. Each combination of 1% removed nodes thus constitutes an answer to the question: "what can happen, given a specific perturbation?" – i.e. each combination is a risk scenario. Furthermore, since the removal is random, each possible combination has an equal probability of occurring, which answers the question: "how likely is it, given that perturbation?". Finally, by estimating the negative consequences (more on this below in *Implication #3*), *given* the occurrence of a specific risk scenario, the last question, "if it does happen, what are the consequences?", is also answered.

When network analysis is applied to the study of large-scale infrastructure systems and the interest is in many simultaneous failures, the number of possible risk scenarios is enormous. This implies that it is practically impossible to identify *all* possible risk scenarios – i.e. the ideal of *completeness* is problematic. Instead, network analysis employs Monte-Carlo simulation where a large sample of all possible risk scenarios is drawn and the consequences of each are estimated[49]. The sample of risk scenarios drawn by the Monte-Carlo simulation is thus used to *represent* all possible scenarios. The result, when following these procedures, is a list of risk scenarios (the number being equal to the sample size), and their corresponding probabilities (the probability being equal to the inverse of the sample size) and negative consequences, which *is* the vulnerability of the system to the specific perturbation in question.

It is also possible to relate criticality to the operational definition of vulnerability. Criticality can then be defined as the *vulnerability of the infrastructure network to failure in the specific component/set of components*. Thus, the failure of a specific component or a specific set of components is assumed to constitute the specific perturbation to the system. By identifying all risk scenarios that can occur due to the perturbation and their corresponding probabilities and negative consequences, the vulnerability of the system can be estimated in accordance with the operational definition; and the more vulnerable the system is to failure in a specific component, the more critical is the component. In many cases, contextual factors can affect which consequences arise due to specific failures. In an electric power system, for example, the consequences of failures may depend on the time of year, time of day, and the power demands at the time of the failures, etc. Such

[49] The research group developed computer software used for simulation. The program is called NetCalc and it was developed using the Microsoft .NET framework. Later this program was implemented in a Matlab code that also included the code for analysing critical components.

conditions will therefore principally lead to the fact that several risk scenarios are possible given specific failures. In this thesis (in Papers I and II), however, the system modelling has been assumed to be *deterministic* in the sense that a specific failure or set of failures is related to only one risk scenario and therefore a single negative consequence. Such an approach is somewhat of a simplification, because it requires assumptions regarding the contextual factors in order to estimate what can be referred to as a "characteristic consequence" of the failure; however, it reduces rk are equivalent to Definitions in this fry, making the analysis practically feasible. feasible.

DC 3a: The method should more extensively account for functional properties of the technical infrastructure networks than do the prevailing methods.

Justification 3a: Many of the suggested network-based approaches for analysing the robustness and vulnerability of complex systems essentially neglect the functional properties of networks. For example, a common way to calculate network performance is in terms of the connectedness of the network[50]. Such an approach would not make a difference between different types of nodes – but for many types of networks the type of node matters (i.e. which function the nodes have). In an electric power distribution system, for example, generators, transformers and in-feeds play crucial roles, and if they lose the connection to the "customer nodes", it does not matter if the customer nodes are well connected – they will not have power supply anyway. Thus, even though a network analytic approach is adopted, it is possible (and necessary) to capture at least the essential functional properties of the particular network of interest[51] and choose a network performance measure that is adapted for that system. Of course, the more functional aspects that are captured, the more computationally demanding the simulation will become.

DC 3b: The method should focus on the degradation in the services provided by the infrastructures to society rather than only technical aspects of the system.

Justification 3b: Many of the existing network-based approaches focus mainly on the technical aspects, for example by characterising the network performance as the

[50] Connectedness can be characterised in terms of the "average geodesic length" for all pairs of nodes in the network. A geodesic length is the length of the shortest path, i.e. the number of nodes that have to be traversed between two nodes in the network.

[51] Accounting for some functional/dynamic aspects (e.g. capacity constraints, loads, etc.) of technical infrastructure networks has been suggested in e.g. Holme and Kim (2002), Motter and Lai (2002), Crucitti et al. (2004b), Kinney et al. (2005), and Michaud and Apostolakis (2006).

fraction of nodes that have lost contact to the network. Hence, what the effects are for the society that depends on the infrastructure services are not addressed. If a method for vulnerability analysis ought to be applicable in a societal context, then the network performance measures (measures of negative consequences) must be able to describe the societal consequences of disruptions and perturbations.

Implication #3: The general modelling approach adopted in the present thesis will differ between two types of models – one *structural* model and one *functional* model (see Figure 5-2). Taken together these models constitute the total system model. The structural model consists of the nodes and the connections between the nodes (i.e. the edges). In network theory, perturbations are represented as removals of nodes and edges in the structural model. The functional model describes the extent to which the system is able to provide its intended services. For example, a simple functional model for an electric power distribution system is that in order for a substation to have power supply a physical connection to an in-feed node must exist[52]. Hence, in the functional model assumptions regarding functional characteristics are implemented (which of course depends on the type of system that is modelled), and in order to evaluate the function the structural model is used as an input – since the structure affects the function.

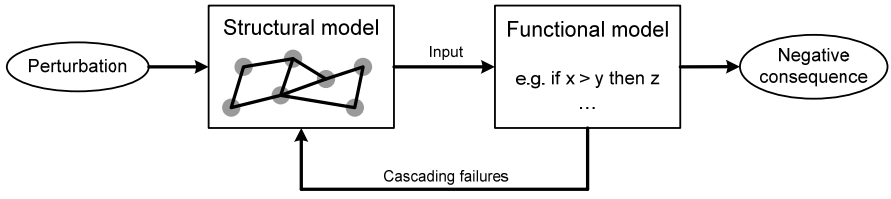


Figure 5-2. The distinction between structural and functional model when modelling technical infrastructure networks.

In order to account for the societal consequences of perturbations, the concept of *Customer Equivalents* (CE) is introduced. Each node in the network is characterised in terms of a CE that aims to express the magnitude of the societal consequences given that the node is out of function (i.e. cannot provide infrastructure services to the customers dependent on that node). Different factors may affect the CE for a node, such as number of customers, type of customers (e.g. hospitals vs. households), non-delivered services (e.g. unsupplied energy, quantities of water not

[52] This is the functional model used in paper I. In paper II, the functional model was refined to also account for the capacity of the in-feed nodes and the loads of the substations. Further refinements are of course also possible, for example by also accounting for capacity limits in the power lines, etc.

reaching the customers), etc. Note that the exact characterisation of CE will not be prescribed in the method since that depends on the type of infrastructure system of interest and the underlying values governing the analysis.

DC 4a: Aggregate metrics for expressing global vulnerability should be included in the method.

Justification 4a: The results from a global vulnerability analysis are usually plots expressing the network performance as a function of the number or fraction of removed components. By studying these plots, conclusions regarding the vulnerability of the system can be drawn. More specifically, if the curve is very steep (i.e. the network performance degrades very quickly) the system is vulnerable. However, it can be difficult to interpret these curves and be able to compare different systems and the vulnerability to different perturbations. Therefore, it would be very useful to have access to metrics that aggregate information from the performed simulations and express some interesting characteristics of the system related to vulnerability. Of course, at the same time it is important to acknowledge that the aggregation process may lead to a loss of relevant information[53].

DC 4b: A strategy for screening among possible combinations of failures in order to identify especially interesting ones should be included in the method.

Justification 4b: The aim when analysing component criticality is to enable the analysis of several simultaneous failures. However, when systems are fairly large, the "combinatorial explosion" leads to a vast number of possible combinations of failures. Even though the simulations can be performed within reasonable time, the output of the simulations becomes rather difficult to handle. Therefore, strategies for screening among failure combinations are useful so that especially interesting sets of component failures are highlighted.

Implication #4: A measure referred to as Societal Vulnerability Coefficient (SVC) is proposed to simplify the interpretation of the plots generated in the vulnerability analysis. SVC is a number between 0 and 1 and expresses the area beneath the curve shaped by the performance measure as a function of the fraction of removed components (e.g. from no to all removed nodes). An SVC close to 0 means that very small negative consequences arise due to the specific type of perturbation (e.g. only when the fraction of removed nodes is very large). An SVC close to 1 means

[53] This is analogous to the relation between the answers to the risk triplets, which is the outcome of a risk analysis, and risk measures such as the expected consequence.

that the negative consequences arise rather quickly (a small fraction of removed components are enough to degrade the system) due to the specific perturbation.

Another proposed measure is the Design Coefficient (DC). It describes the correlation between the order in which a particular node loses the infrastructure service, when exposing the infrastructure system to some type of attack strategy, and the Customer Equivalents of that node (i.e. describing the importance of that node). The DC is a relative measure that describes to what extent the infrastructure system is designed to provide more reliable services to the more important nodes than to less important nodes.

When analysing multiple simultaneous failures, the number of possible combinations of failures becomes very large. However, the consequences of many of these combinations of failures are *not* due to a *combined effect* of two failures, but rather due to the fact that one or several of the *individual failures in themselves* leads to large consequences. If this is the case, such individual failures will be identified when analysing the criticality of failures of single components. However, very few new insights would be gained if these components were identified as critical when analysing two (or more) simultaneous failures. What is interesting when considering several simultaneous failures is those combinations of components where the individual failures are not critical but where the combined effects of the failures lead to large consequences. Therefore, a screening strategy based on the magnitude of the *synergistic consequences* of several simultaneous failures is proposed. Synergistic consequence is defined as a consequence of two (or more) components that cannot be derived from the consequence of the individual failures (or individual subsets). When using the magnitude of synergistic consequences for screening among critical sets of components, more important information can be extracted from the simulations performed.

Summarizing the proposed method

The structure of the proposed method is presented in Figure 5-3. It consists of five basic steps where the first is about defining the problem. This, or similar, steps exist in essentially all methods of risk and vulnerability analysis and is therefore not highlighted here. The second step is about addressing the value basis for the analysis, i.e. what should be regarded as negative consequences. The present method operationalizes this through the concept of Customer Equivalents, as discussed in *Implication #3*. Step 3 is about generating a suitable model of the technical infrastructure network of interest and then implementing it in a computer program. More specifically, this is done in terms of a structural and a functional model, as discussed in *Implication #3*. In step 4, simulations are performed in order to characterise vulnerability. Simulations are conducted both

for analysing global vulnerability and for analysing critical components, as discussed in *Implication #2*. In the global vulnerability analysis, one must decide which attack strategies to employ, and in the analysis of critical components one must decide on how many simultaneous failures to consider. In step 5, the results from the computer simulations must be presented in some comprehensible way. The present method includes two ways of aggregating information from the global vulnerability analysis, and one way of screening among sets of critical components.

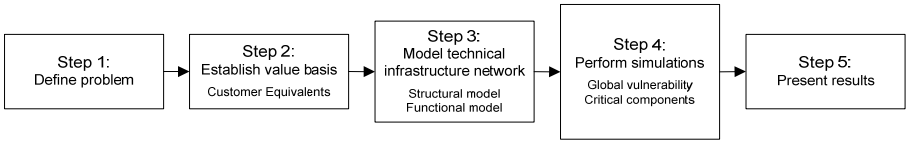


Figure 5-3. The proposed method for analysing the vulnerability of single technical infrastructure systems.

Use method

In paper I (global vulnerability analysis), and paper II (critical components analysis), the method was applied to both simple fictive infrastructure networks and real infrastructure networks. All applications have been performed by the method developers (i.e. the author and colleagues) in the context of power distribution systems.

Evaluate method and learn from use

The applications show that the method is feasible in terms of being applicable for comprehensive vulnerability analysis of fairly large systems, without impractical simulation times (here interpreted as a few days on a standard desktop). In addition, applications to simple fictive networks were useful for achieving a sense of the reasonableness of the analysis results. If only large complex systems had been analysed, it would have been more difficult to identify possible flaws in the method or in the implementation of the method in the computer code.

Establishing the value basis is important in vulnerability and risk analysis. The introduction of Customer Equivalents in the method is claimed to constitute a very simple way for enabling the integration of the value basis in the vulnerability analysis. The applications of the method in Papers I and II, however, have not focussed on this step since it would have required close interactions with relevant decision-makers and stakeholders in the systems, similar to the applications of Apostolakis and colleagues (Apostolakis and Lemon, 2005; Michaud and Apostolakis, 2006; Patterson and Apostolakis, 2007; Koonce et al., 2008). Instead, only rough assumptions have been made by the authors regarding CE. The

recommendation is that when the method is applied in practise, the analysts should assign the CE based on the values that are relevant for that particular analysis.

The application showed that it may be challenging to handle some dynamical aspects of the systems because network modelling is primarily static. Electric distribution systems, for example, are often operated radially but built meshed. If a failure occurs it is possible to reconfigure the network and re-establish the power supply; however, this usually takes some time and requires actions from the operators. When using the present method, one must make assumptions regarding whether reconfigurations should be accounted for (thus ignoring outages during the time it takes to complete the reconfiguration) or not (thus ignoring the possibilities of making reconfigurations), and be aware of the effects of these assumptions.

The functional models of electric distribution systems used in Papers I and II have been rather simple (connectivity model in Paper I and a simple capacity model in Paper II). Nothing in principle prohibits the use of more advanced functional models, which of course would require more data on the systems of interest. The main disadvantage of more advanced functional models, though, is the increased computational time; and since the main goal of the method is broad and comprehensive analyses, very advanced functional models would be difficult to implement. With another purpose for the method, e.g. in-depth analysis of individual scenarios, more advanced functional models would definitely be appropriate.

In the applications it was found that an effective way of using the methods is to compare the simulation results between different systems, different perturbations, and the same system but with and without some vulnerability reduction strategies, etc. Performing such comparative analyses, e.g. in relation to some reference or benchmark system, may yield useful results in addition to analyses of individual systems.

Summary of research contributions

In summary, a method for analysing the vulnerability of technical infrastructure networks has been suggested and tested in small-scale case studies. The method, which has been developed using a structured design science approach, draws on ideas from network analysis and includes two complementing perspectives on vulnerability – global vulnerability and critical components.

5.2.2 Research question 1b

Paper III comprises the primary basis for answering this question. But since the question essentially is a follow-up question to Research question 1a, Papers I and II are also relevant. The question is: *how should a method for analysing the vulnerability of multiple interdependent technical infrastructure networks be designed?*

Purpose of the method

Based on the discussions in Chapter 1.4.1 and 2.2, the following purpose can be stated for the method:

> *The purpose of the method is to comprehensively analyse the vulnerability of multiple interdependent technical infrastructure networks, especially accounting for large-scale perturbations, which can be used in practise as a basis for societal decisions regarding how to reduce the vulnerabilities of these systems.*

Method construction process

The method addressed in this research question is essentially an extension of the method developed for single infrastructure systems. The same design criteria have therefore also guided the development of the present method – these will therefore not be repeated here. In addition, a number of additional design criteria are specified.

DC 1a: The method must be able to model functional and geographic dependencies[54].

Justification 1a: Since the purpose of the method is to be able to account for dependencies between infrastructure systems, some way of modelling them must be implemented. There are many proposed categorisations of interdependencies and dependencies in the literature; see e.g. Rinaldi et al. (2001), Zimmerman (2001), and Lee et al. (2007). These have in common that two different types of

[54] An *interdependency* is usually defined as a *bidirectional relationship* between two infrastructures (Rinaldi, 2004). Most often they constitute macro-properties of interconnected systems rather than relationships between individual components of two different systems. A *dependency*, on the other hand, is a *unidirectional relationship* between systems or components, and dependencies often also exist between components in two different systems, i.e. on a micro level. In this thesis, infrastructure interdependencies will be modelled by explicitly modelling the relations between the components of the infrastructures, i.e. the dependencies. Therefore, the term dependencies will predominantly be used.

dependencies are distinguished, although both the terminology and level of detail differ. The two types are here referred to as *functional* and *geographical* dependencies.

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

Vulnerabilities due to functional dependencies have been exploited in several past events, e.g. the storm Gudrun (Energimyndigheten, 2005) and the 1998 Ice Storm in Canada (Chang et al., 2007). This has also been the case with respect to geographical dependencies, such as in the Kista power disruption (Deverell, 2003) and Hurricane Katrina (Leavitt and Kiefer, 2006). Furthermore, in many cases it is actually a combined effect of functional and geographical dependencies that determines the severity of the negative consequences due to strains. As such, this points to a need for including them in vulnerability analyses.

DC 1b: The method should be able to analyse critical geographic locations

Justification 1b: One of the goals of this method development is that the analysis should be comprehensive, especially in looking beyond the N-1 criterion frequently used to design critical infrastructures (IRGC, 2006). In the method for analysing the vulnerability of single infrastructures, two perspectives (global vulnerability and critical components) of vulnerability were used to strive towards a comprehensive picture of vulnerability, recognising that all possible risk scenarios cannot be captured. These two perspectives are relevant also when considering multiple interdependent infrastructures. However, since the issue of gaining a comprehensive picture of vulnerability is exacerbated, a third perspective of vulnerability should be added, namely analysis of critical geographical locations; see Patterson and Apostolakis (2007) and Jenelius and Mattsson (2008) for two examples. In an analysis of critical geographical locations, the goal is to identify geographic areas where components and infrastructures are co-located, i.e. there are geographical dependencies, making the locations critical should any hazard, such as

adverse weather or malicious acts, expose the area. Analysis of critical geographical locations may of course be relevant for single infrastructure systems as well, but it becomes even more relevant for multiple infrastructures where there may be different system owners that are not aware of where other systems are located.

In most method proposals for analysing interdependent infrastructures, a single perspective on vulnerability is adopted. However, if several perspectives on vulnerability are employed, it is argued that a more comprehensive analysis is enabled.

Implication #1: The same general method and modelling approach as used in the analysis of single infrastructure networks is used for the case of multiple interdependent infrastructures. This for example includes separating between a structural and a functional model of the individual systems. When modelling the interdependent infrastructures, the structural models of the systems constitute the interface between the various systems. The functional dependencies between the systems are modelled as *dependency edges* between two nodes *or* edges in two different systems. For example, if a fresh water pumping station is dependent on a power supply, it is modelled as a dependency edge to the node in the power system that supplies the pump. If the node in the electric power system is not able to provide its intended service, the dependency edge to the pumping station in the fresh water distribution system is removed. The effect of this removal is evaluated in the functional model of the fresh water distribution system, where a *functional condition* for the pumping station could be that a dependency edge to the power system must exist – otherwise the pump loses its function.

Hence the cascading effects between the infrastructures spread through the dependency edges. When a component not functions, its dependency edges (if any) to other systems are removed. As long as there are any changes in the dependency edges, the functional models are updated for the affected systems. This iterative loop is then continued until no more changes occur in the dependency edges.

Geographical dependencies are captured by simply specifying their geographic coordinates. The effects of geographic dependencies are then addressed when analysing critical geographical locations. More specifically, in the analysis of critical locations the geographic area is covered by grid cells. All components within a specific grid cell are then removed and the magnitude of the consequences that arise determines the criticality of that location.

Summarizing the proposed method

In Figure 5-4, the proposed method for analysing interdependent infrastructure systems is presented. It is an extension of the method proposed for single interdependent infrastructures that includes one additional step, modelling dependencies (both functional and geographical), and one additional perspective of vulnerability, critical geographical locations.

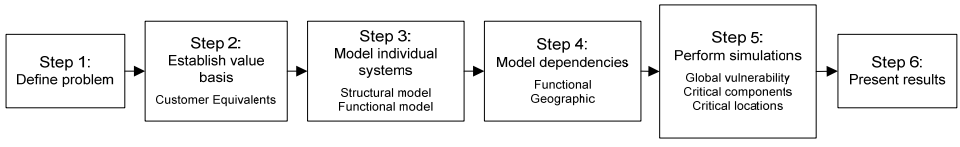


Figure 5-4. The proposed method for analysing interdependent infrastructure systems.

Included in the method is also a simulation model where the models of the interdependent infrastructures (steps 3 and 4) are used to perform simulations from the three perspectives of vulnerability.

Use method

The method has been applied in a case study of the railway system in southern Sweden, consisting of five interdependent infrastructures that must function in order for the operation of trains to function. The railway system was chosen primarily because there is essentially only one owner of the system, the Swedish Railway Administration. The case study primarily focused on the system modelling and simulation (steps 3-5). To some extent, fictional data was used since the main purpose of the application was to gain insights into the applicability and feasibility of the suggested approach to model and analyse the vulnerability of interdependent infrastructures.

Evaluate method and learn from use

The application of the method shows that it is feasible for analysis of large-scale interdependent infrastructures. Several perspectives of vulnerability could be addressed without an impractical simulation time. It should be noted, though, that some fairly rough assumptions have been made regarding the functional models of the infrastructure systems. In order to gain even more useful insights of the vulnerability of the system, these assumptions should be reviewed and possibly revised and refined. This should be done together with stakeholders and expertise from e.g. the Swedish Railway Administration. It is important that the effects of possible refinements on the simulation times are carefully considered. Only a slight

refinement, e.g. in terms of modelling the systems with slightly higher level of detail, could lead to much longer total simulation times.

The application shows that restoration times for different components in the infrastructures are very important for the vulnerability and criticality. In the application, rough restoration times were assumed for each system. The times differed between systems but not within a system. However, in reality there may be large variations in restoration times depending on several factors. One example is the capability of restoration crews. If a major strain affects the system it is likely that restoration times will be prolonged since there are not enough restoration crews, equipments, etc. Another example is the fact that the restoration time varies for different types of failures in a system.

Summary of research contributions

In summary, a method for analysing the vulnerability of multiple interdependent technical infrastructure networks has been suggested and tested in a railway case study. The method, which has been developed using a structured design science approach, includes three complementing perspectives on vulnerability – global vulnerability, critical components and critical geographic locations.

5.2.3 Research question 2

Paper IV comprises the basis for answering this question, which is: *how should a framework for post-event risk and vulnerability analysis and evaluation of emergency response systems be designed?*

Purpose of the framework

Improving emergency response capabilities is an important activity in the broader process of reducing risks and vulnerabilities in society. Gaining insights from past events and implementing changes that are influenced by those insights is one way of improving emergency response capabilities. The following purpose can be stated for the framework developed in the present thesis:

> *The purpose of the framework for post-event risk and vulnerability analysis and evaluation of emergency response systems is to gain insights into the functioning of the ERS in a past event that can be used to improve future emergency response capabilities.*

The framework construction process

DC 1: The framework should address issues related to the values governing the evaluation.

Justification 1: Values describe what are important to us and what we fundamentally care about. No analysis can be performed without a value foundation, since it would be impossible to know what aspects of the world one should focus on. Nor would any evaluation be possible, since value judgements are required to be able to draw conclusions regarding whether the performance of an emergency response system can be seen as successful/acceptable. Whether the emergency response was successful/acceptable simply depends on whether or to what extent the overall objectives, which can be stated for the emergency response, are achieved. In addition, values are also needed when suggesting and implementing changes to improve the emergency response systems, since an improvement per definition is about modifying a system in order to achieve a better fulfilment of the objectives.

Implication #1: Without explicitly specifying the values used as a basis for an analysis and evaluation, an implicitly assumed value basis will guide the evaluation. However, since the value basis is implicit, the actors involved may not have reflected on what they consider as important in the particular context, which would mean that their values are not necessarily well-represented by those implicitly assumed. In addition, by not treating values explicitly, there is no way of addressing and overcoming potential differences in the values held by different actors. Since all analyses and evaluations are guided by values, some actors may not accept the conclusions of the evaluation because their values do not correspond to the value basis of the evaluation. This would severely diminish the value of performing analyses and evaluations.

The approach chosen here is to first discuss and specify an overarching set of values for the particular emergency response operation that is common to all actors involved in the emergency response. More specifically, the values are specified in terms of a set of objectives for the emergency response as a whole. These objectives will of course be a very high, system-level description of the values guiding the emergency response. Often, in an emergency management context, they are related to meeting the needs of the affected population. Of course, different actors play different roles in the emergency response system, so even if an actor in principle agrees with the system-level objective, the objectives that guide a certain actor's actions will probably be much more adapted to its specific role in the emergency. In the end, though, the success of the emergency response depends on to what extent the system-level objectives are met; therefore, it is important that the objectives of the actions taken by various actors during the emergency response correspond well to the system-level objectives. Otherwise it could be questioned whether the role of the specific actor should be redefined. In summary, values

should be described explicitly in terms of system-level objectives. In addition, the objectives of the actions taken by various actors should be described, as well as their relations to the system-level objectives. These objectives will then guide the evaluation of the emergency response system.

DC 2: The framework should address issues related to the complexity of the systems involved.

Justification 2: An emergency response system can generally be described as a complex system that includes many elements of different kinds (both technical and social) as well as many different relations and interactions between these elements. Understanding such complex systems and designing good strategies for improving them is not an easy task. In these complex systems, one is not likely to find simple answers in terms of e.g. locating a "bad apple" (usually an individual) and subsequently deleting or replacing the "bad apple" leading to system improvements (Dekker, 2002). Instead, it is more likely that a large set of factors and their interactions together shape the performance of complex systems (Leveson, 2004), such as emergency response systems. As a consequence, in order to properly understand these systems, it is not enough to study parts of the system in isolation; the aim must rather be to strive for a broad view of the emergency response system, including interactions and dependencies between various parts of the system.

Implication #2: The present framework strives to deal with the issue of complexity by generating an *explicit model* of the emergency response, similar to what is done in e.g. Programme Theory (McLaughlin and Jordan, 1999). The model is primarily generated from the views and perceptions of the people who were involved in the emergency response. In addition, any available documentation from the event is also used. The primary goals of generating the system model are to create a common understanding of the events in question and to explicate how different actors involved in the response perceived the course of events. The model is then used as a starting point for discussions regarding the performance of the emergency response system as well as for broadening the analysis to also address counterfactual scenarios (see further below).

The process of generating the explicit model starts with mapping the actors involved in the emergency response. An actor could be a formal organization (e.g. county administration board), a part of an organization (e.g. municipal department), an informal group (e.g. volunteers) or a single person – depending on the level of detail that is appropriate for the analysis. The methods used in mapping the actors are document studies and interviews with involved actors. Interviews with key actors initiate a "snowballing process" (Wasserman and Faust,

1999), where additional actors are successively identified in the interviews. At some point, either new actors will not appear or the analyst must decide that the analysis is sufficiently complete.

The identified actors have performed some tasks and activities during the emergency response that may have affected how the events unfolded; the next step, therefore, is interviews with the actors to identify these tasks as well as the actors' objectives in performing the tasks. Of course, actors do not perform tasks in isolation from each other. The next step of the model generating process is therefore to map out what the actors were dependent on in performing the different tasks. Three categories of task dependencies are suggested in the framework, namely dependencies of *resources*, *technical infrastructures* and *other actors performing specific tasks*. In addition, the tasks performed by the actors also have effects on the surroundings of the actor, e.g. in terms of influences on other actors' task performance or on the needs of the affected population. These influences are also mapped out in this phase. Each dependency is characterised in terms of its *strength*, which implies how seriously the ability of performing a task is affected by e.g. the unavailability of a specific resource (on which the task performance depends). Finally, a system model for the emergency response as a whole can be constructed based on the data gathered when mapping the actors, tasks and dependencies. The purpose of the system model is to facilitate the understanding of the functioning of the emergency response, and it can be used as an input to discussions of the system performance.

DC 3: The framework should address issues related to the validity of the information on which the analysis and evaluation is based.

Justification 3: The issue of obtaining information about emergencies that have occurred is problematic. The main reason is that the information must often be elicited from people involved in the emergency, and this information may be distorted or incomplete for at least three reasons. First, each actor of course only perceives a very small part of the total emergency response, and it is not necessarily so that they even can remember everything of relevance after the event. Second, human memory is susceptible to several biases (Heath, 1998), and especially relevant here is hindsight bias (Fischhoff, 1975). Hindsight bias can result in people revising their perceptions of what happened in an event and how they experienced it based on information that became available and evident *after* the event. Third, it is common that people become reluctant to provide a full account of how they perceived and experienced the course of events. The reason is that they may fear being criticised or even punished because of their actions in the emergency response (Heath, 1998). Due to the existence of these three problems of

obtaining as complete an account as possible of what actually happened, it is important to consider and design the framework so as to minimise their negative effects.

Implication #3: Overcoming the issue of information validity is not an easy task – and it is not likely that the issue can be fully solved because of the complexity of most emergency response operations. The present framework addresses this in two different ways. First, each time the framework is employed it is important to clearly state and communicate that the purpose of using the framework is *not* to find scapegoats and people to blame, but rather to learn as much as possible from the response. Therefore, this is essentially about creating a relationship of trust between the analysts and the people involved in the emergency response so that they feel they can give their full account of the course of events. Second, cross-validation of information sources is used to alleviate the effects of memory biases. More specifically, cross-validation is a type of triangulation procedure where information about the same aspect of the emergency response is elicited from several sources. For example, in eliciting dependencies, each actor is first asked to describe what affected their ability of performing a certain task. Then each actor is also asked to describe what effects they perceived that the performance of their tasks had. Thus, it is possible to compare the statements of two actors regarding the same information. If there are any inconsistencies between their statements (e.g. actor A perceived its actions affected actor B's ability to perform a certain task but actor B did not perceive that actor A's actions had an influence), a dialogue between the two can be initiated and a consensus can be sought.

DC 4: The framework should address issues related to the limiting conditions under which the emergency response system operated.

Justification 4: One problem when analysing and evaluating emergency response operations is that conclusions of the system performance are often based on the final outcome of the emergency. Only using the outcome as a basis for the evaluation would hence lead to the conclusion that the response was good if no people were harmed and that the response was bad if there were many fatalities. However, limiting conditions may exist that keep the emergency response system from acting so that negative consequences are avoided. For example, if an explosion occurs that causes many *immediate* fatalities, the emergency response system could simply not have acted in any way to avoid these fatalities *independent* of how it was designed or how it acted during the response. Another limiting condition could be that *given the resources* available in the emergency response system at the time of the event, it could not have acted so the negative consequences would have been avoided. Only if the emergency response system had had access to another set of

resources could the negative consequences have been avoided. In such a situation, it is important not to conclude that the emergency response system performed badly, since they could not have acted in any way to avoid the negative consequences. Instead, it could be concluded that the emergency response system was simply not designed for handling the event (it lacked some essential resource), which subsequently of course could lead to a need for implementing some proactive measures.

Implication #4: It is important that any conclusions regarding how well the emergency response system performed take the limiting conditions into account. The present framework addresses this issue by stressing that an effort must be made to make the limiting conditions visible early in the analysis and evaluation – i.e. to describe what the preconditions were for the emergency response. When subsequently discussing and evaluating the emergency response system, the performance must be seen in the light of the limiting conditions.

DC 5: The framework should aid in broadening the scope of the possible conclusions that can be drawn, i.e. enable conclusions to be drawn regarding events other than the one from which the analysis commenced.

Justification 5: A common limitation of analyses and evaluations that are performed after an emergency has occurred is that the only focus is on that specific course of events. In only having this narrow focus there is a risk that e.g. an organisation only tries to improve their capability to respond to the same event if it should reoccur. However, obviously future emergencies will always differ in some way from past emergencies – often significantly. In addition, if the emergency response system becomes overly adapted to manage a specific event, there is a risk that the capability to handle other events is reduced. Therefore, it is desirable that frameworks used to analyse and evaluate the emergency response to past events aids in broadening the scope of the conclusions that can be drawn.

Implication #5: The present framework aids in broadening the scope of the conclusions that can be drawn from a past event by suggesting that counterfactual scenarios should be analysed. A counterfactual scenario is a scenario that did not occur but could have, had any of the system elements or environmental variables been in other states. For example, in the actual emergency that occurred, the weather might have been favourable. Assuming that the weather had been less favourable (e.g. much lower temperature, higher wind speeds) would constitute a counterfactual scenario, and the analysis of that scenario would concern how the actors' abilities to perform their tasks and the performance of the emergency response system as a whole *given* the new set of conditions would have been

impacted. A counterfactual scenario can be seen as a type of risk scenario from the operational definitions of risk and vulnerability, i.e. it is a description of a hypothetical future course of events. Since risk scenarios *contingent* on a specified set of conditions are addressed, the framework is termed post-event RVA.

In the framework it is suggested that counterfactual scenarios should be systematically analysed by altering all, or a chosen set (e.g. the most critical) of, system elements. The system model that was generated for the actual response is used as a point of departure for the analysis of counterfactual scenarios. Use of the model facilitates the understanding of the performance of the system as a whole, including how local changes in the system have repercussions for the system as a whole, since it explicates the relations between various elements in the system.

Summarizing the proposed framework

From the design criteria and their implications above, a framework can be suggested (see Figure 5-5). The framework consists of three main steps, where the first one deals with defining the preconditions of the post-event RVA. This especially includes clearly specifying any limiting conditions (discussed in Implication #4) and specifying the overall objectives for the emergency response (discussed in Implication #1). Step 2 constitutes the generation of the system model and the analysis of counterfactual scenarios. In step 3 the emergency response system is evaluated on the basis of the analyses performed, and conclusions are drawn regarding whether and how the system should be improved.

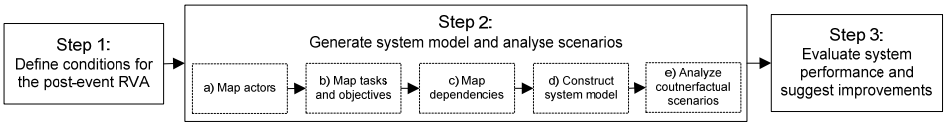


Figure 5-5. The proposed framework for analysing and evaluating emergency response operations.

Use framework

The framework has been employed in a pilot case study where the response operations in a municipality due to the severe storm Per were studied. Per struck southern Sweden in early 2007 and caused extensive and prolonged power outages and disturbances to telecommunication and transportation systems. A number of seminars were carried out, each involving 3-5 persons from various departments within the municipality. In the case study, step 2 was emphasised, especially in generating the system model of the emergency response operation.

Evaluate framework and learn from use

Although the case study constituted a small-scale application of the framework, it indicated that the framework can be applied in a practical context and provide important insights about the response operation. These insights in turn can provide a good foundation for preparedness planning.

In the application it was seen that the primary benefit of using the proposed framework for analysing and evaluating emergency response systems is that it increases the understanding of how individual actors affect other actors as well as the emergency response as a whole (in terms of to what extent the overall objectives can be met). This is especially due to the participatory generation of the explicit model of the emergency response. The explicit model further facilitates a structured way of thinking when it comes to what actually happened as well as when it comes to what could have happened given other circumstances.

One key challenge when it comes to using the framework in practise was choosing the appropriate level of detail when generating the system model. It is impossible to talk about a "correct" level of detail since this depends on the purpose of the analysis and the time and resources available to carry out the analysis. However, a too detailed model would lead to difficulties in both generating the model of the whole system of interest as well as interpreting the model. Too rough a model, on the other hand, would lead to a model with too low fidelity to say anything interesting about the actual system. It is likely that with increased practical experience with the framework, an appropriate level of detail will be easier to find.

Summary of research contributions

In summary, a framework for performing post-event RVA of emergency response systems has been suggested and tested in a pilot case study. The framework, which has been developed using a structured design science approach, is centred on developing an explicit system model, primarily based on the views and perceptions of the actors involved. The model aims at facilitating the understanding of the functioning of the emergency response system, and is used as a basis for discussions regarding the performance of the system as well as for discussions about counterfactual scenarios.

5.2.4 Research questions 3a and 3b

Paper V comprises the basis for answering the research questions 3a and 3b. The first of these questions is a descriptive one: *how are risk and vulnerability analyses carried out in Swedish municipalities?* The second question is normative: *how should the risk and vulnerability analysis processes (studied in question 3a) be improved?* Here

these questions are addressed simultaneously since they are closely related: the answer to question 3a was used as a basis for question 3b, and question 3b directed the attention of the empirical study in question 3a (this is further explained in the paper).

Design criteria for research question

Question 3b is a design research question, dealing with improving the practises of municipal RVAs. Design criteria should therefore be specified in analogy to the method development process previously described and applied.

DC1: The proposed changes should lead to improved fulfilment of the purpose as stipulated by legislation.

Justification 1: At the core of any design problem is the purpose (see section 4.1) and the evaluation and improvement of an artefact (such as a RVA) must be related to its purpose. Since the performance of RVA, at least partly, stems from a regulatory requirement the municipal RVA should fulfil the purposes as stipulated by Swedish legislation. Individual municipalities can of course have additional purposes; however, these are not addressed in the present research question.

DC2: The proposed changes should be feasible given the context of the RVA processes.

Justification 2: Changes in the RVA processes are suggested in order to obtain a better fulfilment of the stipulated purposes. One requirement when it comes to improving an artefact is good knowledge about the context in which the artefact is embedded (March and Smith, 1995); otherwise it is not likely that the changes are feasible. A contextual factor can for example be that the municipal staff has no experience in conducting RVAs. A proposed change that would require extensive experiences with RVA would therefore have small likelihood of leading to a successful outcome.

Purposes and desirable characteristics of the municipal RVAs

From the Swedish legislation, two purposes were derived which are relevant for the quality of the analyses at the municipal level. First, *the municipal RVA should generate a good knowledge basis for decision-making regarding risk and vulnerability reducing measures in the municipality*. Second, *the RVA processes should in themselves contribute to decrease vulnerability and risk through increased disaster response capability, enhanced safety culture, increased mental awareness, etc.* Since these purposes provide a rather high-level and abstract description of the municipal RVAs, more concretely expressed desirable characteristics and functions were

specified for each of these two purposes. The desirable characteristics were justified primarily using research literature and logical reasoning (and further described in Paper V).

Insights from the empirical study

A total number of eight municipalities were included in the study. However, in two pairs of municipalities the RVA processes were highly coordinated, which means that six *different* RVA processes were studied. The study was directed to create an overall understanding of the RVA processes and to gain insights regarding whether or to what extent the municipal RVAs had the characteristics and functions that can be described as desirable.

The overall focus of most analyses was primarily the municipal administration rather than the municipality as a geographic area (although there is overlap between the two perspectives). Several of the municipalities started the RVAs by mapping out values and objects that are especially important to protect in an emergency management context. In addition, all analyses included some phase in which a broad identification of undesirable events, or scenarios, was performed. Most often these two steps were carried out in brainstorming-like sessions. For each event identified, semi-quantitative estimates of the likelihood and negative consequences (e.g. on a scale of 1-4) were made in most analyses. Then, in-depth analyses of the emergency response capabilities were performed. These analyses were based on the broad identification of possible hazards and events, and most often only one event was chosen for in-depth analysis (in some case a few events were chosen). The analysis of emergency response capability was carried out in a table-top exercise where a hypothetical scenario was described and the participants then discussed how the scenario would have been dealt with. Finally, based on the discussion, including any possible identified deficiencies, measures for improving the response capability were suggested.

In five of the municipalities, specific analyses were performed in each municipal department/district, and in all of the analyses studied the municipal administration as a whole was also addressed, although two of these seemed to mainly consist of summaries of the results from the analyses performed at the municipal department/district level. Two of the analyses were slightly different in that a broad identification of undesirable events was carried out on a *multi-municipality* level, and then a complete analysis was performed at the municipality level with respect to a certain class of risk.

The participants in all analyses studied were essentially only people from the municipal administrations, and in many cases it was only people within a single

municipal department who interacted. Furthermore, in some analyses the participants were managers at the municipal officer level, whereas other analyses mostly involved operational staff. Still other analyses included a mixture.

Evaluation and suggestion of improvements

The evaluation was then carried out by comparing the desirable characteristics with the characteristics of the analyses studied. This evaluation, in turn, constituted the basis for discussing and suggesting potential improvements.

It was seen that several possibilities for improvements exist. One potential improvement for creating a better decisions basis is to increase the involvement of external actors who have relevant expertise, e.g. experts on various hazards, and strive to utilize existing data and scientific findings. However, since municipalities have limited resources, it is important that the supporting authorities assist in this process. In addition, in order not to negatively affect the fulfilment of the other purpose (benefits from the processes themselves) it is important that expert knowledge and empirical and scientific data are appropriately *integrated* in the analysis without losing its interactive and deliberative character.

Other suggested improvements include increasing the interaction between people from different municipal departments and increasing the involvement of external actors, including the public. Of course, this would require more resources; resources that perhaps are not available today. Therefore, this should be seen as a long-term goal and it requires that the role of RVAs in municipalities' prevention and preparedness activities is extended.

One interesting finding in the evaluation was also that many interviewees emphasised the importance of the RVA processes in themselves contributing to decreased risk and vulnerability, rather than using the outcome of the analyses as a basis for decisions. This is in contrast to the most commonly emphasised purpose of risk and vulnerability analyses in the research literature.

Summary of research contributions

In summary, the RVA practises in eight Swedish municipalities were studied and evaluated. The evaluation was performed using a systematic design science approach, with respect to two purposes as stipulated by Swedish legislation, and suggestions for improvements in the RVAs were specified in relation to each of the two purposes.

5.2.5 Research question 4

Paper VI comprises the basis for answering research question 4, which is: *how are people's judgments of disaster seriousness affected by the following disaster characteristics:*

- *number of fatalities in the disaster,*
- *number of serious injuries in the disaster,*
- *economic losses in the disaster,*
- *cause of the disaster.*

One problem for preference elicitations is that no method is free of bias, i.e. the elicitation procedures simply affect the preferences that are elicited from the participants, see e.g. Payne et al. (1999) for a discussion on the "construction" of preferences. Since different methods trigger different biases, the use of several methods can provide deeper insights regarding people's preferences; e.g. if the use of several different methods points at the same principal findings, one can be much more certain that the elicited preferences are rather valid. To this end, two fundamentally different methods were used to elicit the preferences.

The elicitations were performed using students as participants. Of course, ideally, a risk analysis should be based on values and preferences of people that are potentially affected by or otherwise relevant for the risk-related decision. However, since such elicitations are rarely performed in practise, elicitations from other groups, such as the one performed within this thesis, can be used as *one* input regarding what value basis should be used for the analysis. Of course, since the elicitation was performed on a rather homogenous group, one has to be cautious regarding how the results are generalised.

It is not appropriate to speak about how important different attributes are in general, e.g. without considering the possible values and ranges of the attributes. At the most extreme, if an attribute has identical values for all considered scenarios (e.g. 100 fatalities), the attribute should not at all affect people's judgment of how serious a scenario is compared to other scenarios. Therefore, it is important that the findings from studies like this are related to the ranges of the attributes considered. The present study considered the following ranges:

- Number of fatalities: 0 – 1000
- Number of serious injuries: 0 – 4000
- Economic losses: 0 – 40 billion Swedish Kronor
- The cause of the disaster: natural, accidental, act of terrorism

The two methods used in the study provided slightly differing results; however, the ordinal relation for the importance of the attributes was the same for most

participants. The study found that (given the ranges above) the number of fatalities was in general seen as the most important attribute, followed by the number of serious injuries. Economic losses and the cause of the disaster were in most cases seen as the least important attributes. At the same time, both these attributes seemed to significantly affect many people's judgement of disaster seriousness. Especially interesting is the fact that the cause of the disaster actually seems to affect several of the participants' judgements of disaster seriousness (where terrorist acts are seen as more serious than natural events). This is interesting since according to utility theory only the consequences, i.e. not the cause, should affect decisions. Something that makes the interpretation of the results, related to the importance of the disaster cause, somewhat more problematic however is the fact that it could not be definitely concluded whether it is the cause *per se* that affects people's judgements. There were some indications that some people speculated about secondary consequences of scenarios. Some for example argued that the occurrence of a terrorist act could indicate that the likelihood of future acts increases, which made them judge terrorist scenarios as being more serious.

Summary of research contributions

Two different preference elicitation methods were used to study how the perceived seriousness of disasters is affected by four different disaster characteristics. Although attributes related to physical harm were seen as most important, there are some indications that the cause of the disaster may also affect people's preferences. The results can be useful for discussions of the value bases of risk and vulnerability analysis, especially in situations where elicitations are not performed with the relevant stakeholders for the specific situation.

5.3 Contributions related to design research

This thesis has two main research perspectives, one normative and one descriptive, where the emphasis has been on the normative one. The literature on the philosophy of science and the scientific method mostly addresses the descriptive perspective. Principles of normative research are dealt with to a lesser extent, and since this thesis is primarily normative a great deal of effort has been devoted towards developing and specifying a normative design research process (see section 4.1). The approach draws on theories and ideas from the field of *design research*. Although the formulation of the design research process did not constitute a main research question, it is argued that the field of risk and vulnerability analysis can benefit from its ideas – therefore, it is seen as a contribution of this thesis.

The field of risk and vulnerability analysis is highly normative, and method development is a core activity. However, it seems to be rather rare that method development is approached in a systematic and transparent way where the purpose

of the method is clearly expressed; design criteria are specified and justified; and finally how the method satisfies the criteria is explicated. Presenting such a logical line of reasoning is argued to have a great value. First, it is claimed that it is more likely that the suggested method actually fulfils its intended purpose. Secondly, it facilitates critical evaluation of the foundation and reasonableness of the suggested method. Thirdly, it makes it easier for potential users to determine to what extent they agree with the normative assumptions made and whether the method suits their purposes. All told, it is argued that the ideas presented in the present thesis constitute one step towards what could be termed a *scientific development of methods*.

6 Discussion and future work

This thesis has suggested three methods and framework RVA, performed one empirical study and evaluation of RVA practises and carried out one study of people's preferences regarding disaster characteristics. The present chapter will discuss these research activities, especially focusing on their implications, and some ideas for future research will be given.

Research question 1 (papers I-III) has focussed on the development of methods for vulnerability analysis of single and interdependent technical infrastructure networks. Within this research activity one main difficulty has been to manage the complexity of the systems of interest. To this end, network analysis was chosen as the general approach for modelling the systems due to its ability to describe and analyse complex large-scale systems (Amaral and Ottino, 2004). Rather early in the research process, however, it was recognised that strict application of network theory has limitations in this area because it neglects the functional characteristics of systems. However, an approach to vulnerability analysis of technical infrastructures must account for functional characteristics. Of course, the downside is that simulations become more computationally burdensome – a great issue since one purpose of the methods is to enable comprehensive analysis with respect to large-scale perturbation. A central concern for analyses in practise is, therefore, to decide on which functional characteristics to include in the model and the level of detail of the models. The importance of this issue has also been stressed in the suggested methods when separating the system model into a structural and a functional part.

When it comes to analysing complex large-scale systems, such as technical infrastructure systems, it is practically impossible to be exhaustive and all-encompassing in terms of capturing *all* possible risk scenarios. However, how the analyses are carried out definitely affects the degree of completeness. On this issue, Haimes argues that one way of addressing complex systems is to develop and make use of *several models* of the same system, where each model is developed from a certain perspective to capture some specific aspects of the system (Haimes, 1998; Haimes et al., 2002). A complement to that approach in the context of vulnerability analysis, which has been employed in the present thesis, is to adopt *several perspectives on vulnerability* within the frame of a single system model. More specifically, in papers I-III three perspectives have been used (global vulnerability, critical components and critical geographical locations), and it is argued that each perspective provides a partial view of the system's vulnerability, but that taken together they provide a more complete depiction of vulnerability. Additional

perspectives on vulnerability are also possible using the same simulation approach. One possible extension is to model "real" hazard exposures and investigate how the infrastructures can withstand these. One example could be to use data on hurricane exposures and the susceptibility of different components to hurricane exposure. In performing this extension, it is likely to be favourable to implement the simulation approach in a GIS framework.

The goal of the methods developed in this thesis has been primarily to enable a broad and explorative analysis without too many preconceived notions about the systems' vulnerability, rather than focusing in-depth on some specific scenarios. Based on the insights from broad and explorative analyses, more detailed and advanced analyses and simulations can then be performed, perhaps by using other modelling approaches. These ideas are consistent with the framework for vulnerability analysis of critical infrastructure systems proposed by Eusgeld et al. (2009). It also harmonises with the "philosophy of multi-methodology", which states that it is advantageous and often necessary to use several methods and perspectives to understand the richness and complexity of reality (Mingers and Brocklesby, 1997; Murray et al., 2008).

A few words should also be said about the limitations of the proposed methods and modelling approaches. The most apparent limitation is that social and organizational factors have not been explicitly taken into account in the models. People and organisations play important roles in both the operation and restoration of infrastructures. One example is the use of restoration times in Paper III. This clearly depends on how the organization responds, including the resources it has. In Paper III restoration times were addressed through rather rough assumptions. However, research has been initiated aiming at more explicitly taking an organization's restoration activities into account (Wilhelmsson and Johansson, 2009).

Several actors in society could benefit from performing vulnerability analyses using the proposed methods, including private utility owners and public actors who have responsibilities for technical infrastructure networks. In Sweden, actors with "critical societal functions" must maintain a "basic level of security" (see section 1.4.1) during extraordinary events – the methods proposed in the present thesis could be used by several of these actors in their work to ensure such a basic level of security. Furthermore, since the focus in the proposed methods is to gain insights into how large-scale perturbations affect the infrastructure systems, it is argued that the methods complement more traditional reliability- and maintenance-oriented methods.

One practical difficulty for vulnerability analyses of interdependent infrastructure systems is that the responsibility and operation of infrastructures is fragmented across many actors and institutions in society (Amin, 2000; de Bruijne and van Eeten, 2007; Kröger, 2008). Analysing these interconnected systems must therefore essentially constitute joint efforts by several actors, or there must at least be a broad agreement among the infrastructure owners. This is not likely to be straightforward. In the Swedish context, authorities included in the "cooperative area"[55] termed "technical infrastructures"[56] should take a leading role in facilitating such multi-actor and large-scale analyses. In addition, authorities with geographic area responsibility (municipalities and county administration boards) should also play a role, since they have a responsibility of coordinating the actors within their respective geographic area. Both the increased interdependencies between technical infrastructures and the increased societal dependencies of infrastructure services suggest that this ought to be a prioritized activity in the future.

Research question 2 (paper IV) focussed on the development of a framework for analysis and evaluation of the response to past emergencies. The main aim of using the framework is to develop an explicit model of the emergency response in a dialogue with the involved actors. The model should then be used to facilitate the understanding of the response activities, and as a basis for discussions of how to improve the response capability of the emergency response system as a whole. To avoid drawing only narrow conclusions regarding the response to the particular event, counterfactual scenarios should be analysed to enable the evaluation of the emergency response system with respect to other potential scenarios as well.

The suggested framework is suitable for joint analyses between several formal organizations, especially organizations that are highly dependent on each other during emergencies. It is argued that such joint analyses can for example increase the mutual understanding among the organizations about each other's roles, responsibilities, resources, and perhaps most importantly an understanding of how they are interdependent, which is something that is likely to improve the response to future emergencies.

[55] In the Swedish emergency management system a number of cooperative areas have been defined. In a cooperative area, a number of central authorities are included that have especially strong relations (e.g. in terms of interdependencies). See http://www.msb.se/Upload/Forebyggande/Krisberedskap/Fact_Coop_areas.pdf?epslanguage=sv (2010-02-15) for information on the cooperative areas.

[56] In the cooperative area called technical infrastructure the following authorities are included: The National Electrical Safety Board, Swedish Energy Agency, National Food Administration, Swedish Civil Contingencies Agency, The Swedish Post and Telecom Agency, and Svenska Kraftnät.

One important challenge related to the framework for analysing emergency response systems is to manage the complexity of these systems. This may lead to the models generated in the framework becoming rather comprehensive – especially when analysing large-scale emergencies – and thereby difficult to grasp. The present thesis has not dealt with how this should be addressed. However, inspiration could be gained from a national study performed by MSB concerned with mapping dependencies between societal actors and sectors (MSB, 2009), where a classification scheme was developed. This scheme aims at facilitating the interpretation of the dependency structures of different actors and sectors. This or similar schemes could prove to be very useful when interpreting the model generated by the framework. In addition, methods and tools from network analysis, e.g. Wasserman and Faust (1999), can prove useful.

Research question 3 (Paper V) focussed on studying and evaluating a number of Swedish municipal RVAs. The study showed that there are possibilities for improving RVA practises, which is expected since these activities are rather new in many municipalities. In the paper a number of changes are suggested that improve the fulfilment of some purpose. The downside is that many of the suggested changes also require more resources (time and manpower) to conduct the analysis, which means that trade-off judgements have to be made. Municipalities, both the ones included in the study and other municipalities in Sweden, can use these suggestions as an input when considering how their future RVA processes should be designed.

The evaluation was performed using the main ideas from the design research approach suggested for method development (see section 4.1). This approach provided a good structure for evaluating RVAs and it is contended that the approach could prove useful in other contexts as well. A key principle of the approach is the importance of explicitly specifying and justifying desirable characteristics and functions for the RVAs which must be derived from some purpose for the analyses. Different purposes lead to different desirable characteristics.

In the evaluation of Swedish municipal RVAs, two different purposes were considered (expressed in the legislation): using the RVA as a basis for risk-related decisions, and that the RVA processes in themselves should contribute to reduced risk and vulnerability. These two purposes may be relevant for a large array of different contexts. The research literature related to risk analysis often emphasises the first purpose (basis for decisions). However, it is argued that the "process benefits" of performing RVA could be highly relevant for many actors performing

various types of RVAs. For example, one of the key purposes in using the framework for post-event RVAs is that the processes should contribute to reduced risk and vulnerability by increasing the participants' knowledge of roles, responsibilities and capabilities and their readiness to act when emergencies occur, and creating relationships of trust.

The evaluation of municipal RVAs, however, also showed that there may be tensions between the purposes, in the sense that some way of performing RVAs leads to better fulfilment of one of the purposes and worse fulfilment of the other. When designing RVA processes, actors therefore have to carefully consider how an RVA process affects the fulfilment of both these purposes and make trade-offs between the two.

The empirical study of preferences (Research question 4/Paper VI) was performed using students as respondents and with respect to four disaster attributes, commonly used to describe disasters that have occurred. Since no method is free of bias, the study used two methods of rather different kinds to gain insights into the uncertainty of the importance of the attributes.

It should be noted that the study has limitations regarding both the participants and the attributes studied. In an actual analysis it is of course preferable to perform value elicitation with the affected parties. However, most analyses carried out today are likely not to perform explicit value elicitations. In those cases, preference elicitations such as the one performed here can be an important input to the choice of value basis for the analysis, of course keeping the limitations of the study in mind.

One interesting finding in the study was that the cause of the disaster seemed to affect many of the respondents' judgement of disaster seriousness. This may have some implications for the practises of both decision and risk analysis. In decision analysis, expected utility theory is the prevailing paradigm, which is a teleological paradigm. This means that decisions should only be based on the consequences of different alternatives. However, if the causes affect how people value different alternatives, decisions are affected by deontological concerns, hence calling for revisions for prescriptive decision making. Furthermore, the common practise in risk analysis is to only consider the negative consequences in the end states of risk scenarios; that is, how the system got to this end state is not relevant when it comes to determining the severity of the scenario. But if the apparent cause of the risk scenarios actually affects how serious the risk scenario is perceived to be by people, risk analysis practises need to somehow account for the cause when determining how serious scenarios are.

A more general reflection is that the value dimension of risk, i.e. what one considers to be worth protecting, in fact must be addressed *before* the dimension that relates to knowledge about the future. The reason is that values simply determine what aspects of the world deserve attention in the analysis (McDaniels, 2000). Unfortunately, this does not seem to be addressed to the same extent in either the research literature or in practise, as the dimension of risk analysis that relates to knowledge about the future. In many technical risk analyses only physical harm, such as fatalities, is considered (Renn, 1998) and there is often no explicit phase where the value basis is discussed and established (Hatfield and Hipel, 2002). But by leaving it implicit and unconsidered, there are no guarantees that the values basis for the risk analysis constitutes a good representation of the relevant stakeholders' values or even that participants in the analyses are actually talking the same language (Nilsson and Becker, 2009).

Being explicit about values is relevant for all types of risk and vulnerability analysis. The present thesis emphasises this both in the suggested methods for vulnerability analysis of technical infrastructures and in the framework for post-event RVA of response systems. In the context of interdependent infrastructure, it would be interesting to perform value elicitations regarding the importance of various infrastructure services, similar to what is done in Apostolakis and Lemon (2005). Such information could be then be used as a basis for strategic decisions regarding what amount of resources should be invested in protecting various types of infrastructure services.

Something that needs to be reflected on in connection with design research and the method development process is the role of subjective judgements. Subjective judgements are required throughout the method development process – from stating the purpose to judging whether the method fulfils the stated criteria. The point of a scientific approach to method development is not to downplay or objectify them, but to explicate them and make the whole reasoning transparent and open for scrutiny – it is primarily this that makes the whole method development process rigorous and scientific. At the same time it is important to realise that the method developer him-/herself may be biased. Of course, the same holds for e.g. descriptive science where it is more likely that a scientist who has suggested a hypothesis interprets observations in favour of his/her hypothesis (van Aken, 2004). Therefore, external evaluation is important in the area of risk and vulnerability analysis methods. However, rigorous and systematic evaluations of proposed methods seem to be rather rare in the field, yet evaluation is as important in normative research as verification and validation of hypotheses and theories are in descriptive research.

6.1 Future research

The suggestions for future research will be specified for each main research activity addressed in the present thesis.

Methods for vulnerability analysis of technical infrastructure networks

There are many challenges related to modelling and analysing technical infrastructure systems, much due to the vast complexities of these systems. The research presented in this thesis constitutes a first step towards dealing with some of these challenges; however, more research is needed. The following areas are claimed to be some of the most important ones:

- More applications of the suggested methods should be made with respect to different types of systems. The method for analysing single infrastructures has so far been applied only to electrical distribution systems, and although the method has been developed to be generally applicable to infrastructure networks, future applications should investigate in-depth whether this is the case or whether the method must be adapted. Based on the new applications, modifications of the method could be proposed (in line with the design research process adopted in the thesis).
- Future research should further address how to model infrastructure systems in order to capture the most important functional features of the systems while still being able to perform comprehensive vulnerability analyses.
- The present thesis has focussed on developing methods for vulnerability analysis, where it is assumed that some perturbation exposes the system. However, in order to evaluate whether potential mitigation measures are cost-effective, the likelihood of perturbations cannot be neglected. Vulnerability analyses must be complemented with "exposure analyses", essentially expanding the analysis into a risk analysis. Future research should address how this should be done and how vulnerability analysis can be used to support decision-making.

Framework for post-event RVA of emergency response

Several possibilities of future research also exist in relation to the suggested framework for post-event RVA:

- More applications of the suggested framework, with respect to different types of emergencies and in different settings, should be carried out with the main purpose of further developing the framework.

- Tools for facilitating analysis and understanding of the generated model of the emergency response system should be developed.
- In practise, there is an upper limit to the number of counterfactual scenarios that can be analysed. Future research should address how to construct these counterfactual scenarios, for example how to choose which variables to "tweak on".
- The suggested framework has been developed to be applicable for analysis of past events. However, the ideas can also be used as a basis for forward-looking analysis. Future research should address this in further detail.

Evaluation of municipal RVAs

A number of possibilities for future research exist in this context:

- The performed study can be described as a rather overall evaluation. In order to gain deeper insights, more in-depth evaluations are needed, for instance by pinpointing specific aspects of the analyses.
- The municipalities selected in the study are not necessarily representative of Swedish municipalities as a whole. Additional evaluations are therefore needed if one wants to gain a complete picture of how RVAs are carried out in Swedish municipalities.
- A number of potential ways of improving the municipal RVAs was proposed in the performed evaluation. It would be interesting to initiate cooperation with some municipality and perform action research (Greenwood and Levin, 2007) both to improve the practices of the municipality and to gain knowledge relevant for RVA theory and method development.
- Future research is needed to gain knowledge of what characteristics the RVAs should have in order to fulfil the purpose related to process benefits. Today not much is known about this (Pelling, 2007); instead this is mostly built on assumptions rather than research.

People's preferences for disaster characteristics

- Preference elicitations should be performed with broader groups of participants and with other attributes in order to study the generalisability of the results.
- More in-depth studies on the effect of disasters on judgements about disaster seriousness should be performed. The aim should be to gain insights about the reasons for the fact that some specific causes seem to be worse than other causes.

7 Conclusions

The overall aim of this thesis has been to improve the analysis of risk and vulnerability in society's proactive emergency management. This has been pursued in two different ways: first, by developing methods and frameworks useful for analysis in this context; and secondly, by understanding practises related to RVA and suggesting how they can be improved. The aims of this thesis are highly normative in that they strive to develop or construct artefacts (in this case risk and vulnerability analyses) in order to fulfil or improve the fulfilment of some purpose. Research activities of this sort can be termed *design research activities* and differ from more traditional natural science activities.

In order to fulfil the aims and answer the research questions posed in this thesis, a design research approach has been developed and applied. The approach stresses the importance of being explicit and transparent regarding the purpose/purposes of the method, the concrete design criteria derived from the purpose/purposes, which also must be justified, and the way the proposed method fulfils the design criteria. In addition, it stresses the fact that method development is an iterative process where insights from method deployment can lead to a need to modify the method, the design criteria for the method or even the desired purpose of the method. It is concluded that the suggested approach provides a good structure for method development. Below, the conclusions related to each of the two aims are briefly described.

Developing methods and frameworks that can be useful in analysing risks and vulnerabilities in society's proactive emergency management:

- A method for analysing single technical infrastructure networks was designed using the proposed design research approach to method development. The method constitutes a simulation-based approach where a model of the system of interest is represented in a structural and functional model. These models are then analysed from both a global vulnerability and a critical components perspective, which enables more in-depth conclusions to be drawn.
- A method for analysing multiple interdependent infrastructures was designed employing the proposed design research approach to method development. The method was an extension of the method developed for single infrastructure systems. In the method both functional and geographical dependencies are taken into account, and a third perspective of vulnerability, analysis of critical geographical locations, is added, which

is a perspective especially important to capture when considering multiple infrastructures.

- One framework for performing post-event risk and vulnerability analyses of emergency response systems was designed using the proposed design research approach to method development. The main point of the framework is to generate an explicit model of the emergency response system that was active during an actual emergency (including actors, tasks, resources, infrastructures and dependencies among these). The model is generated primarily in a dialogue between involved actors, and should then be used to facilitate the understanding of the emergency response as well as to analyse counterfactual scenarios to enable broader conclusions to be drawn.

Understanding practises related to Risk and Vulnerability Analysis and suggesting how they can be improved:

- A design research approach to evaluate risk and vulnerability analyses was outlined, influenced by the approach to method development referred to above, and then applied to evaluate a number of Swedish municipal RVAs. Both document studies and interviews were used as a basis for drawing conclusions regarding whether the studied analysis fulfil the purposes stipulated in Swedish legislation. Based on the evaluations, a number of suggestions for improving the RVAs were suggested. It is concluded that the suggestions can be used as a roadmap or as a basis for discussions when municipalities, as well as other actors, strive to improve their RVA practises.
- An empirical study of people's preferences regarding how a number of disaster characteristics affect their judgements of a disaster's seriousness was carried out. It is concluded that the results of the study can be used by various actors in their performance of RVAs as one input regarding the value basis on which the RVAs should be grounded.

8 References

Abrahamsson, M., Jönsson, H. and Johansson, H. (2008), "Analyzing emergency response using a systems perspective", *Proceedings of PSAM9*, Hong Kong, China.

Abrahamsson, M. and Tehler, H. (2009), "The role of risk and vulnerability analyses in emergency management systems - evaluating regional RVAs in the Swedish emergency management system", *Submitted to a scientific journal*.

Albert, R., Albert, I. and Nakarado, G. L. (2004), "Structural vulnerability of the North American power grid", *Physical Review E*, **69**(025103): 1-4.

Albert, R. and Barabási, A.-L. (2002), "Statistical Mechanics of Complex Networks", *Review of Modern Physics*, **74**(1): 47-97.

Albert, R., Jeong, H. and Barabási, A.-L. (2000), "Error and attack tolerance of complex networks", *Nature*, **406**(6794): 378-382.

Alexander, D. (2005), "Towards the development of a standard in emergency planning", *Disaster Prevention and Management*, **14**(2): 158-175.

Amaral, L. A. N. and Ottino, J. M. (2004), "Complex networks - Augmenting the framework for the study of complex systems", *The European Physical Journal B*, **38**: 147-162.

Amendola, A. (2001), "Recent paradigms for risk informed decision making", *Safety Science*, **40**: 17-30.

Amin, M. (2000), "National Infrastructures as Complex Interactive Networks", In: *Automation, Control, and Complexity: An Integrated Approach*, Samad, T. and Wayrauch, J. (Eds.), New York: John Wiley and Sons.

Amin, M. and Stringer, J. (2008), "The Electric Power Grid: Today and Tomorrow", *MRS Bulletin*, **33**: 399-409.

Apostolakis, G. E. (1990), "The Concept of Probability in Safety Assessments of Technological Systems", *Science*, **250**(4986): 1359-1364.

Apostolakis, G. E. (2004), "How Useful is Quantitative Risk Assessment", *Risk Analysis*, **24**(3): 515-520.

Apostolakis, G. E. and Lemon, D. M. (2005), "A Screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities Due to Terrorism", *Risk Analysis*, **25**(2): 361-376.

Aven, T. (2003), *Foundations of Risk Analysis: A Knowledge and Decision-Oriented Perspective*, Chichester: John Wiley & Sons.

Aven, T. (2004a), "On How to Approach Risk and Uncertainty to Support Decision-Making", *Risk Management*, **6**(4): 27-39.

Aven, T. (2004b), "Risk Analysis and Science", *International Journal of Reliability, Quality and Safety Engineering*, **11**(1): 1-15.

Aven, T. (2007), "A unified framework for risk and vulnerability analysis covering both safety and security", *Reliability Engineering & System Safety*, **92**: 745-754.
Aven, T. (2008), "A semi-quantitative approach to risk analysis, as an alternative to QRAs", *Reliability Engineering & System Safety*, **93**: 768-775.
Aven, T. (2009), "Identification of safety and security critical systems and activities", *Reliability Engineering & System Safety*, **94**: 404-411.
Aven, T. and Korte, J. (2003), "On the use of risk and decision analysis to support decision-making", *Reliability Engineering & System Safety*, **79**: 289-299.
Aven, T. and Kristensen, V. (2005), "Perspectives on risk: review and discussion of the basis for establishing a unified and holistic approach", *Reliability Engineering & System Safety*, **90**: 1-14.
Aven, T. and Renn, O. (2009a), "On risk defined as an event where the outcome is uncertain", *Journal of Risk Research*, **12**(1): 1-11.
Aven, T. and Renn, O. (2009b), "The Role of Quantitative Risk Assessments for Characterizing Risk and Uncertainty and Delineating Appropriate Risk Management Options, with Special Emphasis on Terrorism Risk", *Risk Analysis*, **29**(4): 587-600.
Ben-Haim, Y. (2004), "Uncertainty, probability and information-gaps", *Reliability Engineering & System Safety*, **85**: 249-266.
Bier, V. M. (2007), "Choosing What to Protect", *Risk Analysis*, **27**(3): 607-620.
Boin, A. and Lagadec, P. (2000), "Preparing for the Future: Critical Challenges in Crisis Management", *Journal of Contingencies and Crisis Management*, **8**(4): 185-191.
Boin, A. and McConnell, A. (2007), "Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience", *Journal of Contingencies and Crisis Management*, **15**(1): 51-59.
Bradbury, J. (1989), "The Policy Implications of Differing Concepts of Risk", *Science, Technology, and Human Values*, **14**(4): 380-399.
Brehmer, B. (2008), "Vad är ledningsvetenskap?" *Kungliga Krigsvetenskapsakademiens Handlingar och Tidskrift*, **1**: 43-72. (In Swedish).
Brooks, N. (2003), *Vulnerability, risk and adaptation: A conceptual framework*, Tyndall Centre for Climate Change Research, Norwich.
Brown , T., Beyler, W. and Barton, D. (2004), "Assessing infrastructure interdependencies: the challenge of risk analysis for complex adaptive systems", *International Journal of Critical Infrastructures*, **1**(1): 108-117.
Bunge, M. (2003), "Philosophical Inputs and Outputs of Technology", In: *Philosophy of technology: the technological condition*, Scharff, R. C. and Dusek, V. (Eds.), Malden: Blackwell publishers.
Busby, J. S. and Hughes, E. J. (2006), "Credibility in risk assessment: a normative approach", *International Journal of Risk Assessment and Management*, **6**(4-6): 508-527.

Campbell, S. (2006), "Risk and the Subjectivity of Preference", *Journal of Risk Research*, **9**(3): 225-242.

Cardona, O. D. (2003), "The Need for Rethinking the Concepts of Vulnerability and Risk from a Holistic Perspective: A Necessary Review and Criticism for Effective Risk Management", In: *Mapping Vulnerability: Disasters, Development and People*, Bankoff, G., Frerks, G. and Hilhorst, D. (Eds.), London: Earthscan Publishers.

Chang, S. E., McDaniels, T. L., Mikawoz, J. and Peterson, K. (2007), "Infrastructure failure interdependencies in extreme events: power outage consequences in the 1998 Ice Storm", *Natural Hazards*, **41**: 337-358.

Checkland, P. (1993), *Systems Thinking, Systems Practice*, Chichester: John Wiley and Sons Ltd.

Cook, S. C. and Ferris, T. L. J. (2007), "Re-evaluating Systems Engineering as a Framework for Tackling Systems Issues", *Systems Research and Behavioral Science*, **24**: 169-181.

Cross, F. B. (1998), "Facts and values in risk assessment", *Reliability Engineering & System Safety*, **59**: 27-40.

Crucitti, P., Latora, V. and Marchiori, M. (2004a), "Error and attack tolerance of complex networks", *Physica A*, **340**(1-3): 388-394.

Crucitti, P., Latora, V. and Marchiori, M. (2004b), "A model for cascading failures in complex networks", *Physical Review E* **69**(045104).

Crucitti, P., Latora, V. and Marchiori, M. (2004c), "A topological analysis of the Italian power grid", *Physica A*, **338**(1-2): 92-97.

Crucitti, P., Latora, V. and Marchiori, M. (2005), "Locating Critical Lines in High-Voltage Electrical Power Grids", *Fluctuation and Noise Letters*, **5**(2): 201-208.

Cutter, S. L., Boruff, B. J. and Shirley, W. L. (2003), "Social Vulnerability to Environmental Hazards", *Social Science Quarterly*, **84**(2): 242-261.

Davidson, R. A. (1997), "A Multidisciplinary Urban Earthquake Disaster Risk Index", *Earthquake Spectra*, **13**(2): 211-223.

de Bruijne, M. and van Eeten, M. (2007), "Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment", *Journal of Contingencies and Crisis Management*, **15**(1): 18-29.

Dekker, S. W. A. (2002), "Reconstructing human contributions to accidents: the new view on error and performance", *Journal of Safety Research*, **33**: 371-385.

Deverell, E. (2003), *The 2001 Kista blackout: corporate crisis and urban contingency*, Stockholm: Försvarshögskolan.

Dilley, M. and Boudreau, T. E. (2001), "Coming to terms with vulnerability: a critique of the food security definition", *Food Policy*, **26**: 229-247.

Dunn, K. (2005), "Interviewing", In: *Qualitative Research Methods in Human Geography*, Hay, I. (Eds.), Melbourne: Oxford University Press.

Einarsson, S. and Rausand, M. (1998), "An Approach to Vulnerability Analysis of Complex Industrial Systems", *Risk Analysis*, **18**(5): 535-546.

Energimyndigheten (2005), *Stormen Gudrun – Konsekvenser för nätbolag och samhälle*, Swedish Energy Agency, Stockholm. (In Swedish).

Ennis, R. H. (1964), "Operational Definitions", *American Educational Research Journal*, **1**(3): 183-201.

Esaiasson, P., Gilljam, M., Oscarsson, H. and Wängnerud, L. (2002), *Metodpraktikan: Konsten att studera samhälle, individ och marknad*, Stockholm: Nordstedts Juridik. (In Swedish).

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

Failing, L., Gregory, R. and Harstone, M. (2007), "Integrating science and local knowledge in environmental risk management: a decision-focused approach", *Ecological Economics*, **64**: 47-60.

Farazmand, A. (2007), "Learning from the Katrina Crisis: A Global and International Perspective with Implications for Future Crisis Management", *Public Administration Review*, **67**(1): 149-159.

Fischhoff, B. (1975), "Hindsight ≠ Foresight: The Effect of Outcome Knowledge on Judgement Under Uncertainty", *Journal of Experimental Psychology: Human Perception and Performance*, **1**(3): 288-299.

Fischhoff, B., Watson, S. R. and Hope, C. (1984), "Defining Risk", *Policy Sciences*, **17**: 123-139.

Ford, C. K., Keeney, R. L. and Kirkwood, C. W. (1979), "Evaluating Methodologies: A Procedure and Application to Nuclear Power Plant Siting Methodologies", *Management Science*, **25**(1): 1-10.

Gorman, S. P., Schintler, L., Kulkarni, R. and Stough, R. (2004), "The Revenge of Distance: Vulnerability Analysis of Critical Information Infrastructure", *Journal of Contingencies and Crisis Management*, **12**(2): 48-63.

Governmental Bill (2005/06:133), *Samverkan vid kris - för ett säkrare samhälle*. (In Swedish.)

Greenwood, D. J. and Levin, M. (2007), *Introduction to Action Research: Social Research for Social Change*, Thousand Oaks: Sage Publications.

Gregory, R., Failing, L., Ohlson, D. and McDaniels, T. L. (2006), "Some Pitfalls of an Overemphasis on Science in Environmental Risk Management Decisions", *Journal of Risk Research*, **9**(7): 717-735.

Haimes, Y. Y. (1998), *Risk Modeling, Assessment, and Management*, New York: John Wiley & Sons.

Haimes, Y. Y. (2006), "On the Definition of Vulnerabilities in Measuring Risks to Infrastructures", *Risk Analysis*, **26**(2): 293-296.

Haimes, Y. Y. and Jiang, P. (2001), "Leontief-Based Model of Risk in Complex Interconnected Infrastructures", *Journal of Infrastructure Systems*, **7**(1): 1-12.
Haimes, Y. Y., Kaplan, S. and Lambert, J. H. (2002), "Risk filtering, ranking, and management framework using hierarchical holographic modeling", *Risk Analysis*, **22**(2): 383-397.
Haimes, Y. Y. and Longstaff, T. (2002), "The role of risk analysis in the protection of critical infrastructures against terrorism", *Risk Analysis*, **22**(3): 439-444.
Hallin, P.-O., Nilsson, J. and Olofsson, N. (2004), *Kommunal sårbarhetsanalys*, Stockholm: Krisberedskapsmyndigheten. (In Swedish).
Hamrin, I. and Strömgren, M. (2008), "Regional risk- och krishantering - en studie av samtliga länsstyrelsers risk- och sårbarhetsanalyser", Master's thesis, Department of Fire Safety Engineering and Systems Safety, Lund University, Lund. (In Swedish).
Hansson, S. O. (2003), *Konsten att vara vetenskaplig*, Filosofienheten, Royal Institute of Technology, Stockholm. (In Swedish).
Hansson, S. O. (2005), "The Epistemology of Technological Risk", *Techné: Research in Philosophy and Technology*, **9**(2): 68-80.
Hatfield, A. J. and Hipel, K. W. (2002), "Risk and Systems Theory", *Risk Analysis*, **22**(6): 1043-1057.
Heath, R. (1998), "Looking for answers: suggestions for improving how we evaluate crisis management", *Safety Science*, **30**: 151-163.
Henrion, M. and Granger Morgan, M. (1990), *Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis*, Cambridge: Cambridge University Press.
Hevner, A. R., March, S. T., Park, J. and Ram, S. (2004), "Design Science in Information Systems Research", *MIS Quarterly*, **28**(1): 75-105.
Holland, J. H. (1995), *Hidden Order: How Adaptation Builds Complexity*, New York: Basic Books.
Hollnagel, E. (2004), *Barriers and accident prevention*, Aldershot: Ashgate Publishing.
Holme, P. and Kim, B. J. (2002), "Vertex overload breakdown in evolving networks", *Physical Review E*, **65**(066109): 1-8.
Holme, P., Kim, B. J., Yoon, C. H. and Han, S. K. (2002), "Attack vulnerability of complex networks", *Physical Review E*, **65**(056109): 1-14.
Holmgren, Å. (2006), "Using Graph Models to Analyze the Vulnerability of Electric Power Networks", *Risk Analysis*, **26**(4): 955-969.
Hughes, G. (2006), "The London bombings of 7 July 2005: what is the main lesson?" *Emergency Medicine Journal*, **26**: 666.
IFRC (1999), *Vulnerability and capacity assessment: An International Federation Guide*, International Federation of Red Cross and Red Crescent Societies, Geneva.

IRGC (2006), *White paper on Managing and Reducing Social Vulnerabilities from Coupled Critical Infrastructures*, International Risk Governance Council, Geneva.

Jasanoff, S. (1993), "Bridging the Two Cultures of Risk Analysis", *Risk Analysis*, **13**(2): 123-129.

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

Jenelius, E., Petersen, T. and Mattson, L.-G. (2006), "Importance and exposure in road network vulnerability analysis", *Transportation Research Part A*, **40**: 537-560.

Johansson, H. and Jönsson, H. (2007), *Metoder för risk- och sårbarhetsanalys ur ett systemperspektiv*, Lunds universitets centrum för riskanalys och riskhantering, Lund. (In Swedish).

Johansson, J. and Jönsson, H. (2008), "A Model for Vulnerability Analysis of Interdependent Infrastructure Networks", *Proceedings of ESREL 2008 and 17th SRA-Europe Conference*, Valencia, Spain.

Johansson, J., Jönsson, H. and Johansson, H. (2006a), "Analysing Societal Vulnerability to Perturbations in Electric Distribution Systems", *Proceedings of CNIP 2006*, Rome, Italy.

Johansson, J., Lindahl, S., Samuelsson, O. and Ottosson, H. (2006b), "The Storm Gudrun: a Seven-Weeks Power Outage in Sweden", *Proceedings of CRIS 2006*, Alexandria, USA.

Jönsson, H. (2007), "Risk and Vulnerability Analysis of Complex Systems: a basis for proactive emergency management", Licentiate thesis, Department of Fire Safety Engineering and Systems Safety, Lund University, Lund.

Jönsson, H., Abrahamsson, M. and Johansson, H. (2007a), "An Operational Definition of Emergency Response Capabilities", *Proceedings of 14th TIEMS Annual Conference*, Trogir, Croatia.

Jönsson, H., Johansson, J. and Johansson, H. (2007b), "Identifying Critical Components in Electric Power Systems: A Network Analytic Approach", *Proceedings of Risk, Reliability and Societal Safety, ESREL 2007*, Stavanger, Norway.

Kaplan, S. (1997), "The Words of Risk Analysis", *Risk Analysis*, **17**(4): 407-417.

Kaplan, S. and Garrick, B. J. (1981), "On The Quantitative Definition of Risk", *Risk Analysis*, **1**(1): 11-27.

Kaplan, S., Haimes, Y. Y. and Garrick, B. J. (2001), "Fitting hierarchical holographic modeling into the theory of scenario structuring and a resulting refinement to the quantitative definition of risk", *Risk Analysis*, **21**(5): 807-819.

Kaplan, S., Visnepolchi, S., Zlotin, B. and Zusman, A. (1999), *New Tools for Failure and Risk Analysis - Anticipatory Failure Determination (AFD) and the Theory of Scenario Structuring*, Southfield: Ideation International Inc.

KBM (2006a), *Risk- och sårbarhetsanalyser - vägledning för statliga myndigheter*, Swedish Emergency Management Agency, Stockholm. (In Swedish).

KBM (2006b), *Risk- och Sårbarhetsanalyser: Vägledning för kommuner och landsting*, Swedish Emergency Management Agency, Stockholm. (In Swedish).

Keeney, R. L. (1992), *Value-Focused Thinking, a Path to Creative Decisionmaking*, Cambridge: Harvard University Press.

Keeney, R. L. (1994), "Using Values in Operations Research", *Operations Research*, **42**(5): 793-813.

Kendra, J. M. and Wachtendorf, T. (2003), "Elements of Resilience After the World Trade Centre Disaster: Reconstituting New York City's Emergency Operations Centre", *Disasters*, **27**(1): 37-53.

Khan, F. I., Sadiq, R. and Amyotte, P. R. (2003), "Evaluation of Available Indices for Inherently Safer Design Options", *Process Safety Progress*, **22**(2): 83-97.

Kinney, R., Crucitti, P., Albert, R. and Latora, V. (2005), "Modeling cascading failure in the North American power grid", *The European Physical Journal B*, **46**(1): 101-107.

Klinke, A. and Renn, O. (2002), "A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies", *Risk Analysis*, **22**(6): 1071-1094.

Koonce, A. M., Apostolakis, G. E. and Cook, B. K. (2008), "Bulk power grid risk analysis: Ranking infrastructure elements according to their risk significance", *Electrical Power and Energy Systems*, **30**: 169-183.

Kroes, P. (2002), "Design methodology and the nature of technical artefacts", *Design Studies*, **23**: 287-302.

Kröger, W. (2006), "Critical infrastructures at risk: securing electric power supply", *International Journal of Critical Infrastructures*, **2**(2/3): 273-293.

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

Kuhn, T. S. (1962), *The Structure of Scientific Revolutions*, Chicago: University of Chicago Press.

Kvale, S. (1997), *Den kvalitativa forskningsintervjun*, Lund: Studentlitteratur. (In Swedish).

Lagadec, P. (2006), "Crisis management in the twenty-first century: "Unthinkable" events in "inconceivable" contexts", In: *Handbook of Disaster Research*, Rodriguez, H., Quarantelli, E. L. and Dynes, R. (Eds.), New York: Springer.

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

Leavitt, W. M. and Kiefer, J. J. (2006), "Infrastructure Interdependency and the Creation of a Normal Disaster: The Case of Hurricane Katrina and the City of New Orleans", *Public Works Management Policy*, **10**(4): 306-314.

Lee, E. E., Mitchell, J. E. and Wallace, W. A. (2007), "Restoration of Services in Interdependent Infrastructure Systems: a network flow approach", *IEEE Transactions on Systems, Man, and Cybernetics-Part C: Applications and reviews*, **37**(6): 1303-1317.

Leveson, N. (2002), *System Safety Engineering: Back To The Future*, Aeronautics and Astronautics, Massachusetts Institute of Technology, Cambridge.

Leveson, N. (2004), "A new accident model for engineering safer systems", *Safety Science*, **42**: 237-270.

Lewin, D. (1983), "Engineering Philosophy: The Third Culture?" *Leonardo*, **16**(2): 127-132.

Little, R. G. (2002), "Controlling Cascading Failure: Understanding the Vulnerabilities of Interconnected Infrastructures", *Journal of Urban Technology*, **9**(1): 109-123.

Little, R. G. (2004), "A socio-technical systems approach to understanding and enhancing the reliability of interdependent infrastructure systems", *International Journal of Emergency Management*, **2**(1-2): 98-110.

March, S. T. and Smith, G. F. (1995), "Design and natural science research on information technology", *Decision Support Systems*, **15**: 251-266.

McConnell, A. and Drennan, L. (2006), "Mission Impossible? Planning and Preparing for Crisis", *Journal of Contingencies and Crisis Management*, **14**(2): 59-70.

McDaniels, T. L. (2000), "Creating and using objectives for ecological risk assessment and management", *Environmental Science & Policy*, **3**: 299-304.

McEntire, D. A. (2005), "Why vulnerability matters - Exploring the merit of an inclusive disaster reduction concept", *Disaster Prevention and Management*, **14**(2): 206-222.

McLaughlin, J. A. and Jordan, G. B. (1999), "Logic models: a tool for telling your program's performance story", *Evaluation and Program Planning*, **22**(1): 65-72.

Michaud, D. and Apostolakis, G. E. (2006), "Methodology for Ranking the Elements of Water-Supply Networks", *Journal of Infrastructure Systems*, **12**(4): 230-242.

Mili, L., Qiu, W. and Phadke, A. G. (2004), "Risk assessment of catastrophic failures in electric power systems", *International Journal of Critical Infrastructures*, **1**(1): 38-63.

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

Mingers, J. and Brocklesby, J. (1997), "Multimethodology: Towards a Framework for Mixing Methodology", *Omega*, **25**(5): 489-509.

Morrow, B. H. (1999), "Identifying and Mapping Community Vulnerability", *Disasters*, **23**(1): 1-18.

Motter, A. E. and Lai, Y.-C. (2002), "Cascade-based attacks on complex networks", *Physical Review E*, **66**(065102): 1-4.

MSB (2009), *Faller en - faller då alla? En slutredovisning från KBM:s arbete med samhällskritiska beroenden*, Swedish Civil Contingencies Agency, Stockholm. (In Swedish).

Murray, A. T., Matisziw, T. C. and Grubesic, T. H. (2008), "A Methodological Overview of Network Vulnerability Analysis", *Growth and Change*, **39**(4): 573-592.

Newlove, L. M., Stern, E. K. and Svedin, L. (2000), *Auckland Unplugged*, Stockolm: Copy Print.

Newman, M. E. (2003), "The structure and function of complex networks", *SIAM Review*, **45**(2): 167-256.

Nilsson, J. and Becker, P. (2009), "What's important? Making what is valuable and worth protecting explicit when performing risk and vulnerability analyses", *International Journal of Risk Assessment and Management*, **13**(3/4): 345-363.

Nordin, I. (1988), *Teknologins rationalitet*, Stockholm: Timbro. (In Swedish).

Nordström, H. and Tonegran, D. (2008), "Kommunal krisberedskap i Skåne: Inventering av sju skånska kommuners dokumenterade krisberedskap", Master's thesis, Department of Fire Safety Engineering and Systems Safety, Lund University, Lund. (In Swedish).

Nykvist, S. and Ohlson, E. (2007), "Nätverksteori som verktyg vid risk- och sårbarhetsanalys av eldistributionsnät", Master's thesis, Department of Fire Safety Engineering, Lund University, Lund. (In Swedish).

Olsen, O. E., Kruke, B. I. and Hovden, J. (2007), "Societal Safety: Concepts Borders and Dilemmas", *Journal of Contingencies and Crisis Management*, **15**(2): 69-79.

Palm, J. (2009), "Emergency Management in the Swedish Electricity Grid from a Household Perspective", *Journal of Contingencies and Crisis Management*, **17**(1): 55-63.

Palm, J. and Ramsell, E. (2007), "Developing Local Emergency Management by Co-Ordination Between Municipalities in Policy Networks: Experiences from Sweden", *Journal of Contingencies and Crisis Management*, **15**(4): 173-182.

Paté-Cornell, M. E. (1996), "Uncertainties in risk analysis: Six levels of uncertainty treatment", *Reliability Engineering & System Safety*, **54**: 95-111.

Paté-Cornell, M. E. (2002), "Finding and Fixing Systems Weaknesses: Probabilistic Methods and Applications of Engineering Risk Analysis", *Risk Analysis*, **22**(2): 319-334.

Paté-Cornell, M. E. and Dillon, R. L. (2006), "The Respective Roles of Risk and Decision Analyses in Decision Support", *Decision Analysis*, **3**(4): 220-232.

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

Payne, J. W., Bettman, J. R. and Schkade, D. A. (1999), "Measuring Constructed Preferences: Towards a Building Code", *Journal of Risk and Uncertainty*, **19**(1-3): 243-270.

PCCIP (1997), *Critical Foundations: Protecting America's Infrastructures*, Washington D.C.: President's Commission on Critical Infrastructure Protection.

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

Pelling, M. (2007), "Learning from others: the scope and challenges for participatory disaster risk assessment", *Disasters*, **31**(4): 373-385.

Perrow, C. (1999), *Normal Accidents: Living with High-Risk Technology*, Princeton: Princeton University Press.

Perry, R. W. and Lindell, M. K. (2003), "Preparedness for Emergency Response: Guidelines for the Emergency Planning Process", *Disasters*, **27**(4): 336-350.

Pidgeon, N. (1998), "Risk assessment, risk values and the social science programme: why we do need risk perception research", *Reliability Engineering & System Safety*, **59**: 5-15.

Poser, H. (1998), "On Structural Differences Between Science and Engineering", *Techné: Research in Philosophy and Technology*, **4**(2): 81-93.

Quarantelli, Q. L. (1998), *Major Criteria For Judging Disaster Planning And Managing Their Applicability In Developing Countries*, Disaster Research Center, University of Delaware, Newark.

Quarantelli, Q. L., Lagadec, P. and Boin, A. (2007), "A Heuristic Approach to Future Disasters and Crises: New, Old, and In-Between Types", In: *Handbook of Disaster Research*, Rodriguez, H., Quarantelli, Q. L. and Dynes, R. (Eds.), New York: Springer.

Rasmussen, J. (1985), "The Role of Hierarchical Knowledge Representation in Decisionmaking and Systems Management", *IEEE Transactions on Systems, Man, and Cybernetics*, **15**(2): 234-243.

Rasmussen, J. (1997), "Risk Management in a Dynamic Society: A Modelling Problem", *Safety Science*, **27**(2/3): 183-213.
Rasmussen, J. and Svedung, I. (2000), *Proactive Risk Management in a Dynamic Society*, Karlstad: Swedish Rescue Services Agency.
Renn, O. (1998), "Three decades of risk research: accomplishments and new challenges", *Journal of Risk Research*, **1**(1): 49-71.
Renn, O. (2001), "The need for integration: risk policies require the input from experts, stakeholders and the public at large", *Reliability Engineering & System Safety*, **72**: 131-135.
Renn, O. (2008), *Risk Governance: Coping with Uncertainty in a Complex World*, London: Earthscan.
Rinaldi, S. M. (2004), "Modeling and Simulating Critical Infrastructures and Their Interdependencies", *Proceedings of the 37th Hawaii International Conference on Systems Sciences*, Hawaii.
Rinaldi, S. M., Peerenboom, J. P. and Kelley, T. K. (2001), "Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies", *IEEE Control Systems Magazine*, **21**(6): 11-25.
Salter, J. (1997), "Risk Management in a Disaster Management Context", *Journal of Contingencies and Crisis Management*, **5**(1): 60-65.
SFS (1997:857), *Ellag*, Swedish Code of Statutes, Stockholm. (In Swedish).
SFS (2006:544), *Lagen om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap*, Swedish Code of Statutes, Stockholm. (In Swedish).
SFS (2006:942), *Förordning om krisberedskap och höjd beredskap*, Swedish Code of Statutes, Stockholm. (In Swedish).
SFS (2008:1002), *Förordning med instruktion för Myndigheten för samhällsskydd och beredskap*, Swedish Code of Statutes, Stockholm. (In Swedish).
Shrader-Frechette, K. S. (1991a), "Reductionist Approaches to Risk", In: *Acceptable Evidence: Science and Values in Risk Management*, Mayo, D. G. and Hollander, R. D. (Eds.), Oxford: Oxford University Press.
Shrader-Frechette, K. S. (1991b), *Risk and Rationality: Philosophical Foundations for Populist Reforms*, Berkeley: University of California Press.
Simon, H. (1996), *The Sciences of the Artificial*, Cambridge: The MIT Press.
Slovic, P. (1999), "Trust, Emotion, Sex, Politics, and Science: Surveying the Risk-Assessment Battlefield", *Risk Analysis*, **19**(4): 689-701.
SNAO (2008), *Regeringen och krisen - regeringens krishantering och styrning av samhällets beredskap för allvarliga samhällskriser*, Swedish National Audit Office (Riksrevisionen), Stockholm. (In Swedish).
SOU (2005:104), *Sverige och tsunamin - granskning och förslag*, Swedish Government Official Reports, Stockholm. (In Swedish).

SRV (2003), *Handbok för Riskanalys*, Swedish Rescue Services Agency, Karlstad. (In Swedish).
Stern, P. C. and Fineberg, H., V. (1996), *Understanding risk: informing decisions in a democratic society*, Washington D.C.: National Academy Press.
Stirling, A. (1999), *On Science and Precaution In the Management of Technological Risk*, European Commission Joint Research Centre, Seville.
Strogatz, S. H. (2001), "Exploring complex networks", *Nature*, **410**: 268-276.
Uhr, C., Johansson, H. and Fredholm, L. (2008), "Analysing Emergency Response Systems", *Journal of Contingencies and Crisis Management* **16**(2): 80-90.
UN/ISDR and UN/OCHA (2008), *Disaster Preparedness for Effective Response: Guidance and Indicator Package for Implementing Priority Five of the Hyogo Framework*, United Nations, Geneva.
van Aken, J. E. (2004), "Management Research Based on the Paradigm of the Design Sciences: The Quest for Field-Tested and Grounded Technological Rules", *Journal of Management Studies*, **41**(2): 219-246.
Wasserman, S. and Faust, K. (1999), *Social Network Analysis - Methods and Applications*, Cambridge: Cambridge University Press.
Weber, R. P. (1990), *Basic Content Analysis*, Newbury Park: Sage Publications.
Weichselgartner, J. (2001), "Disaster mitigation: the concept of vulnerability revisited", *Disaster Prevention and Management*, **10**(2): 85-94.
Vesely, W. E. and Rasmuson, D. M. (1984), "Uncertainties in Nuclear Probabilistic Risk Analyses", *Risk Analysis*, **4**(4): 313-322.
Wilhelmsson, A. and Johansson, J. (2009), "Assessing Response System Capabilities of Socio-Technical Systems", *Proceedings of TIEMS 2009*, Istanbul, Turkey.
Wisner, B. (2001), *Notes on Social Vulnerability: Categories, Situations, Capabilities, and Circumstances*, Environmental Studies Program, Oberlin College, Oberlin.
Wisner, B., Blaikie, P., Cannon, T. and Davis, I. (2004), *At Risk. Natural hazards, people's vulnerability and disasters*, London & New York: Routledge.
von Winterfeldt, D. (1992), "Expert Knowledge and Public Values in Risk Management: The Role of Decision Analysis", In: *Social Theories of Risk*, Krimsky, S. and Golding, D. (Eds.), Westport: Praeger Publishers.
von Winterfeldt, D. and Edwards, W. (1984), "Patterns of Conflict About Risky Technologies", *Risk Analysis*, **4**(1): 55-68.
Zimmerman, R. (2001), "Social Implications of Infrastructure Interactions", *Journal of Urban Technology*, **8**(3): 97-119.
Zio, E. (2007), "From complexity science to reliability efficiency", *International Journal of Critical Infrastructures*, **3**(3/4): 488-508.
Zio, E. (2008), "Reliability engineering: Old problems and new challenges", *Reliability Engineering & System Safety*, **94**(2): 125-141.

The appended papers

Paper I Johansson, J., Jönsson, H. and Johansson, H. (2007), "Analysing the vulnerability of electric distribution systems: a step towards incorporating the societal consequences of disruptions", *International Journal of Emergency Management* **4**(1): 4-17.

Paper II Jönsson, H., Johansson, J. and Johansson, H. (2008), "Identifying Critical Components in Technical Infrastructure Networks", *Journal of Risk and Reliability* **222**(2): 235-243.

Paper III Johansson, J. and Hassel, H. "An Approach for Modelling Interdependent Infrastructures in the Context of Vulnerability Analysis", submitted to *Reliability Engineering & System Safety*.

Paper IV Abrahamsson, M. Hassel, H. and Tehler, H. (2010), "Towards a systems-oriented framework for analysing and evaluating emergency response", *Journal of Contingencies and Crisis Management* **18**(1): 14-25.

Paper V Hassel, H., "Risk and Vulnerability Analysis in Practice: Evaluation of Analyses Conducted in Swedish Municipalities", submitted to *Natural Hazards*.

Paper VI Hassel, H., Tehler, H. and Abrahamsson, M. (2009), "Evaluating the Seriousness of Disasters: An Empirical Study of Preferences", *International Journal of Emergency Management* **6**(1): 33-54.

I

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

Jonas Johansson*, Henrik Jönsson and Henrik Johansson

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

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

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

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

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

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

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

1 Introduction

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

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

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

2 The concept of vulnerability

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

3 Performance measures in electric power networks

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

3.1 Existing performance measures applied to the electric distribution system

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

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

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

3.2 Proposition of a new performance measure

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

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

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

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

4 Proposition of two network analytic measures

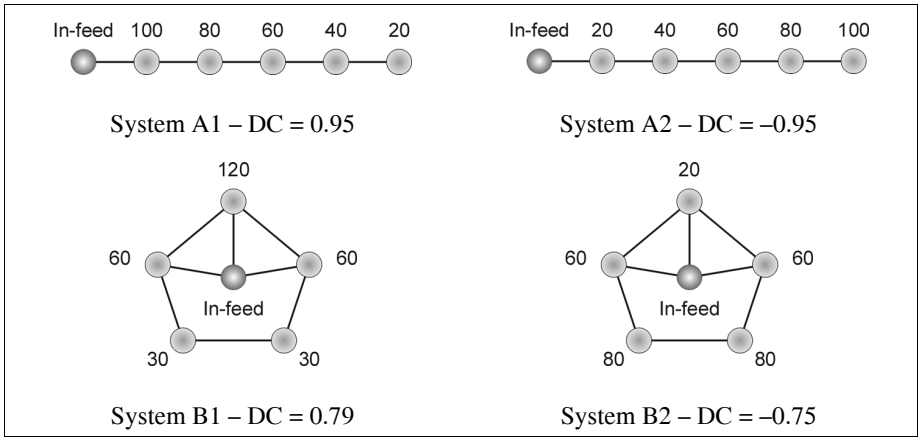
The result usually obtained from network-based vulnerability analyses is a plot of the performance measure as a function of the fraction of nodes or edges that have been removed. By studying this plot, conclusions regarding the vulnerability can be drawn, for example by comparing different systems. However,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

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

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

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

Figure 1 Example of DC values for four different systems*



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

5 Empirical vulnerability analysis of two electrical distribution systems

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

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

Table 1 Basic network characteristics of the two electric distribution systems

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

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

5.1 Strategies to remove nodes and edges

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

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

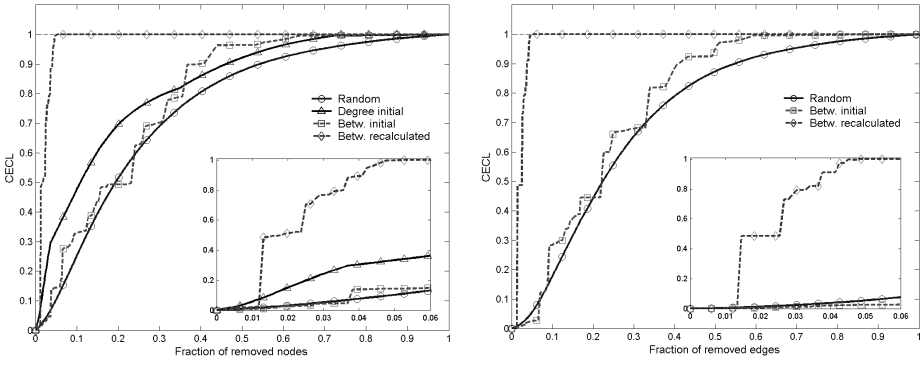
measure is based on the shortest paths between all in-feed points and distribution substations and is calculated as the sum of shortest paths traversing a specific node or edge, similar to the algorithm suggested by Newman (2001). However, instead of calculating the shortest paths between all pairs of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

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

5.2 Analysis and interpretation of simulation results

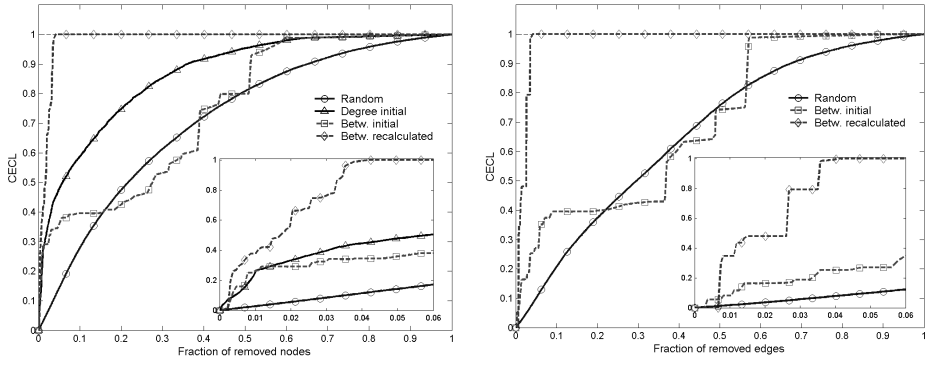
The most harmful removal strategy for System A is, as expected, the recalculated betweenness (Figure 2). For this strategy, all customers have lost power supply after the removal of 5.3% of the nodes or 5.2% of the edges. The strategy based on initial betweenness is only slightly more harmful than the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

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



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

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

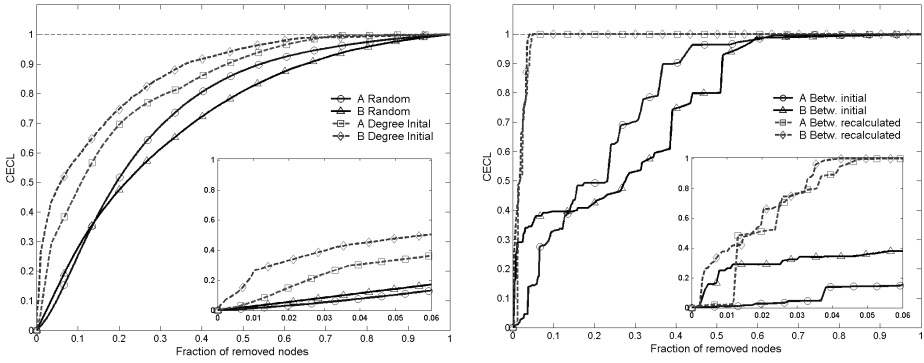


The node and edge-based removal strategies are very similar for both Systems A and B. This is due to the fact that the systems are mainly radially fed, *i.e.*, most nodes have a degree of two. In the remaining part of this paper, we focus on node-based removals, but much of the discussion is equally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

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

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

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



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

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

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

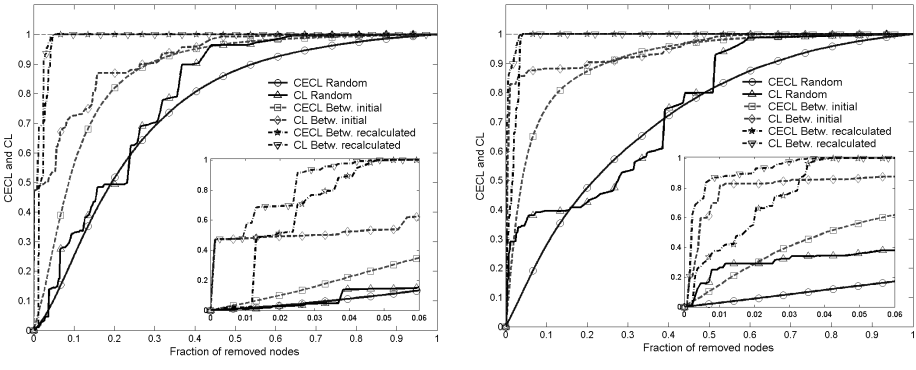
Note: * The letter in this column refers to the system that scores best on the particular measure

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

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

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

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



6 Discussion

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

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

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

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

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

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

7 Conclusion

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

Acknowledgements

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

References

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Notes

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

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

II

Identifying critical components in technical infrastructure networks

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

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

DOI: 10.1243/1748006XJRR138

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

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

1 INTRODUCTION

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

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

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

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

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

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

2 THE CONCEPTS OF VULNERABILITY AND CRITICALITY

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

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

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

3 CRITICALITY OF FAILURE SETS

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

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

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

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

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

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

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

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

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

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

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

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

4 CRITICALITY OF COMPONENTS

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

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

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

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

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

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

5 ELECTRIC DISTRIBUTION SYSTEM MODELLING

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

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

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

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

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

6 EXAMPLE OF A SMALL SYSTEM

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

Three sizes of failure sets are considered; 1, 2, and 3. Even for this small network there are 78 failure sets of size 2 and 286 failure sets of size 3: however only a few of these are synergistic; 4 and 10 sets, respectively. In Fig. 2 scatter plots of all synergistic failure sets of size 2 and size 3 are presented. The figures show that some failure sets give rise to large consequences where the synergistic fraction is small. This indicates that a large part of the total consequences can be referred to a subset of the failure

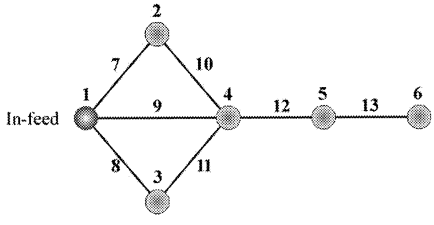


Fig. 1 Example network. The numbers in the figure correspond to the component number of the specific node or edge

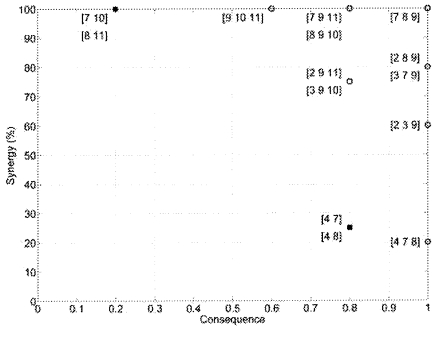


Fig. 2 Consequence-synergistic scatter plot of synergistic failure sets of size 2 (filled squares) and size 3 (circles). The consequences of the failure sets, $C(F)$ are presented on the horizontal axis and the percentage of the synergistic consequences is presented on the vertical axis

Table 1 Ranking of the criticality of failure sets*

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

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

set. Consider, for example, the {4 8} set, which means that components 4 and 8 have failed, see Fig. 2. In this case the failures cause a power loss to nodes 3, 4, 5, and 6, and most of the consequences can be referred to the individual failure of component 4, since this leads to a loss of power supply to components 4, 5, and 6. Only the power loss to node 3 constitutes a synergistic effect. In Fig. 2 it can also be seen that the failure set {7 8 9} is highly critical (maximum consequence) with a 100 per cent synergistic consequence, i.e. none of the consequences of the failure set can be referred to any of its subsets. This set can be contrasted with {4 7 8}, which leads to the same consequences but only has 20 per cent synergistic consequences, because most of the consequences derive from the critical subsets {4 7} and {4 8}, which in turn to a large extent is due to the critical component {4}. These scatter plots can thus be valuable when identifying failure sets of special interest, i.e. sets with large consequences *and* with a large synergistic fraction.

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

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

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

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

Table 3 Component contribution to the synergistic consequences

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

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

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

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

7 ANALYSIS OF AN ELECTRIC DISTRIBUTION SYSTEM

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

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

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

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

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

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

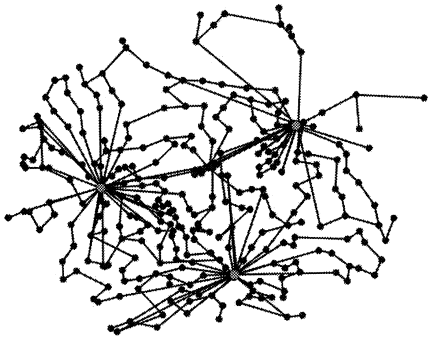


Fig. 3 Overview of the electric distribution system. The larger circles indicate in-feed nodes and the smaller circles indicate load nodes and transfer nodes

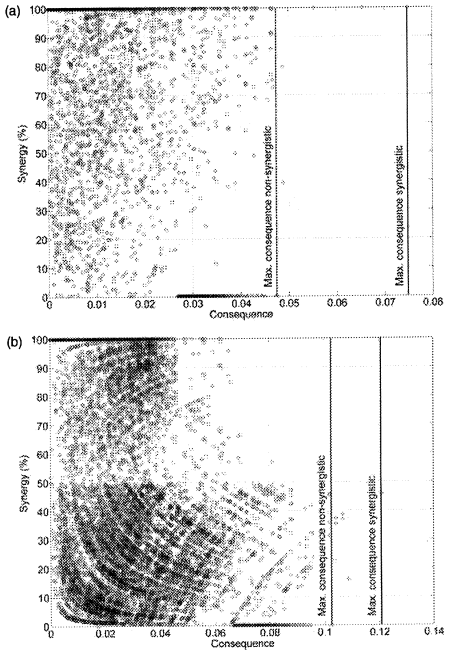


Fig. 4 Consequence-synergistic scatter plot of synergistic failure sets of size 2 (a) and size 3 (b). The consequences of the failure sets, *C(F)*, are presented on the horizontal axis and the percentage of the synergistic consequences is presented on the vertical axis. Synergistic failure sets are represented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

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

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

Each of the selected failure sets in Table 4 contains at least one bus bar at the 130/11 kV substations, indicating that these are highly critical components for the system. This result complies with common knowledge of electrical distribution systems. None of the 130/11 kV transformers are listed as highly critical components, since the in-feed capacity is roughly twice as high as the peak power demand and therefore the remaining transformers are able to supply the customers even if up to three of them should fail.

Table 4 Ranking of failure sets according to their criticality*

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

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

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

Table 5 Criticality of components in single and multiple failures

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

Table 6 Component contribution to the synergistic consequences

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

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

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

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

8 DISCUSSION

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

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

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

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

9 CONCLUSION

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

ACKNOWLEDGEMENTS

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

REFERENCES

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

III

An Approach for Modelling Interdependent Infrastructures in the Context of Vulnerability Analysis

Jonas Johansson[a,c] and Henrik Hassel[b,c]

[a] Department of Industrial Electrical Engineering and Automation, Lund University, Box 118, SE-221 00 Lund, Sweden.
jonas.johansson@iea.lth.se (corresponding author)

[b] Department of Fire Safety Engineering and Systems Safety, Lund University, Box 118, SE-221 00 Lund, Sweden.
henrik.hassel@brand.lth.se

[c] Lund University Centre for Risk Analysis and Management (LUCRAM).

Abstract
The technical infrastructures of the society are becoming more and more interconnected and interdependent, i.e. the function of an infrastructure influences the function of other infrastructures. Disturbances in one infrastructure therefore often traverse to other dependent infrastructures and possibly even back to the infrastructure where the failure originated. It is becoming increasingly important to take these interdependencies into account when assessing the vulnerability of technical infrastructures. In the present paper, an approach for modelling interdependent technical infrastructures is proposed. The modelling approach considers structural properties, as employed in graph theory, as well as functional properties to increase its fidelity and usefulness. By modelling a fictional electrified railway network, which consists of five systems and interdependencies between the systems, it is shown how the model can be employed in a vulnerability analysis. The model aims to capture both functional and geographic interdependencies. It is concluded that the proposed modelling approach is promising and suitable in the context of vulnerability analyses of interdependent systems.

Keywords
Critical infrastructures, Interdependencies, Vulnerability Analysis, Modelling, Networks

1 Introduction
Critical infrastructures constitute the backbone of the society by providing it with services that are essential for its functioning [1]. Disruptions in infrastructural services may inflict large consequences to health, safety, security and the economy. In addition, since these infrastructure services also are essential for effective emergency and disaster response, breakdowns may also cause indirect impact in the form of delayed or hampered response. The consequences of the vulnerabilities in critical infrastructures therefore propagate to the people, organisations and communities that depend on them. This in turn means that risk management efforts that have a societal perspective must encompass the critical infrastructures that are located in the area of interest [2]. Since the society's dependency of infrastructure services currently are increasing [3], and thus its vulnerability to breakdowns, such risk management efforts are becoming more and more important.

Since today's society is very dynamic, including fast technological developments and new types of threats, it is increasingly important that these risk management efforts are proactive. We can no longer wait for failures and breakdowns to illuminate the vulnerabilities that are inherent in our systems. Instead we must strive to anticipate future problems, emerging threats and

vulnerabilities, and identify effective risk reduction strategies before wide spread disturbances occur. Risk and vulnerability analyses can help establishing a good basis for decisions regarding risk reduction and control [4]. In a risk and/or vulnerability analysis, increased knowledge is sought about the systems of interest, including what threats that expose the systems and what consequences that may arise from those threats that materialize.

Critical infrastructures are often described as large-scale, spatially distributed systems with high degrees of complexity. These complexities largely stem from the vast functional and spatial dependencies and interdependencies that exist among the infrastructure systems [5], which enable failures to cascade from a system to other systems [6]. There may even be feedback loops causing the failure to cascade back to the system from where the failure originated. Such cascading failures have been witnessed in several recent crises and disasters, for example in the U.S. power outage in 2003 [7], the storms Gudrun [8] and Per in Sweden 2005 and 2007, respectively, and Hurricane Katrina [9]. Analyses conducted on infrastructure systems in isolation from the systems with which they interact, do not capture secondary and higher-order effects; the result being that the negative consequences of disturbances are underestimated – possibly drastically. In addition, without systematic analyses, such higher order effects are often very difficult to anticipate and understand the effects of. Therefore, a comprehensive and holistic modelling approach is needed, where interconnected infrastructure systems are being studied as "a system of systems" [10].

Much effort is currently devoted to develop models and methods capable of analyzing interdependent infrastructure systems – for an overview of methods and models see [11]. These models and methods can broadly be divided into two categories. The first category can be termed *predictive approaches*. Predictive approaches aim at modelling and/or simulating the behaviour of a set of interconnected infrastructures in order to, for example, investigate how disturbances cascade between the systems. A wide range of different perspectives and ways of representing the systems of interest exist; including for example economic-mathematical models [12], economic-system dynamics models [13], agent-based models [14], and network modelling approaches [15]. The appropriateness of using the one model or the other in a predictive vulnerability analysis clearly depends on the purpose and perspective of the analysis. The second category is called *empirical approaches*. Empirical approaches aim at studying past events in order to increase our understanding of infrastructure dependencies. Furthermore, the purpose is to identify patterns of interest to policy and decision-making, such as how often failures cascade between infrastructures and patterns related to the extent the society is affected by infrastructure failures caused by interdependencies. The framework proposed by a research group from University of British Columbia [16]-[17] provides one good way of structuring empirical analyses of infrastructure interdependencies. Other empirical analyses include Zimmerman's and colleagues' [18]-[19].

The two categories of approaches just described are complimentary, which is also pointed out by McDaniels and colleagues [16], when it comes to using them as input to risk and vulnerability analyses or as a basis for decisions regarding prevention or mitigation. The predictive approaches can provide important information of the particular systems of interest and facilitate for the implementation of a proactive approach to risk management and critical infrastructure protection. The empirical approaches, on the other hand, can provide important information regarding general patterns of infrastructure interdependencies and how failures cascade between different types of systems. Empirical studies are thus very important for the general understanding of infrastructure interdependencies and can provide input both to the predictive models as well as to decision-making and policy.

The challenges for understanding, characterizing and modelling these systems are immense, and the current efforts in this field are still in an early stage (e.g. [6],[11],[20]). The existing methods and models address the same issue, the impact of interdependencies, but from different

viewpoints. We argue that models and methods that have different viewpoints are necessary in order to appropriately and comprehensively address the issue of interdependencies, i.e. there is no universal, all-encompassing model. This is also pointed out by both Eusgeld et al. [21] and Murray et al. [22]. The suggested approach focuses on systematically and comprehensively finding potential high consequence scenarios. More specifically, the aim is to develop a predictive modelling approach for interdependent infrastructures and to briefly exemplify its use in a vulnerability analysis context. The modelling approach builds on earlier work of the authors [23]-[24] and on ideas from network analysis [25]. In order to demonstrate the applicability of the model it is used to study the vulnerability of a fictional electrified railway system, which consists of the physical railway track, two internal electrical power systems, a telecommunication system and in-feed points from external electrical distribution systems.

2 Perspectives on vulnerability

Risk and vulnerability analyses are essential tools for proactive risk and crisis management. The meaning of the concepts, and the interrelationship between them, however, vary considerably between different disciplines, and even within a particular discipline (e.g. [26]). It is therefore important to be clear and explicit about how these concepts are being used in the present context.

Here, risk is broadly seen as a combination of the "probability and severity of adverse effects" [27]. In order to adequately analyze risk one must identify all relevant risk scenarios, and for each scenario estimate its associated likelihood of occurrence and negative consequences [28]-[29].

The concept of vulnerability has two closely related interpretations in the research literature, which are relevant here. In the first interpretation vulnerability is seen as a global system property that expresses the extent of the adverse effects caused by the occurrence of a specific hazardous event (see e.g. [30]-[31]). This interpretation of vulnerability is thus very closely related to the definition of risk stated previously; the main difference being that the identification and characterization of risk scenarios are conditioned upon the occurrence of a specific hazardous event or strain.

In the second interpretation, vulnerability is used to describe a system *component* or an *aspect* of a system [15],[26],[32]-[33]. With this interpretation a component, for example, is said to be *a vulnerability* of a system if the failure of that component cause large negative consequences to that system. In the present paper, such a component will be referred to as a *critical component* and the term vulnerability will be used to describe a system property in accordance with the first interpretation stated above. For a more detailed discussion on the concept of critical components see [24].

Another version of the second interpretation of vulnerability, which is relevant in the context of interdependent infrastructures, is *critical geographical locations*. These criticalities stem from the co-locations of components in various infrastructure systems. Due to the co-locations, an event that occurs in some geographic location, such as a malicious act or adverse weather, may affect several different components in one or several different infrastructures simultaneously. Locations where such an event would lead to large negative consequences would therefore be termed critical geographical locations (see e.g. [34]-[35] for two approaches addressing critical geographical locations).

The model presented here aims to facilitate the analysis of all perspectives referred to above, i.e. global system vulnerability, critical components and critical geographical locations. This is because by employing several analytical perspectives *complementing* insights regarding the system's

vulnerability can be gained. Using several analytic perspectives is argued to be especially important for the analysis of complex systems.

The three perspectives of vulnerability analysis can be seen as a part of a more comprehensive risk analysis. In order to enforce appropriate risk mitigating measures, the identified vulnerabilities must be addressed in a larger scheme that encompasses an analysis of the threats and hazards that might exploit these vulnerabilities (especially including their probability). Note, however, that the present paper will only address the vulnerability part of risk.

3 Characterizing interdependencies

An approach for modelling interdependent infrastructure systems must address the issue of how to characterize interdependencies. But before describing different ways of characterizing interdependencies and the way chosen in the present paper, the meaning of the term itself should be clarified since different interpretations exist in the literature. Rinaldi et al. [36] argue that an interdependency is a *bidirectional relationship* between two infrastructures – the state of infrastructure *i* is somehow dependent on the state of infrastructure *j*, *and* vice versa. From this view interdependencies are macro-properties of coupled systems; they do not in general exist between individual components of systems. Other interpretations, however, do not necessarily treat interdependencies as bidirectional relationship; instead they are seen as *unidirectional* relationship between systems, thus treating dependencies and interdependencies as synonyms (see e.g. [16]). In the present paper, Rinaldi and colleagues' definition of interdependency will be used. Furthermore, the term dependency will be used to describe unidirectional relationships that can also exist on the micro level of systems, i.e. the state of one or several *components* in a system is dependent on the state of a component in another system. Therefore, only the term dependencies will be utilized when describing relations between components and the term interdependencies will be used when discussing coupled infrastructures in a macro-perspective.

Dependencies can be direct (of first order), which often are quite easily spotted and their existence well known. However, dependencies can also be indirect, i.e. of higher order. For example, if infrastructure *i* is dependent on infrastructure *j* and infrastructure *j* is dependent on infrastructure *k*, then a second order dependency exists between infrastructure *i* and *k*. Such higher order dependencies are much more difficult to spot and it is more difficult to make sense of their effects without explicit modelling and simulation.

Several authors have suggested frameworks and methods for characterizing and analyzing interdependencies. One of the more commonly cited framework for characterization is the one proposed by Rinaldi et al. [36], where interdependencies are characterized as either *physical* (an output from a system is required as an input to another system and vice versa), *cyber* (the state of a system is dependent on information transmitted through an information infrastructure), *geographic* (two or more systems can be affected by the same local event, i.e. they are spatially proximate), and *logical* (includes all other types of interdependencies, for example related to human behaviour). Zimmerman et al. [18] propose a somewhat coarser classification where infrastructure interdependencies are either seen as *functional* or *spatial* (where spatial is identical to geographic interdependency as referred to above). Furthermore, in another paper Zimmerman and colleagues [19] use the term geographic interdependency to denote a power outage that spread across several US states rather than being contained in one state. Thus, their use of the term geographic interdependency differs from Rinaldi and colleagues'.

In the present paper interdependencies will be classified as either functional (including physical, cyber and logical interdependencies from the classification proposed by Rinaldi et al., since these can be treated the same basic way) or geographical (from the classification proposed by Rinaldi et

al.). A literature search conducted by the authors revealed that only a few models aim to capture geographic dependencies. The model proposed by Patterson and Apostolakis [34] is one example; however, that model does not capture any functional interdependencies.

4 Proposed model

This section describes how the individual systems are modelled and how dependencies are characterised in the modelling approach.

4.1 Modelling the individual systems

The proposed model, which is summarized in Figure 1, is inspired by the field of network theory (see e.g. [25] and [37]), where two basic components, nodes and edges, build up the model of the system. This approach is appropriate for modelling systems that have clearly defined components, such as technical infrastructures. In contrast to strict network theory (graph theory) where only topological features are studied, we advocate that physical and functional properties of the studied systems must be incorporated for the model to be of real practical value. Therefore, each infrastructure is represented both in terms of a *network model* and a *functional model*.

In the network model the system's physical components are represented as nodes (e.g. bus bar in a power system and a switch in a telecommunication system) and edges (e.g. power lines and opto-fibers). The network structure provides a common modelling platform, since all infrastructures are modelled in the same fundamental way.

In the functional model of each infrastructure the function of the system is described. Both physical and operational characteristics are incorporated in the functional model. For example, the functional model of a power distribution system could specify that a distribution substation can provide electricity to its customers and to dependent systems, if there is an unbroken path, given by the network model, to an in-feed node and that proper operational activities are carried out. In order to evaluate an individual system's performance, the functional model is used together with the network model and the system's dependencies to other systems.

The location of infrastructure components are modelled in accordance with geographical coordinates which are defined in a three dimensional Cartesian coordinate system. This enables geographical vulnerability analysis, thus addressing geographical dependencies between components. The effects of geographical dependencies are addressed when analyzing critical geographic locations, further described in section 5.3.2.

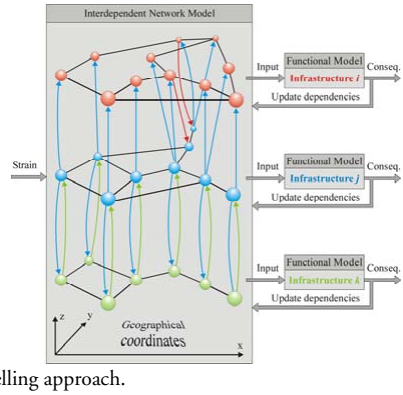


Figure 1. Overview of modelling approach.

4.1 Modelling functional dependencies

Functional dependencies between infrastructures are modelled explicitly as edges between nodes in different infrastructures. These edges are henceforth called *dependency edges* in order to distinguish them from the edges within the individual systems. If an infrastructure is not able to supply the demanded service the outgoing dependency edge is removed, thus signalling the unavailability of the desired service to other infrastructures. The effect of a removed dependency edge is evaluated separately in the functional model of each of the dependent infrastructures. This means that each infrastructure only sees and acts upon local information regarding dependencies.

To further illustrate how dependencies are modelled, the example of the power distribution system, mentioned in 4.1, is continued here. In this case a telecommunication system is dependent on power supply to function; therefore, dependency edges exist between distribution substations in the power distribution system and nodes in the telecommunication system. When a power distribution substation loses its function, all its dependency edges to the nodes in the telecommunication system are removed and the consequences of the removed dependencies are evaluated in the functional model of the telecommunication system. Since telecommunication nodes are highly dependent on electric power supply, they will loose their function if no alternative source of power exists (alternative connection to the electric distribution system, diesel generator, battery back-up, etc.).

Once the individual systems and their dependencies to other systems have been modelled, these models are merged into a model for the interdependent system of systems as a whole. This enables higher-order dependencies to be captured, which is essential for any interdependency analysis approach.

4.3 Incorporating temporal aspects in the model

The consequences of strains in infrastructure systems are usually twofold, both the consequences in terms of the magnitude of interrupted services (e.g. the number and type of customers affected) and in terms of the duration of the interruption. In order to capture the temporal aspect of the consequences, it is necessary to incorporate estimates of the duration of the components unavailability due to various strains, which yields a dynamical modelling approach. In order to capture the duration of unavailability due to strains, estimated repair times are used.

Technical infrastructures are usually very tightly coupled, in the sense that interruptions in one infrastructure directly have an impact on a dependent infrastructure. However, buffers are often used in order to make couplings between systems somewhat less tight. An example of a buffer is having stocks with fuel in a district heating system, rendering the system less vulnerable to disruptions in the fuel supply. Another example is uninterruptible power supply (UPS) systems between electrical supply systems and telecommunication systems. The buffers usually have limited capacity in terms of the time it can sustain its function without the service from the infrastructure it depends upon. In the proposed model, such buffers are incorporated as a time delay between the loss of a dependency and the impact of it, where the length of the time delay represents the buffer capacity.

4.4 Modelling strains

The aim of the modelling approach suggested in the present paper is that it should be applicable for vulnerability analysis of interdependent infrastructure systems, meaning that it becomes important to be able to represent strains. As was described earlier, the approach is inspired from the field of network theory; and in analogy to network theory (see e.g. [38]-[39]), strains to the infrastructures will be represented as removal of nodes or edges in the network model of one or several infrastructures. A strain could also be represented as a removal of a dependency edges between two infrastructures, in order to evaluate the direct effects of dependencies. The removal

of components is thus a way of representing that a component is not able to deliver its designed function

4.5 Computer program structure

The present section briefly describes how the modelling approach has been implemented in the computer simulation program, so that it can be more readily used for vulnerability analysis. Examples of the applications will then be given in the railway example in section 5.

The basic idea of the modelling approach is to translate the models of the interdependent infrastructure systems (in a network and a functional part) into computer code and implement it in a computer simulation program. Once implemented, it is possible to systematically evaluate the vulnerabilities of the infrastructures, taking dependencies into account. More specifically, systematic analyses are carried out from the three analytical perspectives as described in section 2. However, independent of the analytical perspective the same basic simulation structure can be used. The simulation is time-dependent and consists of a set of commands that are executed in each time step, which can be structured in four main sub steps, described in Table 1.

Table 1. Structure of the simulation code as executed in each time step.

Sub step	Description
1. *Structural change due to strain and/or repair*	Components are removed due to a strain from the network models. Counters for time left before the components are repaired are updated. When a component is repaired it is added again to the network model.
2. *Functional evaluation for individual systems*	The functional model for each system is used to evaluate the individual system's performance. If any functional change occurs that affects the state of a component, the status of its outgoing dependency edges, if any, are updated.
3. *Changes due to dependencies*	Cascading effects are evaluated by initiating an iterative loop that updates the network and functional models with respect to changes of dependency edges. The loss of a dependency edge is reflected by removing dependent components, i.e. a structural change in the network model similar to step 1. The functional models are then used to evaluate the systems' performance, similar to step 2. The iterative loop is repeated until no further changes occur for any system.
4. *Update buffers*	Any existing buffers, such as remaining capacity of battery-back-up, are updated, if necessary. A new time step is then initiated by starting from sub step 1 again.

5 A Railway Example

The modelling approach is applied to a fictional electrified railway system, similar to the actual railway system in southern Sweden in terms of structural, functional and geographical attributes. The operation of the railway system has first- and second-order dependencies to four other infrastructures, namely: the traction power system, the telecommunication system, the auxiliary power system and finally the electrical in-feed system, in accordance with Figure 2. The vulnerability analysis focuses on the impact of technical interdependencies and in the time-span of up to 24 hours.

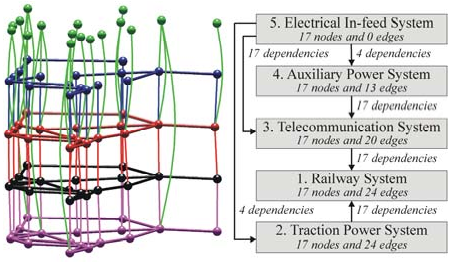


Figure 2. Infrastructure systems that are modelled and an overview of the dependencies that exist between the systems.

5.2 Functional models and dependency modelling

Only the most essential functional properties of the systems are modelled in order to provide a comprehensible example. However, more detailed functional models could be developed in order to increase the fidelity of the result, although there is an upper limit for how detailed the models can be in order for the analysis to stay within reasonable time frames (here reasonable are considered simulation times of 24 h or less).

The functional model of the railway system is implemented as a breadth first search algorithm in order to find out which railway stations are possible to travel to and from, depending on the state of railway system. As long as there is at least one possible way to travel between the stations, it is said that no consequences arise. The loss of service is evaluated as the fraction of travellers not able to reach their desired destination. The numbers of travellers to and from the specific stations are estimated from actual data from the region and an overview of the data is presented in Figure 3. A section of the railway is in function as long as the section has access to the telecommunication system and as long as the traction power system is able to supply electricity, i.e. there are dependency edges to both the telecommunication system and the traction power system. The repair times of nodes and edges are set to 24 and 12 hours, respectively.

The traction power system is only dependent on one other system, namely four in-feed points from the electrical in-feed system. Each in-feed point of the traction power system has a limited power rating, and the other nodes of the system have a loading corresponding to the average power demand. The functional model of the traction power system checks if the nodes of the system are supplied by controlling that: first, there is a path between the node and an in-feed node, and second, that there is enough power available for it to be supplied. The loss of service is evaluated as the fraction of unsupplied nodes. The repair times of nodes and edges are set to 8 and 4 hours, respectively.

The power demand of the telecommunication system is supplied either via the auxiliary power system or the electrical in-feed system. The telecommunication system also has buffers in the form of UPS-supply, with a capacity of 4 hours. This means that when a telecommunication node loses its power supply from both systems it depends upon, it maintains its function for 4 hours. The functional model of the telecommunication system is a straightforward breadth first search-algorithm that checks the possibility of each node to communicate with the rest of the nodes in the network, i.e. communication between two nodes is possible as long as there is a path between them. The loss of service is evaluated as the mean loss of communication for all nodes in the network. The repair times of nodes and edges are set to 6 and 3 hours, respectively.

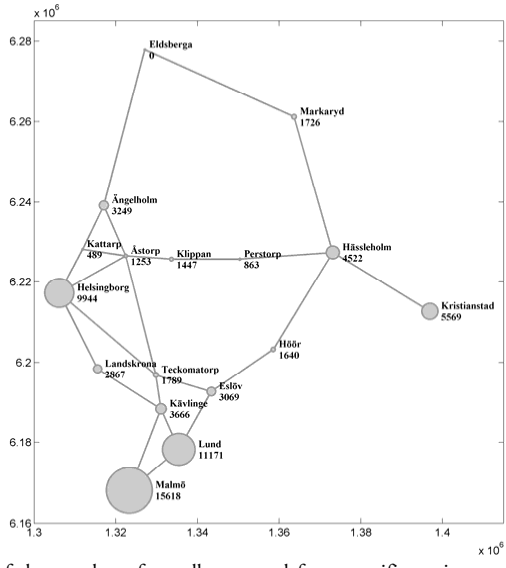


Figure 3. Overview of the number of travellers to and from specific stations per day. The node size is proportional to the number of travellers for a specific station. For each node the name of the station and the number of travellers is given. The axes show the geographic coordinates according to the Swedish coordinate system RT90 (expressed in metres).

The auxiliary power system is an electrical distribution system, owned by the railway company, which is geographically co-located with the traction power system (the power lines are physically located in the same poles as the overhead contact wire for the traction power). It is dependent of in-feed from the external electrical in-feed system. The functional model of the system is the same as the one used for the traction power system, but with other in-feed capacities and power demands. The loss of service is evaluated as the fraction of unsupplied power. The repair times of nodes and edges are set to 6 and 3 hours, respectively.

The external sub-transmission and electrical distribution systems are simplified into one electrical in-feed system. Only the in-feed nodes are considered, i.e. neglecting the structural properties of these systems. The reason for the simplification is that here, the interest is only to evaluate the impact of lost power supply to the traction power system, the auxiliary power system and the telecommunication system. The loss of service is given as the fraction of lost in-feed nodes. The repair time of restoring in-feed nodes are set to 4 hours.

5.3 Exemplifying different types of vulnerability analyses

The exact procedure for a vulnerability analysis depends on the interest in the particular study. One can, for example, have an interest in the vulnerability of one of the infrastructures when the systems it depends on are exposed to strains. One can also have an interest in the vulnerability of several interdependent infrastructures as a whole when one or several infrastructures are exposed to strains. Different interests would lead to somewhat different procedures for vulnerability analysis; however, the same basic modelling approach can be used.

The aim of this example is to exemplify the use of the suggested modelling approach for vulnerability analysis of interdependent technical infrastructures. Results from three different types of vulnerability analyses will be presented – corresponding to the three analytical

perspectives described in section 2. First, a global vulnerability analysis perspective is taken where strains of increasing magnitude are applied to one infrastructure at a time and the consequences of the strain are evaluated for each of the infrastructures, in accordance with the approach presented in [23]. Secondly, a systematic identification of critical components, and sets of components, is carried out in accordance with the approach presented in [24]. Thirdly, a systematic identification of critical geographic locations is carried out by removing components that are spatially proximate to each other and evaluating the consequences – i.e. specifically addressing geographical interdependencies.

The primary focus in each of the three types of analyses is on how the railway system is affected when the systems it depends upon are exposed to strains. The negative consequence for railway system is calculated by summing the loss of service (expressed as the fraction of customers that cannot reach their desired destination) over all time steps. As such, this yields a measure that can be interpreted as lost service hours. For example, if the loss of service is 1 for 2 hours the total consequence will be the same as if the loss of service is 0.5 for 4 hours, i.e. 2. The consequences are thus linearly time dependent. Note that for especially time critical systems, such as industrial refineries, non-linear time dependencies can be incorporated in the model. This can for example be done by implementing consequence thresholds with respect to time, i.e. no or very small consequences up to a certain duration of the disruption but very large consequences when the duration is only slightly longer.

5.3.1 Global vulnerability analysis

The global vulnerability analysis is carried out by randomly removing components, i.e. applying strains to, in the systems that the railway system is functionally dependent on. In a random removal each component in the system that is exposed to strain has an equal probability of being removed. Components are successively removed, while evaluating the consequences that arise in the interdependent systems, until all (or a desired number of) components have been removed. Since the removal is random, each simulation run is likely to yield different results in terms of how the systems are affected.

In Figure 4 the results from 1000 simulations is presented. The result shows the average consequences in the railway system when applying strains to each of the four other systems separately as well as when applying strains to all four systems simultaneously. This type of global vulnerability analysis shows what impact strains to different systems has on a system of interest, in this case the railway system. Consequences that arise for the railway system are solely due to functional dependencies. The shape of the curves differs significantly depending on the system under strain. No consequences arise for the railway system for any magnitude of strain to the auxiliary power system. This is due to the fact that the telecommunication system, which the railway system is dependent upon, has redundant power supply, i.e. also supplied from the electrical in-feed system. The other curves reach a maximum corresponding to the longest repair time for a component in the infrastructure under strain times one, since no travellers can reach their destination when all components have been removed. Different magnitudes of strain for the different systems give very different consequences for the railway system. For example, compare the strain level of 0.1 where the in-feed system gives a consequence of 0.07, the traction power gives a consequence of 0.56 and the telecommunication system of 1.39. This type of plot clearly shows the criticality level of the systems that the railway system depends upon.

Not presented in figure 4, due to reason of clarity, is the variation of possible consequences for different magnitudes of a strain. Figure 5 shows the variation of the consequences for the railway system when components in all four systems, i.e. not the railway system, are removed randomly with equal probability. Left in Figure 5 the maximum, minimum and average consequences in the railway system for various magnitudes of the strains is presented. The figure shows that there

is a wide variation of possible consequences for a given magnitude of strain. Right in Figure 5, the probability that the consequences exceed specified consequence levels as a function of different magnitude of the stains is presented. This type of plot more clearly reveals the different consequences that can arise given a certain magnitude of strain. For example, given the strain of 0.1 the probability that the consequences is equal to or above 2 is 0.55, 4 is 0.16 and 6 is 0.01. Such plots is thus valuable for revealing the varying criticality of components in the systems, a small variation would indicate that there is a small difference in criticality between components while a large variation indicates that some components are highly critical while others are less critical. In order to gain certainty of which these highly critical components are, a more thorough analysis regarding critical components is necessary.

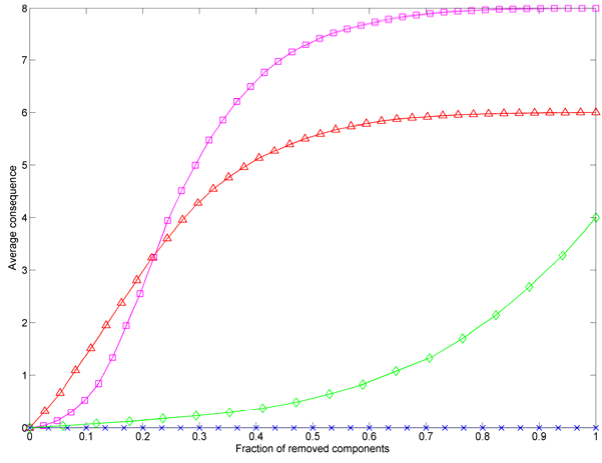


Figure 4. The consequences for the railway system for varying magnitude of the strain when applied to the traction power system (□), the telecommunication system (Δ), the auxiliary power system (x) and the in-feed system (◊) are exposed to random removals. The consequences are averaged for 1000 simulations.

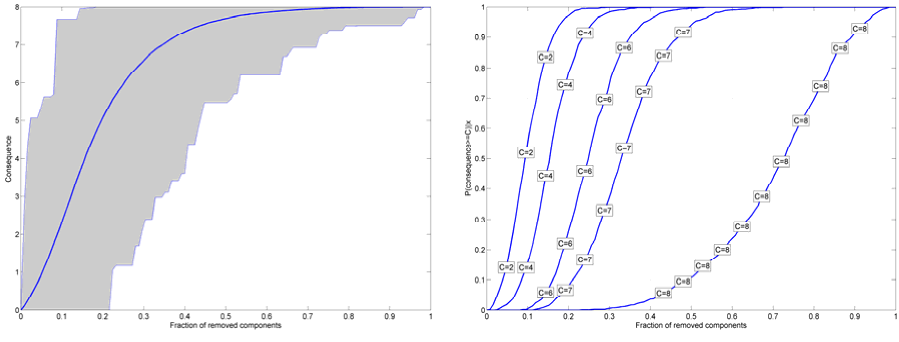


Figure 5. To the left the maximum, minimum and average consequences for the railway system for varying magnitudes of the strain when the traction power system is exposed to a random removal. To the right the probabilities that the consequences exceed the specified consequence levels (C) given the same strain as above. All values are based on 1000 simulations.

5.3.2 Identifying critical components

The identification of critical components requires systematic and exhaustive consequence calculations for any given number of simultaneous component failures. However, a practical issue when analysing combinations of failures is that the number of failure combinations to evaluate increases exponentially as the number of components of the system increases and as the number of simultaneous component failures of interest increases. Therefore, there is an upper limit for where computational times can be considered as feasible. In the present analysis it was feasible to consider single failures and combinations of two and three simultaneous failures. The combination of failed components is not restricted to only one infrastructure, but rather it is the combination of simultaneous component failures in differing infrastructures that often are of greatest interest since this has the greatest potential of discovering unforeseen consequences.

In Table 2 the results from the analysis of critical components are presented. Components in the telecommunication system are generally found to be the most critical ones for the railway system when considering single, two and three simultaneous failures. It is in particular a few telecommunication nodes located in conjunction with the largest stations that are identified as most critical. Besides the telecommunication system, a number of components in the traction power system are also shown to be highly critical. Also shown in the table are the consequences to the other four systems, which give indications of how impacts spread between the studied systems. One interesting example is the comparison of the single failure components ranked 1 and 4, showing how a smaller consequence for the telecommunication system can lead to higher consequences in the railway system.

The analysis of critical components points to a similar result as found in the global vulnerability analysis, where the strains to the telecommunication system lead to largest impact for the railway system when the number of removed components is fairly small. For larger strains, however, the traction power system becomes more critical. One benefit from the analysis is knowledge about which components that contributes the most to the vulnerability of the system as a whole – important when considering how to make the system as a whole more robust.

5.3.3 Identifying critical geographical locations

Analysis of critical geographical locations is addressed by removing components in close proximity to each other. In general terms, this could be due to severe weather conditions or antagonistic threats striking geographically confined areas. Utilized here is a cell space method, where components in the different infrastructures that are co-located in the same cell space are removed. The results of such an analysis are dependent on the cell size, the shape of cell (square, hexagon, circle etc.) and displacement of the cell grid. Jenelius and Mattsson [35] use square cells and examine the impact of cell size and grid displacement on the result when assessing the vulnerability of road networks under area-covering disruptions. They used square grid cells with three different sizes; 12.5, 25 and 50 km. Patterson and Apostolakis [34] used a hexagonal grid approach to study geographical dependencies between systems in a university campus area. They argue that the choice of cell size has to do with what threats are of concern and they perform an analysis with respect to a bomb with a radius of influence of 7 m.

Table 2. The top ten identified critical components and combinations of two and three components in the infrastructure systems that the railway system depends upon. Consequences are presented for all systems, but the rankings are based on the consequences for the railway system.

Single failure		Consequences				
Rank	System {Component}	System 1 Railway	System 2 Traction	System 3 Telecom	System 4 Auxiliary	System 5 In-feed
1	3 {1}	**2.72**	0	0.71	0	0
2	3 {3}	**1.95**	0	0.71	0	0
3	3 {10}	**1.73**	0	0.71	0	0
4	3 {6}	**1.69**	0	1.37	0	0
5	2 {6}	**1.29**	0.94	0	0	0
6	3 {15}	**0.97**	0	0.71	0	0
7	5 {6}	**0.65**	0.47	0	1.18	0.24
8	2 {30}	**0.65**	0.24	0	0	0
9	3 {2}	**0.64**	0	0.71	0	0
10	3 {12}	**0.57**	0	0.71	0	0
Two simultaneous failures		Consequences				
Rank	System {Component}	System 1 Railway	System 2 Traction	System 3 Telecom	System 4 Auxiliary	System 5 In-feed
1	3 {2} 3 {3}	**4.40**	0	1.99	0	0
2	3 {1} 3 {4}	**4.36**	0	1.99	0	0
3	3 {1} 3 {3}	**4.09**	0	1.37	0	0
4	3 {2} 3 {4}	**4.07**	0	2.51	0	0
5	3 {1} 3 {10}	**4.00**	0	2.51	0	0
6	3 {1} 3 {6}	**3.91**	0	1.99	0	0
7	2 {6} 3 {1}	**3.75**	0.94	0.71	0	0
8	2 {1} 2 {20}	**3.63**	0.47	0	0	0
9	3 {1} 3 {17}	**3.47**	0	1.99	0	0
10	3 {1} 3 {15}	**3.42**	0	1.37	0	0
Three simultaneous failures		Consequences				
Rank	System {Component}	System 1 Railway	System 2 Traction	System 3 Telecom	System 4 Auxiliary	System 5 In-feed
1	2 {1} 2 {2} 2 {4}	**5.45**	1.88	0	0	0
2	3 {2} 3 {3} 3 {10}	**5.37**	0	3.09	0	0
3	3 {1} 3 {4} 3 {6}	**5.25**	0	3.57	0	0
4	3 {1} 3 {4} 3 {10}	**5.19**	0	3.53	0	0
5	2 {6} 3 {2} 3 {3}	**5.19**	0.94	1.99	0	0
6	3 {2} 3 {3} 3 {6}	**5.18**	0	3.09	0	0
7	2 {6} 3 {1} 3 {4}	**5.16**	0.94	1.99	0	0
8	2 {2} 2 {4} 5 {1}	**5.07**	1.41	0	1.18	0.24
9	2 {2} 2 {4} 2 {19}	**5.07**	1.18	0	0	0
10	3 {3} 3 {5} 3 {10}	**5.06**	0	3.44	0	0

In the present analysis square grid cells are used. The interest, as in the previous two types of vulnerability analyses, is in the consequences that arise in the railway system due to its functional dependencies to the systems that are affected by the geographically confined strain. Therefore, all components within a cell, except for components in the railway system, are removed. In Figure 6 the results of analyses with two different cell sizes, one where the cell size is 5 x 5 km and one where the cell size is 2.5 x 2.5 km, are presented. Both cell sizes shows the same general result, namely that the most critical geographical locations correspond to the areas where the largest stations are situated. The most critical location gives rise to a consequence of 4.02 and the least critical location, above zero, give rise to a consequence of 0.32. Geographical locations where only edges are situated are generally not critical. The reason is that no consequences arise as long as there is some path enabling the travellers to reach their destinations. Since the railway system has several alternative routes between the stations, with the exception of the railway track between Hässleholm and Kristianstad as seen in Figure 2, no consequences arise when only a single path is impassable. When two separate paths are affected simultaneously however, see the Malmö-Lund-Kävlinge area in Figure 2, consequences can arise. As the cell size gets smaller, however, there are fewer areas where cells cover several paths, as can be seen when comparing the two different cell sizes in Figure 6.

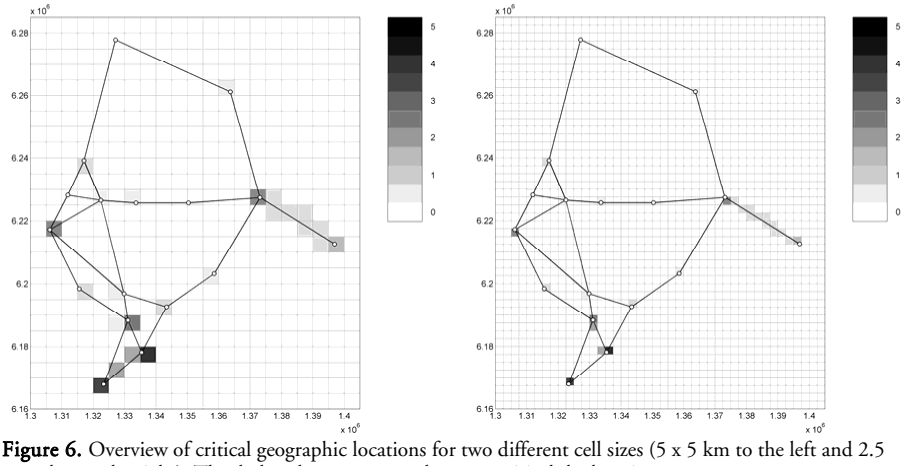


Figure 6. Overview of critical geographic locations for two different cell sizes (5 x 5 km to the left and 2.5 x 2.5 km to the right). The darker the squares are the more critical the locations are.

6 Discussion

The proposed modelling approach has been described and exemplified in a brief vulnerability analysis of an electrified railway system. The example shows the value of the proposed modelling approach in identifying vulnerabilities due to functional and geographical dependencies. Without a modelling approach that accounts for functional and geographical dependencies, the impact of strains on interdependent infrastructures will most likely be highly underestimated. Another benefit of using a systematic and comprehensive modelling approach supported by computer modelling is that higher order dependencies can also be captured, which otherwise are very difficult to take into account and understand the effects of.

The functional models used in the example have, admittedly, been rather coarse; however, more refined models can be implemented while still using the same analytical approach. Of course, more refined models put demands on more detailed information and require longer computational times, which can constitute considerable challenges for analyses in practice. The

simulation times for the railway example were fairly short, due to the small size of the studied system and the rather rough representation of the systems. In order to increase the fidelity of the models of the railway infrastructure systems, it is appropriate to develop the functional models in cooperation with stakeholders and expertise from each of the infrastructures, utilizing existing knowledge of how these systems function. In addition, the negative consequences considered in the example should be seen as only a part of the actual consequences that arise in the railway system. For instance, consequences related to delays for travellers and to transportation of cargo were not addressed.

Something that was found important for the results of the performed vulnerability analysis is the repair times for the various components in the different infrastructures. Here plausible repair times for the different systems were simply assumed, however, they are always associated with a great deal of uncertainty. For example, they are most often dependent on the extent and type of strain. In an electric distribution system, for example, strains that cause many failures in the system will most likely also cause longer repair times, since repair resources, such as repair crews and spare parts, are limited. In addition, strains can lead to conditions making repair work more difficult, for example a severe storm making roads impassable. Wilhelmsson and Johansson [40] have suggested a method that addresses the question of more accurately estimating repair times; in particular, the effect of type and magnitude of strain on repair times. It would be fruitful to combine the modelling approach suggested in the present paper and this method for estimating repair times. Another way to address the issue of repair time is to conduct sensitivity analyses in order to find out how much the results are affected by changes in repair times. It is also possible to conduct systematic simulation studies, with respect to repair times, in order to identify critical thresholds.

The global vulnerability analysis shows how systems withstand strains and how the consequences cascade to dependent systems. In the example the focus were on examining the vulnerability for all magnitudes of strain, i.e. from none to all of the components removed in one or several systems. It is also possible to carry more in-depth analysis for a lesser magnitudes of strain, for example running more simulation for strains up to 10% of removed components. The global vulnerability analysis gives information of the criticality of different systems and gives an indication of whether or not the components in the system can in general be considered equally critical or that their criticality varies.

In the critical component analysis it was seen that some components are highly critical in themselves causing combinations of failures including these components to also be highly critical. However, highlighting these components as critical when considering simultaneous failures adds little new information since their criticality was already highlighted when considering single failures. More interesting are the components that are not critical in themselves but turn up to be critical when they fail simultaneously, since these are more difficult to recognize. In applying the ideas presented by Jönsson and Johansson [24], related to synergistic consequences, it would be possible to screen among combinations of component failures in order to more readily highlight such especially interesting combinations of failures. Another difficulty related to identification of critical components is that different rankings are generated for different numbers of simultaneous failures. However, being able to generate a single criticality ranking for components s would be highly valuable, e.g. as a basis for prioritization of resource. In Jönsson and Johansson [24] a procedure for generating such aggregated importance measures was suggested, which is also applicable in the present context.

The identification of critical geographic locations used a straightforward square grid approach and no explicit reference is made to a specific threat of interest. Since the specific threat influences how the infrastructures are affected, a more thorough analysis should address how the threat

characteristics influence the choice of cell size and cell shape. In addition, some threats do not affect all infrastructures and components within infrastructures in the same way. In an electrical distribution system, for example, storms are much more likely to affect overhead power lines than underground cables. When it comes to floods, on the other hand, the opposite could be more likely. Furthermore, the time factor can be important to take into account, since some threat exposures, such as adverse weather, are prolonged over time. In the example the systems were widely geographically dispersed and highly co-located, leading to rather few grid cells with consequences and few locations where the systems are simultaneously affected in a non-obvious way. This would probably be different if the analysis would address the vulnerability of interdependent technical infrastructures in a city.

Although it may be theoretically possible to model interdependent infrastructure systems of basically any size, substantial practical difficulties exist regarding system mapping and modelling. When it comes to mapping the systems, problems related to data availability may arise, since the infrastructures are usually owned and operated by different owners and usually in a highly competitive market. In order to get access to the relevant data, a broad consent among stakeholders is definitely needed, but not always as easy to achieve. Another problem is the sheer sizes, with respect to the number of components, of many infrastructure systems and that the number of dependencies may be vast. Abstractions and simplifications are thus necessary both in order for the mapping and the modelling to be viable. The goal must be to derive a model that is sufficiently accurate, i.e. that captures enough of the functional characteristics of the systems. The issue of making trade-offs between fidelity and sophistication on the one hand and abstractions and simplifications on the other hand is to a large extent still an open question in the research field [21].

The next step of this research is to perform a large-scale analysis of multiple infrastructures, using actual data as input. Collaboration has been initiated with the Swedish Rail Administration, owner of a system with multiple interdependent infrastructures, thus avoiding some of the above stated issues.

7 Conclusions

In the present paper, an approach for modelling interdependent infrastructures systems has been presented. It is argued that the model enables studying the impact of interdependencies in technical infrastructures in a predictive manner. It is further argued that the modelling approach is useful for analyzing the vulnerability of system of systems, as illustrated in the example. The model requires that the systems are possible to describe in terms of a network model and a functional model, which is possible for most, if not all, technical infrastructures. The network models provide a common interface between the different infrastructure systems. The functional models are used to evaluate a system's performance, given information about its structure and its dependencies of other infrastructures. It is concluded that the scalability and flexibility of the modelling approach renders it suitable for vulnerability analysis of large-scale interdependent technical infrastructures.

Acknowledgments

This research has been financed by the Swedish Emergency Management Agency, which is greatly acknowledged. The authors also express their gratitude to Associate Professor Olof Samuelsson and Senior Lecturer Henrik Tehler for their valuable comments regarding the earlier conference version of this paper.

References

[1] de Bruijne M, van Eeten M. Systems that Should Have Failed: Critical Infrastructure Protection in an Institutionally Fragmented Environment. Journal of Contingencies and Crises Management 2007; 15(1): 18-29.

[2] Buckle P, Mars G. New approaches to assessing vulnerability and resilience. Australian Journal of Emergency Management 2000; 15(2): 8-14.

[3] Boin A, McConnell A. Preparing for Critical Infrastructure Breakdowns: The Limits of Crisis Management and the Need for Resilience. Journal of Contingencies and Crises Management 2007; 15(1): 51-9.

[4] Aven, T. Foundations for Risk Analysis: A Knowledge and Decision-Oriented Perspective. London: Chapman & Hall Ltd. 2003.

[5] Zimmerman R. Social Implications of Infrastructure Interactions. Journal of Urban Technology 2001; 8(3): 97-119.

[6] Little RG. Controlling Cascading Failure: Understanding the Vulnerabilities of Interconnected Infrastructure. Journal of Urban Technology 2002; 9(1): 109-123.

[7] U.S.-Canada Power Systems Outage Task Force. Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations. Washington: U.S. Department of Energy. 2004.

[8] Johansson J, Lindahl S, Samuelsson O, Ottosson H. The Storm Gudrun a Seven-Weeks Power Outage in Sweden. Presented at CRIS2006. Alexandria, 2006.

[9] Leavitt WM, Kiefer JJ. Infrastructure Interdependency and the Creation of a Normal Disaster. Public Works Management & Policy 2006; 10(4): 306-314.

[10] Little RG. A socio-technical systems approach to understanding and enhancing the reliability of interdependent infrastructure systems. International Journal of Emergency Management 2004; 2(1-2): 98-110.

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

[12] Haimes YY, Jiang P. Leontief-Based Model of Risk in Complex Interconnected Infrastructures. Journal of Infrastructure Systems 2001; 7(1): 1-12.

[13] Min HJ, Beyler W, Brown T, Son YJ, Jones AT. Towards modeling and simulation of critical national infrastructure interdependencies. IIE Transactions 2007; 39: 57-71.

[14] Brown T, Beyler W, Barton D. Assessing Infrastructure Interdependencies: the challenge of risk analysis for complex adaptive systems. International Journal of Critical Infrastructures 2004; 1(1): 108-117.

[15] Apostolakis GE, Lemon D. A Screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities Due to Terrorism. Risk Analysis 2005; 25(2): 361-376.

[16] McDaniels T, Chang S, Peterson K, Mikawoz J, Reed D. Empirical Framework for Characterizing Infrastructure Failure Interdependencies. Journal of Infrastructure Systems 2007; 13(3): 175-184.

[17] Chang SE, McDaniels TL, Mikawoz J, Peterson K. Infrastructure failure interdependencies in extreme events: power outage consequences in the 1998 Ice Storm. Natural Hazards 2007; 41: 337-358.

[18] Zimmerman R, Restrepo CE. The next step: quantifying infrastructure interdependencies to improve security. International Journal of Critical Infrastructures 2006; 2(2-3): 215-230.

[19] Restrepo CE, Simonoff JS, Zimmerman R. Uraveling Geographic Interdependencies in Electric Power Infrastructure. Proceedings of the 39th Hawaii International Conference on Systems Sciences, Hawaii, USA. 2006.

[20] Rinaldi SM. Modeling and Simulating Critical Infrastructure and Their Interdependencies. Proceedings of the 37th Hawaii Conference on Systems Science, Hawaii, USA. 2004.

[21] Eusgeld I, Kröger W, Sansavini G, Schläpfer M, Zio E. The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures. Reliability Engineering & System Safety 2009; 94:954-963.
[22] Murray AT, Matisziw TC, Grubesic TH. A Methodological Overview of Network Vulnerability Analysis, Growth and Change 2008; 39(4): 573-592.
[23] Johansson J, Jönsson H, Johansson H. Analysing the Vulnerability of Electric Distribution Systems: a Step Towards Incorporating the Societal Consequences of Disruptions. International Journal of Emergency Management 2007; 4(1): 4-17.
[24] Jönsson H, Johansson J, Johansson H. Identifying Critical Components in Technical Infrastructure Networks. Journal of Risk and Reliability 2008; 222(2): 235-243.
[25] Newman ME. The structure and function of complex networks. SIAM Review 2003; 45(2): 167-256.
[26] Haimes YY. On the Definition of Vulnerabilities in Measuring Risks to Infrastructures. Risk Analysis 2006; 26(2): 293-6.
[27] Haimes YY. Risk Modeling, Assessment, and Management. New York: John Wiley & Sons; 1998.
[28] Kaplan S, Garrick BJ. On the Quantitative Definition of Risk. Risk Analysis 1981; 1(1): 11-27.
[29] Kaplan S, Haimes YY, Garrick BJ. Fitting hierarchial holographic modeling into the theory of scenario structuring and a resulting refinement to the quantitative definition of risk. Risk Analysis 2001; 21(5): 807-819.
[30] Dilley M, Boudreau TE. Coming to terms with vulnerability: a critique of the food security definition. Food Policy 2001; 26:229-247.
[31] Salter J. Risk Management in a Disaster Management Context. Journal of Contingencies and Crises Management 1997; 5(1): 60-5.
[32] Aven T. A unified framework for risk and vulnerability analysis covering both safety and security. Reliability Engineering & System Safety 2007; 92(6): 745-754.
[33] Einarsson S, Raussand M. An Approach to Vulnerability Analysis of Complex Industrial Systems. Risk Analysis 1998; 18(5): 535-546.
[34] Patterson SA and Apostolakis GE. Identification of critical locations across multiple infrastructures for terrorist actions. Reliability Engineering and System Safety 2007; 92: 1183-1203.
[35] Jenelius E, Mattsson L-G. The vulnerability of road networks under area-covering disruptions. Proceedings of INFORMS Annual Meeting. Washington D.C. 2008.
[36] Rinaldi SM, Peerenboom JP, Kelley TK. Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies. IEEE Control Systems Magazine 2001; 21(6): 11-25.
[37] Albert R, Barabási A-L. Statistical Mechanics of Complex Networks. Review of Modern Physics 2002; 74(1): 47-97.
[38] Holme P, Kim BJ, Yoon CH, Han SK. Attack vulnerability of complex networks. Physical Review E 2002; 65(056109).
[39] Albert R, Jeong H, Barabási A-L. Error and attack tolerance of complex systems. Nature 2000; 406(6794): 378-382.
[40] Wilhelmsson A., Johansson J. Assessing Response System Capabilities of Socio-Technical Systems. Proceeding from TIEMS 2009. Istanbul, Turkey. June 9-11.

IV

Towards a System-Oriented Framework for Analysing and Evaluating Emergency Response

Marcus Abrahamsson, Henrik Hassel, and Henrik Tehler

Department of Fire Safety Engineering and Systems Safety, Lund University, PO Box 118, SE-221 00 Lund, Sweden. E-mail: marcus.abrahamsson@brand.lth.se

Information can be provided by studying and evaluating past emergencies and the response in connection to them. This information would then be useful in efforts directed at preventing, mitigating and/or preparing for future emergencies. However, the analysis and evaluation of emergency response operations is not an easy task, especially when the operation involves several cooperating actors (e.g. the fire and rescue services, the police, the emergency medical services, etc.). Here, we identify and discuss four aspects of this challenge: (1) issues related to the values governing the evaluation, (2) issues related to the complexity of the systems involved, (3) issues related to the validity of the information on which the analysis and evaluation is based and (4) issues related to the limiting conditions under which the emergency response system operated. An outline of a framework for such an analysis and evaluation, influenced by systems theory, accident investigation theories and programme evaluation theories dealing with the above aspects, is introduced, discussed and exemplified using empirical results from a case study. We conclude that the proposed framework may provide a better understanding of how an emergency response system functioned during a specific operation, and help to identify the potential events and/or circumstances that could significantly affect the performance of the emergency response system, either negatively or positively. The insights gained from using the framework may allow the actors involved in the response operation to gain a better understanding of how the emergency response system functioned as a whole, as well as how the actors performed as individual components of the system. Furthermore, the information can also be useful for actors preparing for future emergencies.

1. Introduction

When a part of society, e.g. a community, is affected by an emergency, a system made up of various actors and resources, for example, official agencies such as the fire and rescue services, the police and the emergency medical services, as well as actors from the private sector and non-profit organizations, becomes involved in response to the event. Such a system of actors and resources, here called an *emergency response system* (Uhr, Johansson, & Fredholm, 2008), can be regarded as a *complex socio-technical system* (Ropohl, 1999; Comfort & Kapucu, 2006). A socio-technical system involves elements of both a social (individuals, actors, groups, organizations, etc.) and a technical nature, i.e. artefacts of different kinds (it may also involve natural objects). Although there is no generally accepted definition of complexity, a system is often considered complex if it contains a large number of components that interact in many different ways (Simon, 1996; Axelrod & Cohen, 2000). In the present context, the behaviour of an emergency

response system is, to a large extent, affected by its social elements, and the interactions between such elements are usually intense. As a consequence of this, it is often difficult to predict how such a system will behave and, for the same reason, it may also be difficult to determine how it behaved in an actual response operation and to understand the reasons for its behaviour. Finding answers to questions such as: "How did the system perform during the emergency response operation?" and "What could have significantly affected the performance of the system?" is not an easy task. This issue is dealt with in the present paper.

In the next section, the challenges encountered in analysing and evaluating the performance of an emergency response system are discussed in relation to four aspects: (1) issues related to the values governing the evaluation, (2) issues related to the complexity of the systems involved, (3) issues related to the validity of the information on which the analysis and evaluation is based and (4) issues related to limiting conditions under which the emergency response system operated during the response. Based on this discussion, an outline of a framework for the analysis and evaluation of the performance of emergency response systems is introduced and exemplified in Section 3[1].

2. Challenges in the analysis and evaluation of emergency response systems

At least four challenging aspects are related to analysing and evaluating the performance of an emergency response system. *Firstly*, such an evaluation will, to some extent, be based on value judgements, i.e. implicit or explicit accounts of what we care about (Keeney, 1992). Value judgements will guide the focal point of the evaluation process, as well as the conclusions drawn based on the observations, for instance in terms of recommendations for future improvements. Value judgements are highly related to the question of how successful a specific response operation is considered to be. Without values with which to assess the operation, one cannot know whether it was successful or not. One way of approaching this issue when analysing and evaluating emergency response is to find and describe a common overarching set of values, expressed, for instance, as objectives of the emergency response system at a fairly high level of abstraction, which can be used to guide the evaluation. In practice, such objectives may differ between specific response operations. However, they are predominantly related to meeting the needs that arise over time and space in the population affected by the emergency in question. From a systems perspective, and with reference to Rasmussen's discussion on abstraction hierarchies (Rasmussen, 1985), it is possible to relate the high-level objectives at the system level to the objectives of the respective actors and their actions during the emergency. For instance, at the emergency response system level one, objective might be to protect the lives and health of those affected, which may, for example, be manifested at the actor level by actions to provide shelter during a severe storm: see Figure 1. By explicitly stating the objectives (which reflect the underlying values) of the various actions taken during the emergency response, and the way in which they are related to the overarching objectives of the emergency response system, the evaluation can be directed towards establishing the extent to which the high-level objectives were met.

Secondly, the complexity of emergency response systems and of the context in which they operate affect the way in which they can be analysed, understood and evaluated. In order to understand not only what happened during the emergency but also *why* the system behaved as it did and the outcome was what it was, an effort must be made to understand the relationships and dependencies between the actors involved, as well as the context in which they were operating. The issue of complexity is by no means new or exclusive to the study of emergency response systems; there is an abundance of literature in various fields dealing with such matters. Nevertheless, we would like to briefly discuss two areas from which we have benefited when working towards a framework for the analysis and evaluation of the performance of emergency response systems in emergency and crisis situations. Firstly, an analogy can be drawn with the field of accident investigation, in which several researchers have highlighted a number of recent changes in society, such as the increasing complexity and coupling of systems, the rapid pace of technological change, etc., that challenge traditional accident investigation techniques and underlying accident models (Rasmussen & Svedung, 2000; Leveson, 2004). A common idea in this research area is that 'a single factor is seldom the only

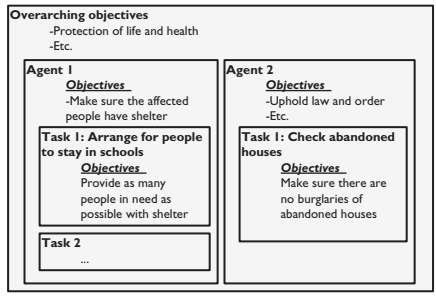


Figure 1. Illustration of different tasks and objectives in an emergency response system.

"cause" of an accident; it is more common that the "cause" stems from a complex set of factors and their interactions' (Jönsson, 2007, p. 48). Regarding accidents in this way has led to the development of accident models based on systems thinking (see, for instance, Rasmussen, 1997; Hollnagel, 2004; and Leveson, 2004). The central issue, which is similar to that in the present context, is that it is not sufficient to try to identify what might have caused an accident by considering the individual parts of the system in isolation, for instance by attempting to find the 'guilty individuals' (Catino, 2008). Human error has traditionally been seen as a common factor to blame in accident investigations. However, Reason (2000) argues that in a 'system approach', rather than a 'person approach', human error should be seen as the consequence of 'upstream systemic factors', rather than as the cause itself. Similar ideas have also been proposed by Dekker (2004) and Woods and Cook (2002). Despite the important difference between accident analysis and the evaluation of emergency response operations (i.e. accident analysis focuses primarily on what led to the accident, while we are primarily interested in the management of the situation *given* that an accident has already taken place, or some other kind of extreme event has affected society), we are of the opinion that similar models, which are suitable to deal with the complexity of the event and the systems involved, are required. A more detailed discussion of the relation between accident investigation and the evaluation of emergency response operations has been provided by Abrahamsson, Jönsson, and Johansson (2008).

Another field from which we can gain an insight when attempting to analyse and evaluate system performance in complex settings is that of evaluation and programme theory, sometimes referred to as the logical framework approach, e.g. (McLaughlin & Jordan, 1999; Davies, 2004, 2005; Rogers, 2008). The logical framework approach has been used extensively to guide evaluations in various (often complex) settings. In summary, this approach involves generating a plausible model of how a programme will work in a specific context to reach its goals. The elements or stages in such a logical model generally include *resources/inputs*, *activities, outputs* and *goals*, and a description of the context in which the programme will work (although there is some variation among the different approaches: see, for instance, Davies, 2004). For an extensive description of the approach and examples of its use, see for instance McLaughlin and Jordan (1999), Gasper (2000) and Rogers (2008). According to McLaughlin and Jordan (1999), some of the benefits of using such models are that:

- they facilitate a common understanding of the programme and expectations regarding resources, customers reached and results, and are thus helpful in sharing ideas, identifying assumptions, etc., and
- they are helpful for programme design or improvement in that it is possible to identify the critical elements required to achieve the goals, redundant elements and inconsistencies, etc.

Although programme theory usually has a forward-looking perspective, in that one is often trying to generate a plausible model of how the programme *will work* in a specific setting, while we are primarily interested in understanding how an emergency response system *has worked* in a specific setting, there is a common need to define the goals (which reflect the underlying values) explicitly (to guide the evaluation) and to obtain an explicit model reflecting the involved actors' perception of how the actions taken were related to those goals. Furthermore, in attempting to improve emergency response systems to be able to better deal with future emergencies, one needs to be able to identify the critical elements of the operation. It should be mentioned, however, that some criticism has been directed towards the logical framework approach, or rather the way in which it has been used in some cases (see, for instance, Gasper, 2000). The main criticism has been directed towards the use of fairly simple, linear models to describe the relationships between the inputs, in terms of resources and activities, and the outputs and goals, the argument being that they simply do not reflect the complexity of real life. In recent years, several suggestions for generating models more suitable for handling this situation, i.e. models capable of handling feedback loops, variations in scale, conflicting objectives, etc., have been proposed by, for instance, Davies (2004, 2005) and Rogers (2008).

The *third* challenging aspect is associated with the validity of the information upon which the analysis and evaluation is based. In most instances, the main source of information regarding the course of events during an emergency situation is interviews with the people who were actually involved in the operation. This may be problematic from at least two perspectives. Firstly, a number of biases of human memory and judgement have been identified, suggesting that people make unreliable witnesses (Heath, 1998). Perhaps the most prominent kind in this setting is hindsight biases (Fischhoff, 1975), suggesting that given historic information on an event, people tend to revise their perception of the event. For a discussion on ways of addressing the possible effects of hindsight biases in an evaluation, see Heath (1998). For a more general discussion on methodological issues related to disaster research, including those of timing, access and generalizability, see for instance Stallings (2006) and Tierney (2002). Secondly, people may be more or less reluctant to

provide a full account of their perception of the events, especially when they feel threatened by criticism or vulnerable to blame assignment (Heath, 1998). According to Heath, there are two types of evaluation:

- the search for correction in terms of reducing the incidence of crises or of impacts of those crises and
- the search for assignment of guilt (an extreme case of which is scapegoating) and criminal proceedings by which we can make judgement upon the guilty parties.

He further argues that 'Given that both types of evaluation commence along the same or parallel path of seeking to identify the cause of the crisis and how the response of the crisis was handled, it is not too surprising that the missions of cause-and-consequence and guilt blur together', and consequently one must make it clear that 'judgements made about guilt will be done by some other group of people and some other process and not by the evaluation process set up to improve crisis management' (Heath, 1998). Similarly, Catino (2008) uses an overview of the literature concerning the tension between 'individual blame' and 'organizational function logics' in accident analysis, to build an argument in favour of the 'organizational function logics' as the basis for such an analysis when the objective is to understand the dynamics of an accident. Among the requirements for success in such an effort are the adoption of a 'no-blame safety culture' and the use of models for organizational analysis suited to the complexity of the event (Catino, 2008).

Fourthly, when discussing the performance of an emergency response system in an emergency situation, attention should be directed to the limiting conditions under which the system operated in that specific situation. For instance, could some of the negative consequences simply not be avoided in the response phase? For example, if the event itself, say an explosion of some sort, caused several *immediate* and unavoidable casualties this should not affect the evaluation of the performance of the emergency response system during post-impact management. Clearly, these casualties could not have been avoided by carrying out the emergency response operation in any other way. On the other hand, if the explosion wounded several people who might have received help faster, then the constraints on the emergency response system might not have made it impossible to get help to them faster, thus saving more lives. It is important to note that the point of departure for the evaluation is the response operation given the circumstances at the time of the emergency. Therefore, one must differentiate between the analysis and the evaluation of the actual performance and that of what might have happened if the circumstances had been different, e.g. if an actor had had greater resources.

In summary, when working towards a framework for analysing and evaluating emergency response operations, where the objective is to facilitate the understanding of the performance of the emergency response system during an emergency or a crisis situation, a number of important issues must be addressed. These are numbered 1–4 below:

(1) There is a need to be explicit concerning the underlying values and objectives when evaluating emergency response operations. Without values on which to assess the system performance, there is no way of determining whether the response operation was successful or not.
(2) It is advantageous, or may even be necessary, to adopt a systems perspective, considering the emergency response system as a whole, and to use models capable of dealing with the level of complexity involved and that facilitate a common understanding of the situation being evaluated.
(3) There is a need for careful design of the interview situation in the data acquisition phase of an analysis and evaluation, to clearly articulate the purpose of the analysis and evaluation to those contributing to the process, and to explicitly address the effects of hindsight and other biases.
(4) There is a need to explicitly try to make the limiting conditions under which the emergency response system operated visible when analysing and evaluating its performance. Were there other ways of affecting the objectives of the system in a positive way that were not exploited, or were the actions taken the only ones or the best possible?

In the following section, the general outline of what we consider a first step towards a framework for analysing and evaluating emergency response operations influenced by the challenges outlined above is presented, discussed and exemplified using a case study. References to the four issues above are given in the text to clarify which one of them is addressed by the part of the framework being discussed.

3. An outline of a framework for analysing and evaluating emergency response operations

On the most general level, the suggested framework consists of three main parts; see Figure 2. The first involves defining the conditions for the evaluation in terms of describing the events that led to the initiation of the response, the preconditions under which the emergency response system operated and establishing the objectives of the emergency response operation at the highest system level, i.e. for the total emergency response system. This part is directly related to issue

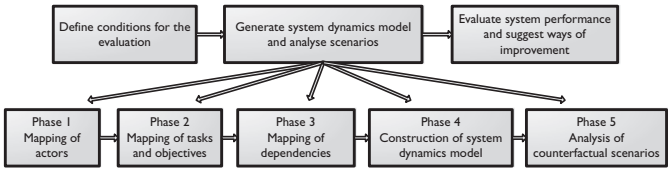


Figure 2. The different phases of the framework.

numbers 1 and 4 above. The second part, which is the main focus of the present paper, concerns constructing and analysing a model of the response system during the emergency. The different phases of this part are further discussed in Section 3.1. The third part is related to the actual evaluation, based on the analysis in the second part, in terms of whether the performance of the emergency response system during the emergency was acceptable and how it could be improved.

Before entering into a more detailed discussion of the construction and analysis of a model of the emergency response system, some brief remarks should be made regarding the first and the third parts of the framework. As discussed in Section 2, in order to establish a foundation for the evaluation in terms of whether the system performance was acceptable or not, there is a need to explicitly state the objectives of the whole emergency response operation. In this paper, we will not elaborate further on how this can be done in practice, as much has been published on this topic elsewhere, and we refer the reader to Keeney's standard textbook (Keeney, 1992). Establishing the values governing the analysis and evaluation in this way addresses issue number 1 above. In the following section, we will focus on the analysis part of the framework, where the objective is to generate an understanding of how the emergency response system performed and why the outcome was what it was. We would like to emphasize that we consider analysis and evaluation to be two separate processes; evaluation, as described above, being intrinsically subjective, while in the analysis phase, one should strive towards objectivity in the sense that the aim is to describe what actually happened during the emergency without making judgements as to whether the performance was acceptable or not.

3.1. Constructing and analysing a system dynamics model

The most central part of the suggested framework, or at least the part given the most attention in this paper, is a procedure for generating a model of the emergency response system and the environment in which it was operating and, based on that model, a procedure for the systematic analysis of counterfactual scenarios, i.e. scenarios that did not occur but could have, had any of the system elements or environmental variables been in other states. A full account of the challenges related to modelling complex socio-technical systems such as an emergency response system is beyond the scope of the present paper (for a discussion on approaches to understanding, modelling and analysing complex systems, see Jönsson, 2007, pp. 39–48), but some general points will be made. It is important to realize that there is generally more than one adequate way to represent a realworld system (Ashby, 1957; Haimes, 1998; Ropohl, 1999), and that the system definition and description will always be dependent on the purpose of the modelling and the person/persons conducting it. There may be many ways to describe a system, but in essence, it consists of defining the *elements* of the system, the *relations* between those elements and the *boundaries* of the system, i.e. distinguishing between what is part of the system and what is part of the system's *environment*. In Figure 3, a schematic illustration of how the system is modelled in this approach is given. The small circles represent system elements, which, in our case, can be categorized as *actors, resources* and *technical infrastructures*. The elements inside the dotted box are those making up the emergency response system, i.e. the system to be evaluated. The total system model (delineated by the larger box) may also contain elements that are not part of the emergency response system,

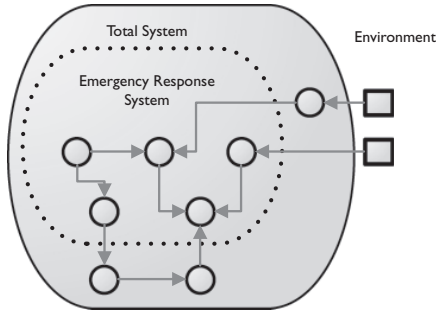


Figure 3. A general system model.

which one wants to study in terms of relationships, e.g. interdependent technical infrastructures such as the electrical power grid and the telecommunications system. The small squares outside the system represent variables in the system's environment that can influence the system, but that are not of interest in modelling interdependencies, for instance, the weather conditions during the event.

The main source of information regarding the elements and relations in the model, besides documentation pertaining to the event, is interviews, performed both individually and in the form of workshops, with the actors who participated in the response operation. The construction of a model as described above serves at least two purposes. Firstly, it provides an explicit representation of how the actors involved perceived the situation. In some sense, the objective is to generate a common ground based on the different actors' points of view and on the documentation related to the event in question, which is directly related to issue number 2 above. These sources of information are successively used to cross-validate the information obtained. Although it does not fully solve the problem, this cross-validation serves as one way of dealing with the various biases related to peoples' memory and perception of what actually happened during an emergency situation, thus addressing issue number 3. Such a procedure is commonly referred to as triangulation and is seen as the best approximation to inferring causal relationships in studies of disaster situations (Stallings, 2006, p. 64). Secondly, the model serves as an input for a systematic analysis of how variations in any of the elements might affect the system's performance, which is further discussed in Section 3.1.5.

The main steps of the procedure used to map out and analyse the elements and relationships that constitute the model of the emergency response system, and the context in which it operated, are presented in the lower part of Figure 2, and are further discussed in the subsequent sections. It should be noted that during an actual analysis, the process will probably not be as linear as indicated in Figure 2. On the contrary, switching back and forth between the different phases is expected and probably advantageous. To test the suggested framework in practice, it was used in a pilot case study involving the analysis of the response operation in a local municipality following a severe storm called *Per*, which struck the southern part of Sweden on 14 January 2007. The storm resulted in long-term power outages, loss of telecommunications in large areas and reduced availability of the road and railroad networks. To illustrate the different phases, some examples from the study of the performance of the emergency response system during *Per* will be presented, together with the introduction of the various phases below.

3.1.1. Phase 1: Mapping of actors

The first phase consists of identifying the actors who were involved in the emergency response operation. The actors involved constitute the first category of elements in the model representation of the emergency response system. The main techniques used in this phase of the case study were document studies (incident reports, media coverage, etc.) and interviews with representatives of various actors using a snowballing process as described, for instance, by Wasserman and Faust (1999) and Uhr and Johansson (2007), which resulted in a list of all the actors active during at least some part of the emergency response operation. Such a snowballing process is often more appropriate for many types of disaster research than traditional probability sampling techniques (Stallings, 2006, p. 63). It is useful to categorize actors, for instance in terms of official agency actors, private trade and industry actors and organized voluntary actors, or in terms of planned structures of actors vs. 'emergent' groups of actors (Drabek & McEntire, 2003). It is also important in this phase to define a suitable level of detail when describing actors, and this is dependent on the purpose of the analysis. For example, in the case study the appropriate level of detail of describing actors was chosen to correspond to the organizational level, for instance *Fire and Rescue Services*, *Police* and *Social Services Department*, because the main objective of this particular study was to analyse the emergency response system as a whole, focusing on the interactions between various organizations.

3.1.2. Phase 2: Mapping of tasks and objectives

In this phase, the objective is to identify the *tasks* performed during the emergency response operation, and the objectives of performing these tasks, for each of the actors in the emergency response system. Again, this is done based on interviews with the actors involved in the response operation. As with the mapping of actors discussed above, one major challenge in this phase is to define and identify tasks at a suitable level of detail. For example, one of the tasks identified by the actor *Fire and Rescue Services* was *Distribute portable power generators and Liquefied Petroleum Gas (LPG) heaters*, which could be further broken down into, for instance, *Distribute portable power generators* and *Distribute portable LPG heaters*, which in turn could be broken down into *Make sure portable power generators/LPG heaters are functional*, *Prioritize those in need of portable power generators/LPG heaters*, etc. Again, the appropriate level of detail in the description of the tasks is dependent on the purpose of the analysis. A parallel can be drawn with Rasmussen's discussion on abstraction hierarchies (Rasmussen, 1985), which implies analysis at three levels – *objective*, *function* and *form* – used to provide an understanding of a system. Objective

refers to *why* the system exists, i.e. what it is for. Function refers to *what* the system must do to attain its objectives and form refers to *how* the system fulfils the functions at a concrete level. In the case of analysing an emergency response system *tasks* correspond to *functions* and *forms* in Rasmussen's terminology. The level of describing tasks in the model of the emergency response system will often correspond to the function level, i.e. a description of *what* was done, where necessary with underlying information on *how* this was done, corresponding to the form level.

As mentioned in the previous paragraph, an effort should be made to identify and describe the objectives of the identified tasks, in this setting often expressed in terms of the needs they were aimed at meeting, which is related to issue number 1 above. One commonly used distinction between different kinds of needs (or demands), i.e. *agent-generated needs* and *response-generated needs*, can be found for instance in the publications by Dynes, Quarantelli, and Kreps (1981) and Quarantelli (1997). In short, agent-generated needs can be said to stem from the specific disaster agent, for instance a flood generating a need for sandbags to provide protection against rising water, while response-generated needs are common to most emergencies as they originate from the response efforts themselves, for instance, the need for effective mobilization of personnel and resources (Quarantelli, 1997). In the end, one could argue that meeting the response-generated needs is simply the means to an end, to adequately meet the needs of the affected community, i.e. the agent-generated needs[2]. Abrahamsson et al. categorized agent-generated assistance needs in the affected community in terms of, for instance, *Protection of life and health, Psychosocial needs* and *Life and function support*, which could be used as input for overarching objectives to guide the evaluation, i.e. objectives at the emergency response system level (Abrahamsson, Johansson, Fredholm, Eriksson, & Jacobsson, 2007). For example, the task *Distribute portable power generators and LPG heaters* performed by the *Fire and Rescue Services* was aimed at meeting the needs of people who were affected by the power outage and had no other means of heating their houses, i.e. agent-generated needs, which could be further categorized as *Life and function support* and, in some cases, *Protection of life and health*, that is, objectives of the total emergency response system at the highest level of abstraction.

Furthermore, for each task, one should strive to construct *performance measures* (Axelrod & Cohen, 2000; Jönsson, Abrahamsson, & Johansson, 2007), i.e. measures that provide information about how well the task was/can be performed. Performance measures may vary between different tasks, but important dimensions often include effectiveness (associated with the extent to which the performance of the task actually satisfies the need) and efficiency (whether or not the task can be performed with reasonable resources). For example, in the pilot study, two of the performance measures specified for the task *Maintain 24 hr telephone service*[3] were *Availability*, measured in terms of the percentage of the time this service was available to the public, and *Situational knowledge*, dealing with the quality of information that could be delivered. The mapping of tasks, objectives and performance measures is closely related to issue numbers 1 and 2 above, i.e. establishing the values governing the actions of the various actors and generating a common understanding on which actors participated in the response and what they did during it.

3.1.3. Phase 3: Mapping of dependencies

In gaining a deeper understanding of how the emergency response system functioned during the response and finding the underlying reasons *why* the response system performed as it did and the outcome was what it was, an effort should be made to identify the circumstances that affected the actors' ability to perform their tasks during the response. Therefore, the third phase involves mapping what and whom the respective actors were dependent upon to be able to perform their own tasks, i.e. *resources*, *technical infrastructures* and *other actors performing specific tasks*. Furthermore, variables in the *environment* that seriously affected, or could have affected, any system elements, for instance the actors' ability to perform their tasks, are also mapped out. In a similar manner, an account should be given of how the various tasks affected the actors' surroundings, for instance in terms of other actors' ability to perform their tasks[4], or in terms of impact on the need for assistance in the affected community. This is closely related to the discussion above on the kinds of needs specific tasks are aimed at meeting and to issue number 2 above.

In addition, for each of the identified relationships, the *direction* as well as a measure of the *strength* of the dependence should be specified. For instance, if an increase in the availability of a certain resource leads to an increased ability to perform a certain task, the relationship between the resource and the task has a positive direction. The strength of the relationship indicates how seriously the ability to perform a certain task is affected by the unavailability of a certain resource. Four levels of strength were used in the present study, ranging from a "marginal effect", meaning that unavailability of the specific resource will reduce the performance measures for that task by less than a third, to a "very serious effect", meaning that the task cannot be performed if the resource becomes unavailable. In Table 1, relationships for the task *Distribute portable power generators and LPG heaters*, performed by the actor *Fire and Rescue Services* are shown as an example.

Table 1. Relationships for the Task Distribute Portable Power Generators and LPG Heaters

Element	Type	Direction	Strength
Fire and rescue services – personnel	Resource	+	Very serious effect
Fire and rescue services – portable power generators and LPG heaters	Resource	+	Serious effect
Regional coordination centre – provide portable power generators and LPG heaters	Task	+	Serious effect
OPTIMERA – supply LPG containers	Task	+	Very serious effect
Passable roads	Technical infrastructure	+	Very serious effect

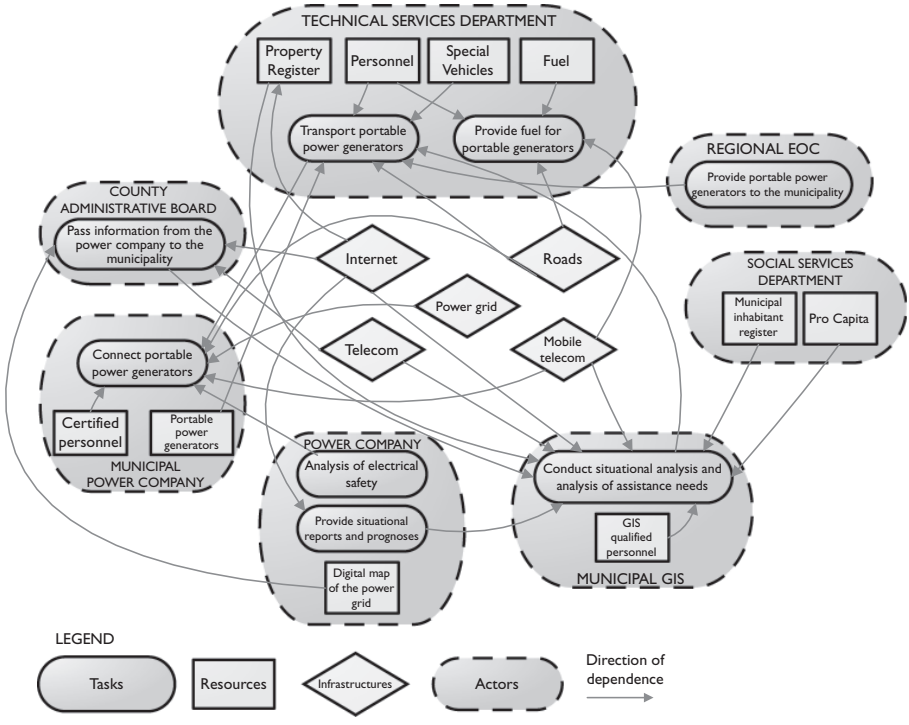


Figure 4. Example of a graphical representation of a system dynamics model, showing the actors involved in the island operation of the electrical power grid after the storm *Per*.

For instance, to be able to perform the task, the *resource* personnel is needed; an increasing availability of personnel leads to an increased ability to perform the task. Furthermore, should no personnel be available for the task, this would have a very serious effect on the ability to perform it: in fact, it would not be possible at all.

3.1.4. Phase 4: Construction of the system dynamics model
Based on the data gathered in the previous phases, a *system dynamics*[5] *model* can be constructed in order to facilitate the understanding of relationships within the emergency response system and between the system and its environment, and thus the function of the system as a whole. In Figure 4, the actors involved in an effort to implement and maintain so-called *island operation* of parts of the damaged electrical power grid in the aftermath of the storm *Per* are used as an example. Island operation involves the use of portable power generators to provide electrical power to parts of the electrical distribution network that are still functional as a temporary solution while the ordinary system is being repaired. In this model, the various actors involved in the island operation, the tasks they

performed and what they were dependent on in terms of resources, infrastructure and other actors in order to carry out those tasks are depicted. For instance, in order to perform the task *Transport portable power generators to the connection point*, the *Technical Services Department* were dependent on *special vehicles* to carry the power generators, *personnel* to do the work, access to *power generators* provided by other actors, *information on where to transport* them from the actor *Municipal GIS* and *passable roads*.

It should be stressed that the model contains more information than that graphically illustrated. With reference to the logic of design, discussed in Section 3.1.2 above, what is depicted in Figure 4 corresponds to the *functions* that the different actors carried out in relation to implementing and maintaining island operation, i.e. *what* they did. Underlying information on the *objective* of each task as well as of the island operation as a whole and, where necessary, more detailed information on the *form*, i.e. *how* they were performed, is gathered in the interviews and used in the evaluation.

The results gathered using the model can then be used as input for discussions on the system performance in the actual scenario, as well as in the analysis of counterfactual scenarios, further described in Section 3.1.5 below. One important aspect that may be analysed using the information is to what extent the response operation followed established plans and procedures. It is important to note that this should not be done with the aim of identifying "erroneous" deviations from the plans because improvization and ad-hoc behaviour are very important for the response system's ability to adapt to new circumstances (Webb & Chevreau, 2006). Therefore, it might be more useful to use it to see whether existing plans and procedures should be changed to facilitate the functioning of the response system.

3.1.5. Phase 5: Analysis of counterfactual scenarios

The purpose of this phase is to broaden the scope of the conclusions that can be drawn from an analysis. In order to achieve this, the system dynamics model is used to systematically analyse all or a chosen set of system elements in terms of what the impact would be on a certain task and/or the system as a whole if the element had been in another state. For instance, what would the effects of a total loss of telecommunications be, in terms of decreasing the capability of various actors to perform their tasks? Furthermore, what effect would this have on the ability of the emergency response system to achieve its objectives? One of the aims of using the system dynamics model as a starting point in such discussions among the participating actors is to allow a more comprehensive and systematic analysis, e.g. in terms of finding relationships, than would be attainable in a less structured "brainstorming" session. It should be noted that the structure of the system dynamics model is by no means fixed during this phase. For instance, variations in the context may call for "new" tasks, perhaps to be performed by "new" actors.

To exemplify this, let us consider one of the elements of the model illustrating island operation in Figure 4. What, for instance, would be the impact on the system involved in that activity if the task *Provide situational reports and prognoses* regarding the state of the electrical power grid performed by the power company, for some reason, was not accomplished? This would mean that the actor *Municipal GIS* would be less effective and efficient in performing its task *Conduct situational analysis* . . . with the objective of identifying the best places to connect portable power generators, taking into account the number of people who could be supplied with electrical power, people with special needs, the state of the damaged power grid, etc. In fact, it was deemed that it may not be possible to perform this task at all without the reports and prognoses of the power company. This in turn would affect the objective of the island operation activity as a whole, i.e. to provide temporary electrical power to as many inhabitants as possible, as quickly as possible, taking into account people with special needs. The goal of the island operation activity is also related to the objectives *Protection of life and health* and *Life and function support* at the emergency response system level. This gives rise to at least two questions: how likely is it that this would actually happen (i.e. the task *Provide situational reports and prognoses* not being performed), and if so, were there alternative ways for the actor *Municipal GIS* to obtain information on the state of the damaged power grid? Discussing issues such as these in a structured manner based on the systematic analysis of counterfactual scenarios as described above will make it possible to draw more extensive conclusions about the system's ability to function in situations that are similar, but not identical to, the actual. It will also facilitate the understanding of which resources, tasks, etc., are critical in achieving the objectives of a system in a given context.

This phase is closely related to the final step in the framework presented in Figure 2, the evaluation of the emergency response system's performance. To clarify the relation, the actual scenario during the emergency can be regarded as one path through the total system's state space (Kaplan, 1997). The total system might have taken a different path through the state space, depending on the performance of the emergency response system and/or variations in its context. In Figure 5, the solid line represents the actual scenario and the dashed lines represent possible scenarios if other decisions had been made or if the circumstances had been different. Assume, for example, that a resource such as a fire

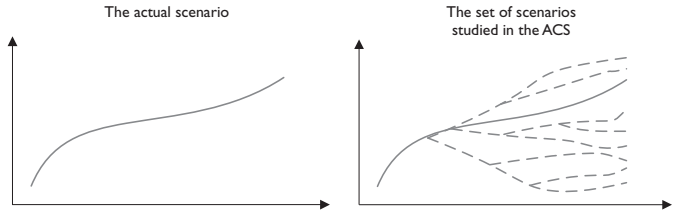


Figure 5. Analysis of counterfactual scenarios, ACS. Each axis represents a specific system variable and a trajectory in the state space (a scenario) represents state changes over time. In the present setting, system variables may include wind speed, temperature, number of households without power supply, availability of emergency telephone service, etc. Because systems are often described using more than two variables, the figures should only be seen as illustrative.

truck that was used during the emergency could have been used differently, reducing the overall severity of the negative consequences of the emergency. We denote the actual scenario A and the alternative scenario B. Let us also assume that the outcome of scenario A was highly undesirable, such as many casualties. When evaluating the performance of the emergency response system, it is very important to keep in mind that although the outcome of the event was very serious, the operation may nevertheless have been performed adequately. The key point here is whether the outcome of the response operation, which reflects the objectives of the emergency response system, would have been significantly better if scenario B (i.e. alternative use of a resource) had taken place rather than scenario A.

4. Discussion

Perhaps the most valuable aspect of the framework presented in this paper is that it provides a structured way of analysing and visualizing how the actions of a certain actor in the emergency response operation are related to the performance of the overall emergency response system, which is of great importance in virtually all kinds of emergency preparedness activities. The results of an analysis performed as described here, together with subsequent evaluation, may serve as input for concrete preparedness efforts related to the design of the emergency response system, for instance, in terms of resource and personnel planning. A similar concept, concerned with the study of hypothetical risk scenarios in risk and vulnerability analyses, is discussed by Abrahamsson et al. (2007).

With reference to the field of accident investigation, this type of analysis, particularly the study of counterfactual scenarios, could be seen as a means of systematically studying how close the system came to some kind of "breakdown", i.e. a severe reduction in the capability to perform the tasks necessary for a successful response in terms of meeting the objectives of the emergency response system in a particular situation. However, it should be stressed that the approach presented in the present paper can, and should, be used not only to investigate what would cause the performance of the emergency response system to be significantly worse but also what would make the performance of the system as a whole more effective and efficient. Being able to "test" the system in a structured way, in terms of the effects if some of the circumstances had been slightly different from the actual ones, will provide important information for forward-looking prevention/mitigation and preparedness efforts. This is something that is not taken into explicit consideration in most available techniques for accident investigation and emergency management evaluation. The analysis of counterfactual scenarios may also serve as a way of reducing the tendency to prepare for the previous crisis, one of the difficulties related to planning and preparing for crises described for instance by McConnell and Drennan (2006).

In the present paper, the applicability of the suggested framework has been demonstrated by brief empirical examples. However, in order to provide empirical validation of the suggested framework, it needs to be applied in more extensive case studies. This will be an important task for future work. More specifically, the plan is to use the framework in a variety of settings, such as emergencies of different types and different scales, in order to identify the strengths and limitations of the framework for further development.

Another major task for future work is to further explore the possibilities of using this approach to modelling and analysis in a forward-looking setting, i.e. while performing risk and vulnerability analyses based on potential future scenarios.

5. Conclusions

In conclusion, the main contribution of the present paper is that it suggests a framework for analysing and evaluating complex multi-actor emergency response

operations. We identify several challenges related to such an endeavour and the framework is specifically designed to address those challenges. As a consequence, the framework has several desirable properties, making it suitable for use in the present context.

First of all, it promotes explicit treatment of values and objectives on which the evaluation of the emergency response operation is based. Secondly, it provides a common ground for the analysis of a specific operation, i.e. it enables various actors to reach an agreement on what they did during the operation, and how they affected each other. Thirdly, as the various actors who participate in analysing the emergency response operation develop the system model of the operation together, the biases that might otherwise have occurred for instance due to people having distorted memories of the event will be reduced. Furthermore, this joint effort to develop the system model may foster knowledge transfer and learning across organizational borders. Fourthly, dealing explicitly with the constraints of the operation and analysing counterfactual scenarios aids the evaluation of the emergency response system's performance as well as the individual actor's performance. More specifically, the structured analysis of counterfactual scenarios broadens the scope of the conclusions that can be drawn from studying one event, thus enhancing the frameworks' potential to serve as a tool to learn from past emergencies and prepare for future ones.

Notes

This is a substantially revised and extended version of a presentation given at The Ninth International Conference on Probabilistic Safety and Management (PSAM9) in Hong Kong, May 2008. We would like to thank the Swedish Emergency Management Agency for funding the research on which this paper is based. We would also like to thank two anonymous reviewers for their useful comments on earlier versions of the paper.

In performing the case study, a computer program was developed by one of the authors to facilitate the collection of the information. The program, which has a user interface written in Swedish, is available upon request.

1. It should be noted that the framework is not intended to be used for analysis and evaluation during an actual emergency, but rather afterwards as a way of generating knowledge about the performance of the emergency response system.
2. This is not to say that response-generated needs are less important. It may be the case that a task directed, for instance, at assisting another actor in the response system proves to be the most critical for the overall success of the emergency response, in terms of meeting the agent-generated needs in the affected population, even though it was not directly directed at meeting such needs.
3. This task was performed by the *Fire and Rescue Services*, providing one of several ways for people to get in touch with the authorities to obtain information on the situation, and what was being done, etc.
4. This is one way of cross-validating the information obtained in the data acquisition phase, i.e. to check for inconsistencies in the statements regarding what the different actors required in order to perform their tasks. In case of conflicting information, for instance, if actor A states that their performance of a certain task affects actor B's ability to perform another task, and this is not recognized by actor B, a dialogue between the two actors (and perhaps others) is sought in order to reach a consensus.
5. The term *dynamic* refers to the fact that we strive to capture how different variables in a system affect, and are affected by, other variables. The time factor can be seen as an implicit part of the framework but it would be possible to make it more explicit by e.g. describing dependencies in terms of how loose/tight they are (i.e. how fast a change is spreading across a dependency). Furthermore, it is also possible to make the time factor more explicit by for example dividing the emergency response into different discrete time segments and collecting data for each segment specifically.

References

Abrahamsson, M., Johansson, H., Fredholm, L., Eriksson, K. and Jacobsson, A. (2007), 'Analytical Input to Emergency Preparedness Planning at the Municipal Level – A Case Study', in Jones, A. (Ed), *TIEMS 2007 Disaster Recovery And Relief – Current & Future Approaches*, Trogir, Croatia, pp. 423–432.

Abrahamsson, M., Jönsson, H. and Johansson, H. (2008), 'Analyzing Emergency Response Using a Systems Perspective', in Kao, T.-M., Zio, E. and Ho, V. (Eds), *PSAM9: Ninth International Probabilistic Safety Assessment and Management Conference*, Hong Kong, China.

Ashby, W.R. (1957), *An Introduction to Cybernetics*, Chapman & Hall Ltd, London.

Axelrod, R. and Cohen, M.D. (2000), *Harnessing Complexity: Organizational Implications of a Scientific Frontier*, Basic Books, New York.

Catino, M. (2008), 'A Review of Literature: Individual Blame vs. Organizational Function Logics in Accident Analysis', *Journal of Contingencies and Crisis Management*, Volume 16, Number 1, pp. 53–62.

Comfort, L. and Kapucu, N. (2006), 'Inter-Organizational Coordination in Extreme Events: The World Trade Center Attacks, September 11, 2001', *Natural Hazards*, Volume 39, Number 2, pp. 309–327.

Davies, R. (2004), 'Scale, Complexity and the Representation of Theories of Change', *Evaluation*, Volume 10, Number 1, pp. 101–121.

Davies, R. (2005), 'Scale, Complexity and the Representation of Theories of Change - Part II', *Evaluation*, Volume 11, Number 2, pp. 133–149.

Dekker, S. (2004), *Ten Questions About Human Error: a New View of Human Factors and System Safety*, Lawrence Erlbaum Associates, Mahwah.

Drabek, T.E. and McEntire, D.A. (2003), 'Emergent Phenomena and the Sociology of Disaster: Lessons, Trends and Opportunities from the Research Literature', *Disaster Prevention and Management*, Volume 12, Number 2, pp. 97–112.

Dynes, R.R., Quarantelli, E.L. and Kreps, G. (1981), *Perspective on Disaster Planning*, Disaster Research Center, University of Delaware, Newark.

Fischhoff, B. (1975), 'Hindsight≠Foresight: The Effect of Outcome Knowledge on Judgement Under Uncertainty', *Journal of Experimental Psychology: Human Perception and Performance*, Volume 1, Number 3, pp. 288–299.

Gasper, D. (2000), 'Evaluating the "Logical Framework Approach". Towards Learning-Oriented Development Evaluation', *Public Administration and Development*, Volume 20, Number 1, pp. 17–28.

Haimes, Y.Y. (1998), *Risk Modeling, Assessment, and Management*, John Wiley & Sons, New York.

Heath, R. (1998), 'Looking for Answers: Suggestions for Improving How We Evaluate Crisis Management', *Safety Science*, Volume 30, Number 1–2, pp. 151–163.

Hollnagel, E. (2004), *Barriers and Accident Prevention*, Ashgate Publishing Limited, Aldershot.

Jönsson, H. (2007), *Risk and Vulnerability Analysis of Complex Systems – A Basis For Proactive Emergency Management*, Department of Fire Safety Engineering and Systems Safety, Lund University, Lund.

Jönsson, H., Abrahamsson, M. and Johansson, H. (2007), 'An Operational Definition of Emergency Response Capabilities', in Jones, A. (Ed), *TIEMS 2007 Disaster Recovery And Relief – Current & Future Approaches*, Trogir, Croatia, pp. 350–359.

Kaplan, S. (1997), 'The Words of Risk Analysis', *Risk Analysis*, Volume 17, Number 4, pp. 407–417.

Keeney, R.L. (1992), *Value-Focused Thinking, A Path To Creative Decisionmaking*, Harvard University Press, Cambridge.

Leveson, N. (2004), 'A New Accident Model for Engineering Safer Systems', *Safety Science*, Volume 42, Number 4, pp. 237–270.

McConnell, A. and Drennan, L. (2006), 'Mission Impossible? Planning and Preparing for Crisis', *Journal of Contingencies and Crisis Management*, Volume 14, Number 2, pp. 59–70.

McLaughlin, J.A. and Jordan, G.B. (1999), 'Logic Models: A Tool for Telling Your Program'S Performance Story', *Evaluation and Program Planning*, Volume 22, Number 1, pp. 65–72.

Quarantelli, E.L. (1997), 'Ten Criteria for Evaluating the Management of Community Disasters', *Disasters*, Volume 21, Number 1, pp. 39–56.

Rasmussen, J. (1985), 'The Role of Hierarchical Knowledge Representation in Decisionmaking and System Management', *IEEE Transactions on Systems, Man, and Cybernetics*, Volume SMC-15, Number 2, pp. 234–243.

Rasmussen, J. (1997), 'Risk Management in a Dynamic Society: A Modelling Problem', *Safety Science*, Volume 27, Number 2/3, pp. 183–213.

Rasmussen, J. and Svedung, I. (2000), *Proactive Risk Management in a Dynamic Society*, Swedish Rescue Services Agency, Karlstad.

Reason, J. (2000), 'Human Error: Models and Management', *British Medical Journal*, Volume 320, Number 7237, pp. 768–771.

Rogers, P.J. (2008), 'Using Programme Theory to Evaluate Complicated and Complex Aspects of Interventions', *Evaluation*, Volume 14, Number 1, pp. 29–48.

Ropohl, G. (1999), 'Philosophy of Socio-Technical Systems', *Techné: journal of the Society for Philosophy and Technology*, Volume 4, Number 3, pp. 59–71.

Simon, H. (1996), *The Sciences of the Artificial*, The MIT Press, Cambridge.

Stallings, R.A. (2006), 'Methodological Issues', in Rodriguez, H., Quarantelli, E.L. and Dynes, R.R. (Eds), *Handbook of Disaster Research*, Springer, New York, pp. 55–82.

Tierney, K.J. (2002), 'The Field Turns Fifty: Social Change and the Practice of Disaster Fieldwork', in Stallings, R.A. (Ed), *Methods of Disaster Research*, Xlibris, Philadelphia, pp. 349–374.

Uhr, C. and Johansson, H. (2007), 'Mapping an Emergency Management Network', *International Journal of Emergency Management*, Volume 4, Number 1, pp. 104–118.

Uhr, C., Johansson, H. and Fredholm, L. (2008), 'Analysing Emergency Response Systems', *Journal of Contingencies and Crisis Management*, Volume 16, Number 2, pp. 80–90.

Wasserman, S. and Faust, K. (1999), *Social Network Analysis – Methods and Applications*, Cambridge University Press, Cambridge.

Webb, G.R. and Chevreau, F.-R. (2006), 'Planning to Improvise: The Importance of Creativity and Flexibility in Crisis Response', *International Journal of Emergency Management*, Volume 3, Number 1, pp. 66–72.

Woods, D. and Cook, R.I. (2002), 'Nine Steps to Move Forward from Error', *Cognition, Technology & Work*, Volume 4, Number 2, pp. 137–144.

V

Risk and Vulnerability Analysis in Practise: Evaluation of Analyses Conducted in Swedish Municipalities

Henrik Hassel

Department of Fire Safety Engineering and Systems Safety, Faculty of Engineering, Lund University, Box 118, 221 00 Lund, Sweden
henrik.hassel@brand.lth.se

Abstract

Risk and vulnerability analysis (RVA) can benefit the process of preventing and preparing for disasters, both by generating a basis for making decisions, and by enhancing risk awareness, safety culture and response capacity through the RVA process itself. In studying and understanding the practises related to RVA, insights can be gained regarding ways in which the RVA can be improved in society, as well as on how methods for RVA can be designed to suit the particular context. However, studies of this sort are rather rare. This paper presents an evaluation of RVA performed by Swedish municipalities, which are important actors in the Swedish emergency management system. This is done by employing a systematic, design science approach outlined in the paper. Document studies and interviews were used to collect data on the analyses performed by the municipalities, and the evaluation shows that there is room for improvement. The results can be especially relevant for municipalities developing their RVA practises, as well as for other actors performing similar types of analyses.

Keywords

Risk and vulnerability analysis, practises, evaluation, design science, municipalities.

1 Introduction

Emergencies of natural, technological or intentional origin may occur in any part of the world, and cause catastrophic damage to individuals, organisations and society in general. Risk and vulnerability analysis (RVA) can play an important role in the process of preventing and preparing for disasters by generating a sound knowledge basis. This has been stressed many times in the research literature (Quarantelli, 1998; Perry and Lindell, 2003; Alexander, 2005), and is being increasingly realised in practise. In Sweden, for example, several agencies (of importance in society) are required by law to conduct regular risk and vulnerability analyses. Several international disaster management agencies have also stressed the importance of conducting proactive risk and vulnerability analysis (IFRC, 1999; UN/OCHA, 2008).

Theoretical concepts, methodological proposals and suggestions for tools useful when conducting RVA and making risk-related decisions abound in the scientific literature. The plausibility of these concepts and proposals is often supported by rational argumentation, small-scale demonstrations and sometimes also full-scale applications, see e.g. Ferrier and Haque (2003), Cruz and Okado (2008), Simpson and Human (2008) and Li et al. (2009). In addition, the literature contains a few reports discussing and defining requirements regarding the quality, validity and reliability of RVA, as well as suggested procedures for reviewing analyses that have been conducted, e.g. Fischhoff et al. (1984), Morgan and Henrion (1990), Stern and Fineberg (1996), Rosqvist and Touominen (2004), Busby and Hughes (2006) and Aven and Heide (2009).

The literature includes very few empirical studies of risk analysis practices, i.e. how risk analysis practitioners actually go about analysing risk and vulnerability, which is also pointed out by Strömgren and Andersson (2010). Studies of this type are highly relevant for risk and disaster research for at least two reasons. First, empirical studies may provide insight into aspects of risk analysis practises that need to be improved in order to improve the quality of the analysis. Second, empirical studies of risk practises may identify needs for modifications or improvements in theory and methodology. It is important to note that method development does not necessarily mean more advanced methods, which is often the "natural" measure taken in risk analysis research. Instead, empirical insight may reveal constraints on risk analysis practitioners, e.g. lack of time or resources, which may prevent or restrict the optimal use of existing theories and methods. Thus, rather than demonstrating the need for more advanced and comprehensive methods, this could indicate a need for simpler methods that provide satisfactory results. In other words, if a researcher is trying to develop methods suitable for practical use, then he or she should be conversant with the everyday situation of risk analysis practitioners.

This paper focuses primarily on RVAs performed within the Swedish emergency management system[1]. According to Swedish legislation, all central authorities, municipalities, county councils and county administration boards are required to perform RVAs (SFS, 2006:544, 2006:942). The legislation related to RVAs is relatively new, and the first few studies at different governmental levels have revealed some deficiencies in the Swedish RVA system (Hamrin and Strömgren, 2008; Nordström and Tonegran, 2008; SNAO, 2008; Abrahamsson and Tehler, 2009; MSB/SKL, 2009). Especially notable are the conclusions drawn by the Swedish National Audit Office (SNAO) in its audit of issues related to disaster preparedness at national level. The SNAO concluded that analyses on all governmental levels had deficiencies that made it impossible to obtain a comprehensive picture of risks and vulnerabilities at national level (SNAO, 2008).

A principle of the RVAs performed in the Swedish emergency management system is that analyses on all governmental levels should be regarded as a system, which means that it should be possible to make overall analyses and decisions on higher governmental levels based on analyses performed at lower levels. This stresses the importance of local level analyses, since poor quality at this level will be reflected in RVAs performed at higher levels. In addition, the Swedish emergency management system is based on the principle of proximity, i.e. an emergency should be dealt with at the lowest possible level in society, again stressing the role of the local level. Hence, a good place to start to try to improve the Swedish RVA system is at local level analyses performed by municipalities.

The present paper has two main aims: one descriptive and the other normative. The descriptive aim concerns studying how RVAs are conducted in a number of Swedish municipalities, while the normative aim concerns evaluating these RVAs and suggesting how the analyses can be improved. Although the study focuses primarily on Swedish municipal RVAs, it may have much broader implications since the evaluations and suggestions for improvements, to a large extent, concern general aspects of RVAs. The conclusions of this study may therefore be useful in improving other actor's RVAs. The paper is organised as follows. In Section 2, the approach to evaluating and improving RVAs is outlined, in Section 3, Swedish legislation is analysed to delineate the desired purposes of municipal RVAs, and in Section 4, the empirical study, conducted in eight Swedish municipalities is introduced. Section 5 presents the results of the evaluation of

[1] Information on the Swedish emergency management system can be found on the website of the Swedish Civil Contingencies Agency: http://www.msb.se.

these RVAs, and in Section 6 the results are discussed, focusing especially on possible improvements and implications. Finally, the conclusions are briefly stated in Section 7.

2 A design science approach to evaluating and improving RVAs

Design science is concerned with constructing new, or improving existing, artefacts (van Aken, 2004). Artefacts are most often physical, such as cars, buildings, tools, bridges, paintings, etc. However, they may also be of more abstract type[2], such as methods, constructs, definitions, regulations, philosophies, etc. RVAs and RVA processes can thus be regarded as a type of artefact. This also means that design science can be used to formulate an approach suitable for evaluating and improving RVAs. In Figure 1 the approach adopted in the present paper is outlined, which draws heavily on design science. The separate building blocks of the approach are described in further detail below.

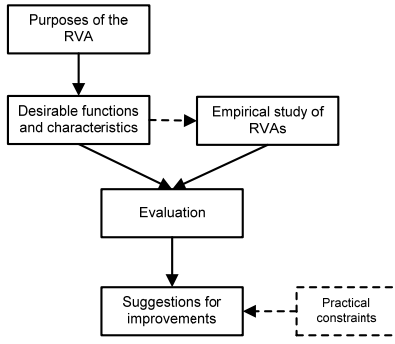


Figure 1. An overview of the design science approach used to evaluate and improve RVAs.

The essence of a design problem lies in building artefacts to achieve certain purposes and goals (Simon, 1996). The first step in a design problem is therefore to establish the purpose of the particular artefact, which essentially means, why an artefact exists or ought to exist and what it should be used for (Brehmer, 2008). In the context of RVA, the risk analysts or decision-makers usually specify the desired purpose, and the evaluation should then be performed with respect to this purpose.

The purpose is a very high-level and abstract description of an artefact (see Rasmussen (1985) for different levels of describing an artefact). In order to fulfil the stipulated purpose an artefact must have concretely expressed desirable characteristics and functions that describe what the artefact must be able to do (Brehmer, 2008). For example, if one purpose of an artefact is to protect the brain from damage due to injury to the head, one desirable characteristic can be that the material of the artefact must be of such a kind that it can withstand the forces exerted on it[3]. Desirable functions and characteristics must be justified, i.e. there must be good arguments that the purpose of the artefact will be fulfilled if the artefact has the stated functions and characteristics. This is in accordance with March and Smith (1995) who argued that one of the quality criteria for design research is the persuasiveness of the claims that the artefact is effective (i.e. that it fulfils its purpose). Justification can sometimes be made by performing or citing empirical or theoretical research in support of the desirable characteristics argued for. When such

[2] Checkland (1993) uses the term "designed abstract systems" to refer to various types of artefacts that do not exist physically in the same way as e.g. cars and hammers, but rather exist as a set of interrelated conceptual thoughts.

[3] Note that the exact material that should be used is not addressed here, i.e. the form of the artefact (Brehmer, 2008), since many types of materials are likely to provide a satisfactory design.

research is lacking, the alternative is simply to present rational argumentation and logical reasoning regarding the validity of the claims. Most importantly, the argumentation must be explicit and transparent to enable the review of any normative assumptions made regarding the relation between purpose and desirable characteristics.

Design always includes a phase in which suggested or existing artefacts are evaluated (Hevner et al., 2004), and the evaluation must be made with respect to the specification of that artefact (Lewin, 1983). In the context of RVA, this means performing empirical studies of RVAs and comparing their characteristics and functions with the characteristics and functions regarded as being desirable. The final step of the design science approach is to consider how the RVAs can be modified in order to better achieve their purposes, i.e. to suggest improvements. Note that, in order to construct effective and feasible artefacts or modifications of artefacts, a good understanding of the context in which the artefact is embedded is required (March and Smith, 1995). In the case of RVA, this is related to insights regarding practical constraints, e.g. access to resources for conducting the analyses (in terms of time and manpower).

3 The purpose of municipal RVA

Swedish legislation requires that municipalities conduct RVA and it also provides the motivation for it, which means that the purpose can be derived from the legislation. Of course, nothing prohibits Swedish municipalities from having additional purposes, but these are outside the scope of this paper since they are likely to vary between different municipalities. The most important legislative documents are the laws[4] and regulations[5] pertaining to municipal RVAs. However, since laws and regulations provide an abstract and condensed description of the purpose, it is necessary to consider the preparatory publications related to the legislation (e.g. governmental bills and inquiry reports)[6].

The overall purpose of the law that regulates municipal RVAs (SFS, 2006:544) is to ensure that municipalities reduce their level of vulnerability and establish a good emergency response capability, e.g. through municipal RVAs, establishing a disaster response plan, education and training. Municipalities should identify and analyse extraordinary events that may occur and how these could affect the municipal organisation. In addition, the analyses should be used as the basis for establishing a disaster response plan. The law also stipulates that the municipality should coordinate various actors' planning and preparedness efforts within its geographic area. Furthermore, according to the closely related regulation (SFS, 2006:637), municipalities should report the measures taken in relation to preparedness to manage extraordinary events to the relevant county administration board.

The preparatory publications include a government bill (Governmental Bill, 2005/06:133) and an inquiry report (SOU, 2004:134)[7], which provide more background and greater detail regarding the intentions of the legislation. The reports are similar regarding topics related to municipal RVAs. It is stated that the primary purpose of the

[4] Legislation issued by Parliament.
[5] Legislation issued by the Government. Note that a regulation is subordinate to a law.
[6] See http://www.sweden.gov.se/content/1/c6/08/48/61/758e413e.pdf for a brief introduction to the Swedish law-making process.
[7] Another important source is the so-called "Municipal agreement" (http://www.kbm-sema.se/upload/2283/kommunernas_uppgift_samhallet-2004.pdf) which is a contract between the Swedish Association of Local Authorities and Regions, and the Government regarding the tasks of municipalities in the context of emergency management. The agreement came into force before the law and regulation referred to above were issued. This is not explicitly addressed here, however, since the government bill and inquiry report cover the content of the agreement.

analyses should be to increase decision-makers' awareness and knowledge regarding threats and risks within the municipal area of responsibility. Analyses should be used as a basis for preparedness planning and the implementation of risk and vulnerability reducing measures, and the analysis processes should develop disaster response capabilities. The scope of the analyses should be the internal municipal organisation as well as partly and wholly owned municipal companies. In addition to the internal focus, municipal RVAs should also include an overall analysis of risks and vulnerabilities within the municipality as a geographic area. It is also emphasized that municipal RVAs should be seen as a basis for analyses at higher governmental levels (regional and national) allowing a holistic picture of risk and vulnerability to be generated at these levels. Finally, the reports state that the analyses, or parts of them, should be communicated to relevant actors in the municipality, including the public.

From this brief analysis of the legislative texts related to Swedish municipal RVAs, two distinct purposes that are relevant for the quality of the analyses at the municipal level can be distinguished. First, the municipal RVA should generate a good knowledge basis for decision-making regarding risk and vulnerability reducing measures in the municipality (Purpose 1). Using RVAs as a basis for, or for informing, risk-related decisions is the purpose most commonly emphasized in the research literature, see e.g. Kaplan and Garrick (1981), Aven (2003), Apostolakis (2004), Paté-Cornell and Dillon (2006), and Aven and Renn (2009). The underlying idea is that if the RVA is of high quality, then it is more likely that the decisions made, given they are informed by the RVA, are of high quality. Secondly, the RVA processes should in themselves contribute to decrease vulnerability and risk through increased disaster response capability, enhanced safety culture, increased mental awareness, etc. (Purpose 2). As such, this purpose addresses risk and vulnerability reductions regardless of any formal decisions made or implemented within the scope of Purpose 1. This view of the purpose of RVA is, however, dealt with to a much less extent in the research literature than viewing RVA as generating data on which to base informed decisions. Therefore, there are far fewer recommendations on how RVA processes should be designed to actually fulfil this purpose.

4 The empirical study

This section provides an overview of the empirical study conducted in Swedish municipalities and used as input for the evaluation. The details related to each of the two purposes defined above are then specifically addressed in the next section. Eight municipal RVAs were selected for evaluation. The selection was based on three criteria. First, the chosen municipalities should represent a range of different sizes. The number of inhabitants in the chosen municipalities ranged from 14 000 to 280 000, and the number of people employed by the municipality ranged from 1000 to 20 000. In the Swedish context, these represent a very large and a very small municipality. Second, the municipalities were located in the southern parts of Sweden for practical reasons. Third, since the objective of the present paper was to study RVA practises, only municipalities that had initiated a fairly structured RVA process were chosen, since otherwise there would have been very little substance to evaluate. The analysis processes were highly coordinated in two pairs of municipalities, which essentially means that six different RVA processes were included in the evaluation.

4.1 Data collection and analysis techniques

In evaluations of risk and vulnerability analyses, including the ones referred to in the introduction, it is common to only study the documentation of the RVA. However, it is the author's opinion that this provides only a partial view of the RVA and the RVA

process. Therefore, both document studies and interviews were used to collect data on the municipal RVAs.

Interviews were conducted with those employed by the municipalities who had a central role in municipal RVA (e.g. coordinators, facilitators). In total, nine semi-structured interviews were conducted, and in three of these more than one person was interviewed simultaneously. Initially, the interviews were aimed at gaining an overall view of how the RVAs had been performed. The interviews were then directed towards gaining more specific insights into the desirable characteristics and functions related to the two purposes.

The documentation from five of the six different RVA processes was studied. Documentation was not publicly available from one of the municipalities at the time of the investigation. To compensate for this, additional interviews were conducted in this municipality. Primarily publicly available documentation was studied. Additional documentation related to the RVAs was not included in the evaluation. Content analysis (Weber, 1990) was then used to analyse the documentation. A number or themes of the RVAs were identified as interesting for the document study. The themes were chosen based on their relevance to either of the two purposes and the desirable characteristics related to these. Various key words were then used to locate segments of the texts that were related to some of the specified themes. The text segments concerning each theme were used to interpret, and make inferences about, how the RVA addressed the theme of interest.

4.2 General characteristics and context of the RVAs

The analyses differed in several ways, regarding scope, the methods used, the people involved and so on; however, they have several features in common. First, broad identification of undesirable events, hazards, or scenarios, similar to a preliminary hazards analysis (PHA), was performed. In several municipalities, this step also included a discussion on, and mapping of the values, objects, etc. considered especially important to protect. Some of the analyses only addressed extraordinary events, whereas others also included more small-scale emergencies (which are covered by other legislation). Second, for each event identified, semi-quantitative estimates of the likelihood and negative consequences (e.g. on a scale of 1-4) were made in most analyses. Third, based on the broad identification of possible hazards and events, one or in some case a few events were chosen and an in-depth analysis of the emergency response capabilities was performed. This was done through an exercise in which a hypothetical scenario was described and a discussion ensued on how the hypothetical scenario would have been dealt with by the actors involved. Fourth, based on the discussion, including any possible identified deficiencies, measures for improving the response capability were suggested.

Most analyses primarily addressed risks and vulnerabilities for the municipal administration rather than the municipality as a geographic area, especially regarding the analysis of emergency response capability. In five municipalities specific analyses were performed in each municipal department/district[8]. In one of these the scope was limited to the scenario analysis of emergency response capability. In all the analyses studied the municipal administration as a whole was also addressed, although two of these seemed mainly to consist of summaries of the results from the analyses performed at the municipal department/district level. Two of the analyses were slightly different in that a broad identification of undesirable events was carried out on a multi-municipality level,

[8] The number of municipal departments ranges from 5 to 25 depending on the size of the municipality.

and then a complete analysis was performed at the municipality level with respect to a certain class of risk.

The information obtained, especially from the interviews, led to a number of insights regarding the context of the RVAs, which are important in identifying relevant practical constraints. A noteworthy insight was the importance of political and management support. A high level of engagement among the participants was also recognised as being important. In cases where adequate support and engagement were not achieved, interviewees mentioned these as factors hindering a successful outcome. Since RVA is a new activity for most municipalities and municipal departments, the RVA coordinators have an important role in demonstrating the value of the RVA and motivating the participants – this is especially important in the early stages of the RVA. A practical constraint identified is that the time available for RVA is very limited. Of course, the time made available is highly influenced by the perceived importance of the analyses in the organisations. However, as one of the interviewees stated, it is important to adapt the time required to perform the analysis to the time participants and managers feel is reasonable, given all their other competing tasks – otherwise their level of engagement may be lower, which could have negative effects on the quality of the RVA.

5 Evaluation of the RVAs

This section presents the evaluation of the municipal RVAs. Desirable characteristics and functions are briefly specified for each of the two purposes, together with short descriptions of the extent to which the studied RVAs have these characteristics and functions (derived from the empirical study). Each purpose is addressed in further detail below, including justification of the specified desirable characteristics and functions, as well as more detailed discussions regarding the most interesting aspects of the evaluation.

5.1 Purpose 1: Good basis for risk-related decision-making

A commonly expressed desirable characteristic in relation to Purpose 1 is detailed and comprehensive documentation of RVAs (Morgan and Henrion, 1990). Documenting the analysis properly, makes external scrutiny and review possible. In addition, it is easier for an organisation to use a previous analysis as the basis for future ones. Several of the studied documents, however, lacked the level of detail and clarity necessary to enable comprehensive external scrutiny. Interestingly, several of the interviewees expressed the opinion that the documentation was not particularly important – instead they assigned greater value to the deliberative processes performed throughout the RVA (this is addressed in more detail under Purpose 2 below).

The research literature on RVA usually argues in favour of focusing on undesirable events/scenarios that may lead to negative consequences, see e.g. Kaplan and Garrick (1981), Haimes (1998), Aven (2007) and Renn (2008). This is also stipulated in the legislation (SFS, 2006:544) as a desirable characteristic. Additionally, most approaches to risk include the characterisation/estimation of the likelihood and severity of each undesirable event, so that e.g. prioritisations are facilitated. All the analyses studied identified and described various undesirable events that could occur. Furthermore, probabilities and negative consequences were also addressed in all the analyses – most often in terms of semi-quantitative estimates.

A desirable characteristic of RVAs is that estimates of likelihood and consequences should be well-founded, e.g. through the use of empirical data, science and expertise (Stern and Fineberg, 1996; Klinke and Renn, 2002). Otherwise, it is possible that inappropriate prioritisations will be made and misdirected measures suggested. In the analyses studied

here, the estimates are based almost exclusively on discussions between the participants. In a few analyses it was claimed that external expertise and statistics had been used; however, in the documentation it is unclear how this was done. Furthermore, most analyses provide very little information on how the estimates were made, e.g. in terms of rational argumentation, which makes it difficult to review them. The key question then is: can the participants in the analyses be said to have suitable expertise for the task at hand? In the case of estimating the probability and consequences of extraordinary events, it is argued that this is not necessarily the case. The participants usually have good knowledge of the organisation's activities, but do not necessarily have any special knowledge about the hazards that may affect the municipality. This is also acknowledged by some of the interviewees. One of them, for example, stated that the estimates were performed by "laymen". When analysing the emergency response capabilities of the municipal administration, the situation is often different. In this context, the participants have the relevant expertise as they are generally chosen because they have good knowledge of the municipal administration's emergency resources, competencies and capabilities, etc.

The analysis of emergency response capability is restricted in another way in several of the studied analyses. This has to do with the fact that scenario analyses are conducted separately within each municipal department. However, it is desirable to include actors from other municipal departments and even external actors. The reason is that interdependencies between the actors make it very difficult to analyse an actor's capability without knowledge about how other actors would have responded, or what roles they would have had in the response. Several of the interviewees stated that many issues discussed during the scenario analyses had to be dismissed, as they lacked knowledge about other actors. Interestingly, two of the municipalities overcame this issue, to some extent, by forming analysis groups for specific scenarios, which included actors who were especially important for a particular scenario.

All the analyses studied included suggestions for measures to reduce risk and vulnerability. In several analyses, measures were suggested in relation to deficiencies in response capabilities identified in the in-depth analysis of scenarios. However, since only a single scenario was often analysed, such an approach may have limitations. First, it is very difficult to know the extent to which the suggested measures are effective in other scenarios, which of course is relevant when evaluating the overall effectiveness of the measures. Second, in focusing only on measures to improve the response capability, the potential for identifying effective preventive measures may be overlooked. In some of the analyses, separate measures were suggested for different categories of risks. While this approach is more comprehensive than focusing only on the ability to respond to a single scenario, the effectiveness of the measures in other categories of risk was not considered. Furthermore, one shortcoming of the analyses studied is that there was generally no description of the impact of the measure on response capability, vulnerability or risk; instead it is implicitly assumed that the measure will have some positive effect in the scenarios or categories of risk studied. Perhaps the likely effects were discussed by the participants, but few attempts were made to document them.

5.2 Purpose 2: The RVA processes themselves should decrease vulnerability and risk

If the RVA process itself is to contribute to a reduction in risk and vulnerability then it must somehow lead to positive changes in the participants' knowledge, understanding, awareness, skills, behaviour, attitudes, etc., which is also a precondition for positive organisational changes (Senge, 2006), for example, in terms of an enhanced safety culture. More specifically, the processes may create an increased awareness of risks and vulnerabilities, and stimulate the individual's self-reflection (Busby and Hughes, 2006;

Pelling, 2007). Although this does not guarantee a reduction in risk and vulnerability, it is certainly a good precondition for people and organisations to change their behaviour, e.g. leading to increased readiness to respond to emergencies. The process may also lead to the exchange of information and knowledge among the participants, e.g. on how future potential events can affect the participants/actors, what roles the various participants will have in the response activities, what resources and capabilities other participants/actors have, and how their actions affect those of others, etc. Finally, the process may also create social networks and relationships of trust between the participants; which in turn can have positive effects on response capabilities in the municipality, e.g., by facilitating cooperation and increasing social capital (Nakagawa and Shaw, 2004).

Evaluating whether the participants involved in the studied RVAs have actually undergone changes in ways that lead to reduced risks and vulnerabilities would require in-depth longitudinal studies of the individual participants. Although this would be very interesting indeed, it is outside the scope of the present paper. Instead, a number of preconditions for these positive changes are specified which can be seen as an initial set of desirable characteristics for the RVA process in relation to Purpose 2. First, there should be broad participation in the analyses since it is the changes in the individual participants that contribute to reduced risks and vulnerability. Analyses conducted by a single person in the municipality or by an external actor, such as an expert consultant, without the broad involvement of the municipality are thus not likely to lead to significant process benefits. Second, much of the positive changes in the participants can be credited to the interactive deliberations between the participants. When, for example, people learn about other actor's roles and resources, increase their knowledge about hazards, create social networks and relationships of trust, and reflect on their behaviour, etc., it is done through discussions and deliberation between the participants. The municipal RVA process should therefore be designed to be highly interactive and deliberative, rather than constitute the results of the work performed by individuals that have not interacted to any significant degree.

Turning to the analyses studied here, the first interesting finding was that many of the interviewees seemed to emphasize the importance of Purpose 2 above that of Purpose 1. One interviewee, for example, stated that it is not particularly important that the estimates of probability and consequences are accurate; it was rather the dialogue between the participants that mattered since this initiates mental reflective process and facilitates mutual learning. Several interviewees also stressed the importance of creating mental awareness of the fact that emergencies can happen. In societies where large-scale emergencies are rather rare (such as in Sweden) this can be very important, since the absence of emergencies often promotes a sense of invulnerability – "these things cannot happen here" ('t Hart, 1997, p.207).

A few analyses, or parts of analyses, were conducted by single individuals who, to some extent gathered, inputs from other actors, but where there was very little broader deliberation between groups of participants. Such approaches do not constitute good preconditions for fulfilling Purpose 2. For the most part, however, the analyses studied were performed by employing an interactive and deliberative approach, e.g. broad discussions on potential future scenarios and detailed discussions on the response to a specific scenario. In several of the analyses, however, these discussions were primarily restricted to discussions between individuals within a single municipal department/district. In addition, virtually no actors from other public or private organisations or any citizens were involved in any of the analyses studied. This restricts the learning and exchange of knowledge and information between municipal departments as well as beyond the municipal organisation.

Research has shown that the attitudes, commitment and involvement of top management are important factors for the safety culture in organisations (Rundmo et al., 1998; Flin et al., 2000; Weick and Sutcliffe, 2001), as well as for risk and preparedness issues in the context of crisis management ('t Hart, 1997; Boin and Lagadec, 2000). Therefore, it is argued that if the higher management levels are represented in the municipal RVA, it is more likely that Purpose 2 will be achieved. In all the analyses studied, the political leaders made the formal decision that RVA should be performed, but otherwise its involvement was limited. Managers at the municipal officer level have played more extensive roles. In some of the analyses (or parts of them) essentially all the participants were managers, while some of the other analyses involved a mixture of managers and operational staff with good knowledge of the "sharp end" of the activities. Finally, in other analyses participation by the management was limited, which could mean that that Purpose 2 will not be fulfilled to the same extent. There are naturally many other parallel processes in which the management can show commitment and contribute to improved safety culture. One should therefore be cautions in drawing the conclusion that these organisations lack a good safety culture.

6 Discussion

The evaluation of the eight Swedish municipal RVAs indicates that, although they contain several desirable characteristics and functions, there are several possibilities for improvement. Here, an improvement is simply seen as a change that leads to the improved fulfilment of some purpose (Churchman, 1968). It is therefore crucial to relate any suggestions for change to one or several purposes. The approach used to evaluate municipal RVAs stresses the role of purpose, and the evaluation was performed with respect to the purposes expressed in Swedish legislation. At the same time, a municipality may have additional purposes or may downplay the importance of some of the purposes expressed in the legislation. In such cases, some of the ways of improving the analyses, discussed below, would not be relevant, or other changes may be more relevant.

A complicating factor is that a change may affect several relevant purposes in terms of being positive for some and negative for others. In these cases, the relative importance of the various purposes must be assessed in order to decide whether a change constitutes a "net improvement". However, since such judgements are essentially subjective, the analysts/decision-makers (i.e. the individual municipalities) are more suitable to make them. Hence, no trade-offs between purposes are prescribed here; instead, potential improvements and their likely effects on the two purposes discussed will be explored, which can then be used as a basis for the decisions of individual municipalities.

Regarding the fulfilment of Purpose 1 (good basis for decisions) expert input and scientific and empirical data play a small role in the analyses studied. One way of improving the fulfilment of Purpose 1 is therefore to increase the involvement of those with the relevant expertise and strive to utilize existing data. In Sweden, there are almost 300 municipalities, all with limited resources for conducting RVAs; however, municipalities can benefit greatly from using the same expertise and data (adapted to their specific contexts). The supporting authorities, i.e. the Swedish Civil Contingencies Agency (MSB) and the administration board of a specific county, can play an important role in facilitating for and providing essential information to municipalities, instead of each municipality having to "invent the wheel" on their own. To some extent MSB already performs activities in this area, for example, publishing general hazards reports, providing experience feedback from past events, etc. In spite of these efforts, however, none of the municipalities studied quoted these as being used as sources of information in

their RVAs. Future work should therefore look into the needs of municipalities in terms information and expert input, and how MSB and the county administration boards can help meet these needs. A potential drawback of increasing the focus on scientific data and external expertise is that the fulfilment of Purpose 2 may be negatively affected, since it may come at the expense of less involvement of, and deliberation between, municipal actors. Hence, in order to ensure the fulfilment of Purpose 2, expert knowledge and empirical data must be appropriately integrated in the analysis without loosing the interactive and deliberative character of the analysis.

Regarding the part of the RVAs that focuses on emergency response capabilities, it was found that the analyses were often made with respect to a single scenario. The obvious question is, to what extent the results of such an analysis are able to provide insight regarding the generic capability of the municipality, rather than that which is specific to a particular scenario. The problem is exacerbated by the fact that in some of the analyses, risk and vulnerability reducing measures were only suggested with respect to that single scenario. This means that more general measures that have the potential of being much more effective considering the total picture of risk and vulnerability, may not have been considered. The recommendation here is therefore to strive to advance beyond the analysis of a single scenario, or at least to include an explicit phase in the scenario analysis discussing the generalisations that can be made from the analysis, in terms of both emergency response capability and risk and vulnerability reducing measures.

The analyses studied differed in terms of who the participants were: some only included municipal managers, some only municipal staff, and some included a combination. Different compositions may convey different benefits. As noted in the previous section, including the management level may improve safety culture and the perception of the importance of issues related to emergency management in the organisation. However, there may very well be municipal staff with more relevant and extensive knowledge of risks and vulnerability, meaning that the decision basis could be improved if these were involved. Perhaps the best composition is a mixture of both managers and staff. This composition was employed in a few of the analyses and the interviewees felt it was an effective composition. It should be noted, however, that it is far from clear which composition is the most appropriate, since this depends on both the purpose of the analysis (is Purpose 1 or 2 perceived as most important?), and the organisational context (e.g. is it already clear throughout the organisation that the management thinks safety and emergency management issues are important?).

As was noted in the evaluation, there was very little external participation in the RVA processes, e.g. in terms of other public or private actors, citizens or interest groups, etc. One reason for this is probably that the requirement to perform municipal RVAs is rather new, which means that several municipalities are still in the initial phase. The analyses have therefore largely been focused on the internal municipal organisation, and ways in which the organisation can respond to and recover from emergencies. In such an analysis, external actors play a smaller role. In expanding the scope of the analyses (recalling that the legislation requires the RVAs to address municipalities as geographic regions due to their responsibilities within geographic areas), participation from external actors becomes more relevant. In the research literature, the broad participation of stakeholders and affected parties, including the public, is often stressed in decision-making processes related to risk (Stern and Fineberg, 1996; Webler et al., 2001; Klinke and Renn, 2002). In the context of municipal RVAs, broad participation can potentially have a number of important benefits. Purpose 1 can be improved through better knowledge of public values, of the local context, of the vulnerabilities and capabilities of the public as well as the private sector, etc. Purpose 2 can be improved by enhancing awareness of risks and

vulnerability, as well as empowering the public, and clarifying responsibilities between the public sector, the private sector and the individual, etc. The drawback is, of course, that much more time and resources are needed to apply such an approach, which may not be available in many municipalities. As a long-term goal, however, it seems to be worth striving towards.

It should be mentioned that all municipalities perform parallel activities related to emergency management, for example, convening "emergency management councils" (which often include both internal and external actors, such as the public, private industry, etc.), performing emergency management drills, etc. These parallel activities can benefit from the municipal RVAs, such as providing information for the design of exercises. In addition, RVAs can benefit from these parallel activities, for example, by using information and knowledge elicited in the processes as input. It is recommended that each municipality consider how these parallel processes can be used to improve the quality, scope and efficiency of the RVA work.

The municipal RVAs selected were not intended to represent Swedish municipal RVAs in general (remember that a criterion for the choice was that the municipality should have come fairly far in the process). In spite of this, it is argued that this study provides several indications of characteristics and issues that are of more general character. The reason for this is that all municipalities conduct their analyses in the context of the same legislation, and are provided with the similar guidance from the central authority, which is likely to influence the characteristics of the municipal RVAs. Furthermore, the evaluation of the eight municipal RVAs should be seen as an initial and general evaluation of two of the relevant purposes. More detailed studies, as well as studies of additional municipalities, are needed to be able to suggest more detailed ways of improving RVA and the Swedish RVA system as a whole. A fruitful future research activity may be to adopt an action research approach (Greenwood and Levin, 2007) to try to implement the ideas for change in a particular municipality.

The findings presented in this paper have some broader implications. The two purposes addressed are likely to be highly relevant for a wide variety of RVAs carried out in other contexts. This means that the discussions regarding desirable characteristics and functions, and the discussion on improving RVA can provide valuable information for other actors. Each actor must, of course, first reflect on whether the suggested desirable characteristics and functions are relevant in that actor's context; and if so, the actors must compare their specific practises with what is argued to be desirable in order to identify possible ways of improving RVA.

The suggested and employed approach to evaluating and improving RVAs, which draws on design science, also has relevance outside the scope of the Swedish emergency management system. According to the approach, an evaluation of RVAs must be carried out with respect to one or several purposes and a set of more concrete desirable characteristics and functions. A key point of the approach is that, in order to ensure scientific rigor, the desirable characteristics must be justified using a logic line of arguments. It is crucial that the line of argument is made transparent, highlighting the assumptions made, since the results of an evaluation are highly contingent on the assumed purpose and derived desirable characteristics. Other purposes in performing RVAs simply mean other desirable characteristics.

The perhaps most interesting finding of the evaluation was that the importance of the process itself was emphasized by the interviewees, rather than the actual data and the formal decisions that resulted from the process. The role of process is stressed in the

literature on disaster preparedness (Quarantelli, 1998) but it is not in accordance with the traditionally expressed aim of risk and decision analysis. There are some indications, though, of increased attention to "process benefits" in the literature on risk analysis. McDaniels and Gregory (2004), for example, argue that learning should be included as an explicit objective in a structured risk management decision process. Learning can be related to other decisions, the process of making decisions, the substance of the issue at hand, decisions with other actors, etc. The role of learning is also emphasized in the "analytic-deliberative process", suggested by a committee of distinguished risk experts, where it is argued that deliberation can become an interactive learning process for participants, and can promote mutual exchange of information and knowledge (Stern and Fineberg, 1996). A parallel can also be drawn with the field of sustainable development, where it is argued that the process of developing sustainability indicators can stimulate a learning process that enhances the overall understanding and management of environmental issues, facilitates community capacity building, stimulates change in individuals and systems, improves the way in which future problems are addressed, and leads to various actors working together on other issues (Fraser et al., 2006; Reed et al., 2006).

Finally, in the field of participatory disaster risk assessment, Pelling (2007) argues that analysis processes can foster self-reflection and self-empowerment among participants. At the same time, he argues that there is very limited evidence as to whether approaches claiming to be participatory actually empower the participants and their communities. Future research must therefore address the question of how RVA processes should be designed so as to achieve the process benefits described above (i.e. Purpose 2 in the present evaluation). In relation to this, it is also essential to consider how this can be done without significantly reducing the quality and rigor of the decision basis generated in the RVA process (i.e. Purpose 1).

7 Conclusions

The present paper reports on an initial evaluation of eight Swedish municipal risk and vulnerability analyses. The evaluation was made with respect to two purposes expressed in the Swedish legislation: RVAs should be used as a basis for decisions regarding risk and vulnerability reduction, and the processes themselves should decrease risks and vulnerabilities. The evaluation was performed using a design science approach, and it was shown that this provided a good means of structuring the evaluation. The key points of this approach is the transparent and logic line of reasoning from purpose to desirable characteristics and functions (including justification); and then finally the comparison with a number of empirically studied analyses.

The findings show that there are some areas for improvement, which was expected since these activities are rather new in many Swedish municipalities. Implementing the RVA process in municipalities and municipal departments/districts and making them work in the long run is not an easy task. Implementing changes and testing new ways of performing analyses must therefore be considered from a long-term perspective. The potential improvements discussed in the present paper can be seen as initial steps for improving the quality of RVAs; however, each municipality, as well as any other actors wanting to use the present evaluation as a basis for improving their RVAs, must analyse their specific situation very carefully to determine which changes are best for them. It is especially important to carefully consider in the reason for conducting RVAs: is it primarily to generate high-quality data that can be used as a basis for decisions, or is it to improve the participants' knowledge, skills, behaviour, etc., and stimulate self-reflection and self-empowerment? Different purposes call for different process designs.

Acknowledgements

The author would like to thank Professor Kurt Petersen, Senior lecturer Henrik Tehler, Doctor Marcus Abrahamsson, Ph.d. student Kerstin Eriksson and Ph.d. student Olof Ekman for valuable comments on the manuscript. The author would also like to thank the Swedish Civil Contingencies Agency (MSB) for funding the research presented in the paper.

References

Abrahamsson, M. and Tehler, H. (2009), "The role of risk and vulnerability analyses in emergency management systems - evaluating regional RVAs in the Swedish emergency management system, Submitted to a scientific journal.

Alexander, D. (2005), "Towards the development of a standard in emergency planning", *Disaster Prevention and Management*, **14**(2):158-175.

Apostolakis, G. E. (2004), "How Useful is Quantitative Risk Assessment", *Risk Analysis*, **24**(3):515-520.

Aven, T. (2003), *Foundations of Risk Analysis: A Knowledge and Decision-Oriented Perspective*. John Wiley & Sons, Chichester.

Aven, T. (2007), "A unified framework for risk and vulnerability analysis covering both safety and security", *Reliability Engineering & System Safety* **92**:745-754.

Aven, T. and Heide, B. (2009), "Reliability and validity of risk analysis", *Reliability Engineering & System Safety*, **94**:1862-1868.

Aven, T. and Renn, O. (2009), "The Role of Quantitative Risk Assessments for Characterizing Risk and Uncertainty and Delineating Appropriate Risk Management Options, with Special Emphasis on Terrorism Risk", *Risk Analysis*, **29**(4):587-600.

Boin, A. and Lagadec, P. (2000), "Preparing for the Future: Critical Challenges in Crisis Management", *Journal of Contingencies and Crises Management*, **8**(4):185-191.

Brehmer, B. (2008), "Vad är ledningsvetenskap?", *Kungliga Krigsvetenskapsakademiens Handlingar och Tidskrift*, **1**:43-72. (In Swedish.)

Busby, J. S. and Hughes, E. J. (2006) "Credibility in risk assessment: a normative approach", *International Journal of Risk Assessment and Management*, **6**(4-6):508-527.

Checkland, P. (1993), *Systems Thinking, Systems Practice*, John Wiley and Sons Ltd, Chichester.

Churchman, C. W. (1968), *The Systems Approach*, Delacorte Press, New York.

Cruz, A. M. and Okado, N. (2008), "Methodology for preliminary assessment of Natech risk in urban areas", *Natural Hazards*, **46**:199-220.

Ferrier, N. and Haque, C. E. (2003), "Hazards Risk Assessment Methodology for Emergency Managers: A Standardized Framework for Application", *Natural Hazards*, **28**:271-290.

Fischhoff, B., Lichtenstein, S., Slovic, P., Derby, S. L. and Keeney, R. L. (1984) *Acceptable Risk: A Critical Guide*, Cambridge University Press, Cambridge.

Flin, R., Mearns, K., O'Connor, P. and Bryden, R. (2000), "Measuring safety climate: identifying the common features", *Safety Science*, **34**:177-192.

Fraser, E. D. G., Dougill, A. J., Mabee, W. E., Reed, M. and McAlpine, P. (2006) "Bottom up and top down: Analysis of Participatory processes for sustainability indicator identification as a pathway to community empowerment and sustainable environmental management", *Journal of Environmental Management*, **78**(2):114-127.

Governmental Bill (2005/06:133), *Samverkan vid kris - för ett säkrare samhälle*, The Swedish Government. (In Swedish.)

Greenwood, D. J. and Levin, M. (2007), *Introduction to Action Research: Social Research for Social Change*. Sage Publications, Thousand Oaks.

Haimes, Y. Y. (1998), *Risk Modeling, Assessment, and Management*, John Wiley & Sons, New York.

Hamrin, I. and Strömgren, M. (2008), *Regional risk- och krishantering - en studie av samtliga länsstyrelsers risk- och sårbarhetsanalyser*. Master's thesis, Lund University, Lund. (In Swedish.)

't Hart, P. (1997), "Preparing Policy Makers for Crisis Management: The Role of Simulations", *Journal of Contingencies and Crises Management*, **5**(4):207-215.

Hevner, A. R., March, S.T., Park, J. and Ram, S. (2004) "Design Science in Information Systems Research", *MIS Quarterly*, **28**(1):75-105.

IFRC (1999), *Vulnerability and capacity assessment: An International Federation Guide*, International Federation of Red Cross and Red Crescent Societies, Geneva.

Kaplan, S. and Garrick, B. J. (1981), "On The Quantitative Definition of Risk", *Risk Analysis*, **1**(1):11-27.

Klinke, A. and Renn, O. (2002), "A New Approach to Risk Evaluation and Management: Risk-Based, Precaution-Based, and Discourse-Based Strategies", *Risk Analysis*, **22**(6):1071-1094.

Lewin, D. (1983), "Engineering Philosophy: The Third Culture?", *Leonardo*, **16**(2):127-132.

Li, H., Apostolakis, G. E., Gifun, J., VanSchalkwyk, W., Leite, S. and Barber, D. (2009), "Ranking the Risks from Multiple Hazards in a Small Community", *Risk Analysis*, **29**(3):438-456.

March, S. T. and Smith, G. F. (1995), "Design and natural science research on information technology", *Decision Support Systems*, **15**:251-266.

McDaniels, T. L. and Gregory, R. (2004), "Learning as an Objective within a Structured Risk Management Decision Process", *Environmental Science & Technology*, **38**(7):1921-1926.

Morgan, G. M. and Henrion, M. (1990), *Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis*, Cambridge University Press, Cambridge.

MSB/SKL (2009), *Kommunernas krisberedskap - avstämning om kommunernas uppbyggnadsperiod 2006-2009*, Swedish Civil Contingencies Agency/Swedish Association of Local Authorities and Regions, Karlstad. (In Swedish.)

Nakagawa, Y. and Shaw, R. (2004), "Social Capital: A Missing Link to Disaster Recovery", *International Journal of Mass Emergencies and Disasters*, **22**(1):5-34.

Nordström, H. and Tonegran, D. (2008), *Kommunal krisberedskap i Skåne: Inventering av sju skånska kommuners dokumenterade krisberedskap*, Master's thesis, Lund University, Lund. (In Swedish.)

Paté-Cornell, M. E. and Dillon, R. L. (2006), "The Respective Roles of Risk and Decision Analyses in Decision Support", *Decision Analysis*, **3**(4):220-232.

Pelling, M. (2007), "Learning from others: the scope and challenges for participatory disaster risk assessment", *Disasters*, **31**(4):373-385.

Perry, R. W. and Lindell, M. K. (2003), "Preparedness for Emergency Response: Guidelines for the Emergency Planning Process", *Disasters*, **27**(4):336-350.

Quarantelli, Q. L. (1998), "Major Criteria For Judging Disaster Planning And Managing Their Applicability In Developing Countries", Disaster Research Centre, University of Delaware, Newark.

Rasmussen, J. (1985), "The Role of Hierarchical Knowledge Representation in Decisionmaking and Systems Management", *IEEE Transactions on Systems, Man, and Cybernetics*, **15**(2):234-243.

Reed, M. S., Fraser, E. D. G. and Dougill, A. J. (2006), "An adaptive learning process for developing ad applying sustainability indicators with local communities", *Ecological Economics*, **59**:406-418.

Renn, O. (2008), *Risk Governance: Coping with Uncertainty in a Complex World*, Earthscan, London.

Rosqvist, T. and Touominen, R. (2004), "Qualification of Formal Safety Assessment: an exploratory study", *Safety Science*, **42**:99-120.

Rundmo, T., Hestad, H., and Ulleberg, P. (1998), "Organisational factors, safety attitudes and workload among offshore oil personnel", *Safety Science*, **29**(2):75-87.

Senge, P. M. (2006), *The Fifth discipline: the Art & Practice of the Learning Organization*, Doubleday, New York.

SFS (2006:544), *Lagen om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap*, Swedish Code of Statutes.

SFS (2006:637), *Förordning om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap*, Swedish Code of Statutes.

SFS (2006:942), *Förordning om krisberedskap och höjd beredskap*, Swedish Code of Statutes.

Simon, H. (1996), *The Sciences of the Artificial*, The MIT Press, Cambridge, USA.

Simpson, D. M. and Human, R. J. (2008), "Large-scale vulnerability assessments for natural hazards", *Natural Hazards*, **47**:143-155.

SNAO (2008), *Regeringen och krisen - regeringens krishantering och styrning av samhällets beredskap för allvarliga samhällskriser*, Swedish National Audit Office (Riksrevisionen), Stockholm. (In Swedish.)

SOU (2004:134), *Krishantering och civilt försvar i kommuner och landsting*, Swedish Government Official Reports. (In Swedish.)

Stern, P. C. and Fineberg, H. V. (1996), *Understanding risk: informing decisions in a democratic society*, National Academy Press, Washington D.C.

Strömgren, M. and Andersson, R. (2010), "The usage of safety management tools in Swedish municipalities", *Safety Science*, **48**:288-295. (In Swedish.)

UN/OCHA (2008), *Disaster Preparedness for Effective Response: Guidance and Indicator Package for Implementing Priority Five of the Hyogo Framework*, Geneva, United Nations.

van Aken, J. E. (2004), "Management Research Based on the Paradigm of the Design Sciences: The Quest for Field-Tested and Grounded Technological Rules", *Journal of Management Studies*, **41**(2):219-246.

Weber, R. P. (1990), *Basic Content Analysis*, Sage Publications, Newbury Park.

Webler, T., Tuler, S. and Krueger, R. (2001), "What Is a Good Public Participation Process? Five Perspectives from the Public", *Environmental Management*, **27**(3):435-450.

Weick, K. E. and Sutcliffe, K. M. (2001), *Managing the Unexpected: Assuring High Performance in an Age of Complexity*, Jossey-Bass, San Francisco.

VI

Evaluating the seriousness of disasters: an empirical study of preferences

Henrik Hassel*, Henrik Tehler and Marcus Abrahamsson

Department of Fire Safety Engineering and Systems Safety
Lund University
Box 118, 221 00 Lund, Sweden
E-mail: henrik.hassel@brand.lth.se
E-mail: henrik.tehler@brand.lth.se
E-mail: marcus.abrahamsson@brand.lth.se
*Corresponding author

Abstract: In making societal decisions concerning hazards with potentially disastrous consequences, it is important to have sound knowledge of how people evaluate the seriousness of disasters. In this study, a group of students evaluated the seriousness of disasters in terms of four basic attributes (and their ranges): *number of fatalities* (0–1000), *number of serious injuries* (0–4000), *economic loss* (SEK 0–40 billion) and *cause of the disaster* (natural, accidental, terrorism). Attribute weights were elicited by two separate methods, which taken together provide insight into the uncertainty of the elicited weights. Most participants regarded the attributes related to physical harm (especially the number of fatalities) as most serious, a finding that must be seen in relation to the ranges of the attributes. In addition, the *cause of a disaster* also affected many of the participants' judgements of its seriousness. This paper's findings are of value to societal decision making, particularly in the case of small to medium-sized projects in which specific elicitations of stakeholders' values are rarely made.

Keywords: scenario evaluation; disaster seriousness; value elicitation; preferences; emergency management.

Reference to this paper should be made as follows: Hassel, H., Tehler, H. and Abrahamsson, M. (2009) 'Evaluating the seriousness of disasters: an empirical study of preferences', *Int. J. Emergency Management*, Vol. 6, No. 1, pp.33–54.

Biographical notes: Henrik Hassel is a PhD student at the Department of Fire Safety Engineering and Systems Safety of Lund University, Sweden. He has a BSc in Fire Safety Engineering, an MSc in Risk Management and Safety Engineering and a Licentiate of Engineering. His current research interests are the risk and vulnerability analysis of complex sociotechnical systems and value input to decision making in emergency management.

Henrik Tehler is an Assistant Professor at the Department of Fire Safety Engineering and Systems Safety of Lund University, Sweden. He has an MSc in Civil Engineering and a PhD in Fire Safety Engineering. His current research interests concern the development of methods for the risk and vulnerability analysis of complex sociotechnical systems.

Marcus Abrahamsson is a PhD student at the Department of Fire Safety Engineering and Systems Safety of Lund University, Sweden. He has a BSc in Fire Safety Engineering and a Licentiate of Engineering. His current research interests are the development of methods for the risk and vulnerability analysis of complex sociotechnical systems as input to emergency preparedness planning.

1 Introduction

In efforts to reduce the risks of disasters,[1] decision makers often need to consider a wide variety of potentially disastrous events. Their decisions can concern what resources should be allocated to prevent a disaster from occurring, mitigating its effects or preparing for it, as well as what risks and hazards efforts of this sort should address. For such decisions, it is highly important to be able to evaluate effectively the seriousness of potential disaster scenarios that differ in the consequences they involve.

The process of making such decisions consists of a factually-oriented and value-oriented part (von Winterfeldt, 1992; Keeney, 1994). The factual part involves identifying the possible outcomes of different alternatives and estimating the probability of occurrence of each outcome. The accuracy of these estimates depends on the validity of the factual knowledge taken into account. For societal decision making of this sort to be fully rational, the best knowledge available should be used (Webler *et al.*, 1995; Cooksey, 1996); therefore, it is highly desirable to use science and experts as "the providers of facts" (DeKay and McClelland, 1996).

In addition to having adequate knowledge of the facts, a thorough understanding of the value aspects of a decision is essential since values determine what are regarded as positive or negative consequences, a matter emphasised by Keeney, who also pointed out that "values are what we care about" (Keeney, 1992) and that they are "essential for guiding decisionmaking" (Keeney, 1994). However, the values connected with decisions in a risk and disaster context often appear to not be dealt with comprehensively enough or to not be made explicit. This reduces the transparency and quality of such decisions. Thus, there is a need for more thorough knowledge of the values involved. The value and preference elicitation procedures developed within decision analysis (von Winterfeldt and Edwards, 1986) and judgement analysis (Cooksey, 1996) can be useful for obtaining such knowledge.

Although the number of fatalities is factual information often taken as a basis for evaluating the seriousness of a disaster, other attributes can be highly relevant as well. A variety of studies of tradeoffs that people are willing to make between low-probability scenarios (in which there are many fatalities) and high-probability scenarios (in which there are fewer fatalities) and the guidelines for such tradeoffs have previously been carried out (*e.g.*, Keeney, 1980; Slovic *et al.*, 1984; Hubert *et al.*, 1991; Abrahamsson and Johansson, 2006). In addition, various methods or frameworks for evaluating the seriousness of disasters or disaster scenarios characterised by multiple attributes have been suggested (Clement, 1989; Keller *et al.*, 1997; Christen *et al.*, 1994; Guidi *et al.*, 2001). Out of the aforementioned studies, it is only that of Christen *et al.* (1994) in which any systematic elicitation of values was performed to determine the tradeoffs between

different attributes, although it was only an expert panel that served as 'value consultants'. Clearly, more thorough knowledge of how people judge the seriousness of a disaster is needed.

Although there may be many attributes relevant in evaluating the seriousness of a disaster, satisfactory evaluations can often be obtained using only a few of these. For example, it is common that disaster databases such as the EM-DAT[2] makes use of only a few attributes, such as the number of fatalities, number of injuries, economic loss and what the main cause of the disaster was. Regarding the disaster's cause, psychological research "has shown that the causes of harms do affect values" (Kahneman and Ritov, 1994). In line with this, negative environmental consequences are perceived as being more serious when humans are to blame for them than when they are caused by natural events (Kahneman and Ritov, 1994; Walker *et al.*, 1999; Brown *et al.*, 2002; 2005; Bulte *et al.*, 2005). Some of the explanations for this that have been suggested include outrage effects, *i.e.*, the emotional upset induced by knowing that humans are to blame (Kahneman and Ritov, 1994) and the feeling of personal responsibility (Walker *et al.*, 1999). Interestingly, the effects of the cause of an event on the values and preferences associated with it appear not to have been studied to any appreciable extent outside the area of environmental losses. Accordingly, it would be of considerable interest to study the manner and extent to which the judgements of the seriousness of a disaster that gives rise to fatalities and injuries are affected by its apparent cause.

In studies of risk perception such as those of Fischhoff *et al.* (1978), Slovic *et al.* (1980) and Renn (2004) and of risk rankings in the studies of Florig *et al.* (2001), Morgan *et al.* (2001) and Willis *et al.* (2004), risks are characterised in terms of multiple attributes. At the same time, studies of these two types differ in the extent to which facts and values are considered separately. In research on risk perception, the factual and value aspects of risks are often investigated in an integrated way in that people's perception of risks are seen as a function both of their beliefs about reality (beliefs regarding facts) and their values. Research on risk ranking, on the other hand, makes a much clearer distinction between facts and values. Florig *et al.* (2001), for example, proposed a method to elicit people's risk preferences in which the levels of the considered attributes are derived from risk assessments based on scientific literature and expert judgements. Risk summaries are presented to persons who rank the involved risks, allowing the values in question to be derived.

In the present study, the major interest is in the value dimension, as it likewise is in the risk-ranking approach just described. That approach involves judgements under conditions of uncertainty, since the risk rankings are made without knowledge of which possible risk scenario will occur. The present study is different in that it involves judgements under conditions of certainty, since our interest is in assessing the seriousness of a particular risk scenario given that it would occur. Note in this connection that risk assessment in its entirety involves the consideration of the complete set of possible risk scenarios, the probability of each scenario occurring and the negative consequences that its occurrence would have and aggregating these assessments over the risk scenarios as a whole (Kaplan and Garrick, 1981; Kaplan *et al.*, 2001). Our concern here, in contrast, is simply with individual risk scenarios and how serious the consequences of the occurrence of some particular risk scenario would be.

In the investigation carried out here of people's preferences regarding disaster scenarios, the employed attributes are the *number of fatalities*, *number of serious injuries*, *economic loss* and *cause of the disaster*. Two fundamentally different methods are used to elicit these preferences: the first is an indirect and holistic method and the second is a direct method involving the judgements of the relative importance of attributes. This makes it possible to gain a deeper insight into the elicited preferences, such as insights regarding uncertainty of the preferences, since the elicitation procedure always affect the results.

2 Method

2.1 Participants

A group of students enrolled in the Master of Science programme in Risk Management and Safety Engineering or the Bachelor of Science programme in Fire Protection Engineering at Lund University, Sweden, participated in the study. All of them were taking courses at the Department of Fire Safety Engineering of Lund University. The topics covered in these courses were closely related to risk analysis and management. The investigation was presented as an empirical study of relevance to risk management. Emphasising this was seen as increasing the students' readiness to take the tasks seriously. Altogether, participation was voluntary. Approximately 81 persons (22 females and 59 males) between the ages of 18 and 45 (mean of about 23) took part in the study. Three separate testing sessions took place in one year. Two of these sessions involved first-year students and the third involved third-year students.

2.2 Materials

The presented questions and tasks could be completed with a computer interface involving software that the authors developed specifically for this purpose. The participants were given extensive instructions and support with the aim of ensuring the quality and validity of their responses. The instructions given to them prior to the sessions included written information explaining the purpose of the study, the main tasks to be performed and the definitions of the attributes to be employed. Before the participants began with their tasks, they were also provided more specific instructions and persons ready to answer any questions that arose were also available throughout the sessions.

2.3 Overview of the elicitation methods

Many procedures for eliciting people's preferences have been proposed (see Borcherding *et al.*, 1991; Weber and Borcherding, 1993), yet it is not entirely clear which are most appropriate to use in a specific context, partly because of the numerous biases that influence people's judgements and decisions (Tversky and Kahneman, 1981; Hershey *et al.*, 1982; Weber and Borcherding, 1993; von Nitzsch and Weber, 1993; Fischer, 1995; Baron, 1997a). No procedure is free of bias and it is also unclear which procedure is least biased (Weber and Borcherding, 1993). Procedures may differ primarily in the biases they trigger and accordingly, in the preferences they yield (Pitz and Sachs, 1984).

Nevertheless, being aware of how the biases called forth by different procedures may distort the elicited preferences can be seen as a first step towards designing elicitation processes that are able to elicit valid preferences.

A commonly made recommendation is to use more than one procedure to elicit preferences (Payne *et al.*, 1999). This can cast light on the validity as well as the uncertainty of the obtained preferences. To this end, two fundamentally different methods, one indirect and one direct, were used here to elicit preferences. The indirect method is similar to the 'policy-capturing' method described by Cooksey (1996), Aiman-Smith *et al.* (2002) and Karren and Woodard Barringer (2002). This method involves participants being asked to make holistic judgements regarding a set of scenarios, each characterised in terms of multiple attributes. Preferences for the different attributes (or attribute weights) are then derived statistically using multiple regression analysis. In the direct method, on the other hand, preferences for the attributes are elicited by asking participants to make direct judgements of the relative importance of different attributes.

These two methods differ in their advantages and drawbacks. First, the indirect method is more time-consuming and is often perceived as more difficult. Secondly, deriving preferences statistically (as in the indirect method) enables one to gain insight into the consistency of the judgements (indicating the adequacy of a picture of the participants' judgements that the model provides), the cross-validity of the obtained results (how well the model generalises) and the statistical significance of the attribute weights. Finally, the fact that the two methods differ in the biases they are prone to allows one to obtain a more adequate conception of the true weights than either method in itself would provide. The direct method is more prone to range insensitivity (von Nitzsch and Weber, 1993; Fischer, 1995), for example, whereas the indirect method is more prone to prominence effects (Fischer *et al.*, 1999).

It is important that the effects of any known biases and heuristics are limited as much as possible. One example of such an effort was to restrict the number of employed attributes, since human cognitive limitations can result in information overload if too many attributes need to be considered simultaneously (Miller, 1994). Since the indirect method demands that the participants make holistic judgements and take all the attributes into account simultaneously, it was deemed likely that using too many attributes would trigger participants into using heuristics to simplify their judgements, for example, through ignoring less salient (though relevant) attributes (Green and Srinivasan, 1978; Fischer, 1979; Weber and Borcherding, 1993).

2.4 Design of the study

The study was designed so that the individual subject was treated as the unit of analysis, *i.e.*, attribute weights were derived for each person separately. The attributes used to characterise each disaster scenario and its consequences were the number of fatalities, number of serious injuries, economic loss and cause of the disaster. The definitions of these attributes are given in Table 1 and the ranges of each are contained in Table 2. The definitions were presented to the participants in the informative material referred to above and could also be accessed by the computer interface. Since very large monetary values

could be difficult to relate to, a number of monetary sums serving as reference points were presented to the participants, such as the economic losses incurred by a hurricane that occurred in Sweden recently.

Table 1 Definitions of the four attributes used in the survey

Attribute	*Definition*
Number of fatalities	The number of persons who died in or as a result of the disaster. The types of persons involved can be seen as representative of the general Swedish population.
Number of serious injuries	The number of persons requiring acute medical treatment because of the disaster, followed in many cases by long periods of recuperation and possibly lifelong impairment. The types of persons involved can also be seen as representative of the general Swedish population.
Economic loss	The economic loss here is expressed in billions of Swedish kronor. It includes the loss of value in terms of property, equipment, infrastructure, crops and the like, together with indirect loss reduction in private and public revenues, increased unemployment and costs for dealing with the emergency.
Cause of the disaster	This concerns the main cause or causes of the disaster, which can be divided roughly into natural causes and causes of human origin (accidental or intentional).

Table 2 The levels and categories of the four different attributes

	Level or category			
Attribute	*1*	*2*	*3*	*4*
Number of fatalities	0	100	500	1000
Number of serious injuries	0	400	2000	4000
Economic loss[1]	0	4	20	40
Cause of the disaster	Accidental	Terrorism	Natural	–

Note: [1] The economic loss is expressed in billion Swedish kronor.

Each participant was tested in a single session, which consisted of five major steps. Testing was mainly done in groups. In Step 1, the participants were asked to provide personal details such as name,[3] age and gender. Steps 2 and 3 involved the use of the indirect method and Step 4 used the direct method. Employing the indirect method first had this particular advantage: since the participants have to consider the attribute ranges rather explicitly, the awareness of ranges that this creates tends to reduce the range insensitivity bias characteristic of the direct method. In Step 5, the participants filled out a short questionnaire concerning how they perceived the study, how they arrived at their judgements and the like. Parts of the session prior to completing the questionnaire typically took about 30 min to complete.

2.4.1 Indirect method

In the indirect method, the participants made holistic judgements of the seriousness of 24 hypothetical disaster scenarios, described only in terms of the four attributes shown in Table 1. The scenarios were designed using a fractional factorial design in which the attributes could take on levels and categories in accordance with Table 2. The levels and categories were combined orthogonally to minimise the correlations between the attributes, since this provides the most straightforward and statistically stable estimates of the regression coefficients (Cooksey, 1996; Karren and Woodard Barringer, 2002). The scenarios were also constructed in that manner to avoid dominant scenarios, *i.e.*, scenarios having a lower (more undesirable) level on all the attributes compared to the other scenarios involved.

The method was designed so that the judgements made by the participants were comparative rather than absolute, since comparative judgements generally provide result of greater consistency (Brown *et al.*, 2002). Therefore, the indirect method was divided into two separate steps. In the first step, the scenarios were presented in pairs and the participants were asked to indicate which scenario they regarded as the most serious. This procedure continued until a rank ordering of the scenarios could be obtained (usually about 75 pairs of scenarios that were compared were needed).[4] Then, the participants had the opportunity to adjust the ordering of the scenarios if they detected any apparent inconsistencies. In the second step, the most serious scenario was anchored at a score of 100 and the least serious scenario, at a score of 0, with the participants being asked to assign a 'seriousness score' of between 0 and 100 to each of the other scenarios. Furthermore, they were also told that the scores should decrease from the top to the bottom of the list to maintain agreement with their previously expressed choices. Although it was possible for the participants to assign scores that deviated from the rank ordering they had created earlier, they were informed when such deviations occurred.

To reduce the occurrence of any systematic biases in the order in which the attributes were presented, a *between*-participant randomisation was carried out. The reason for not changing the order of presentation of the attributes throughout elicitation for each individual participant was that this would have easily led to confusion. In addition, the order in which the scenarios were compared with each other was randomised both within and between subjects.

2.4.2 Direct method

The employed direct method was similar to the 'Max100 procedure' discussed by Bottomley and Doyle (2001). The four attributes and ranges of possible outcomes that each attribute could take were presented to the participants in a randomly ordered list. The participants were asked to assign an 'importance score' of 100 to the attribute that was the most important one for them in making judgements of the seriousness of a disaster. The participants were then told to assign scores to the other three attributes as well, in such a way that the scores indicated the importance of an attribute in relation to the most important one. The participants were instructed that in making judgements of the importance of an attribute, they must take into account the range of each of the attributes and an example was also presented to clarify why this is the case.

2.5 Analysis of data

2.5.1 Judged seriousness and value functions

For each participant, any judgement made of the seriousness S of a disaster scenario was assumed to conform with the multiattribute additive value model shown in Equation 1:

$$S_j = \sum_{i=1}^{4} w_i \times v_i(x_{ij}), \tag{1}$$

where:

j = specific disaster scenario
w_i = the relative weight of attribute i (the relative weights of the different attributes being normalised to sum to 1)
v_i = the single-attribute value function for attribute i (normalised to range from 0 to 1)
x_{ij} = the level or category of attribute i for scenario j.

It is important to note that throughout the paper, a 'higher' value for S indicates a more serious, less desirable disaster scenario.

The value functions for single attributes v_i were not elicited separately, as is often done in a multi-attribute context. Instead, they were simply assumed or derived from the participant's holistic judgements of the seriousness of the disasters in question (the indirect method). A straightforward assumption for the three quantitative attributes here was that the value functions were strictly positive, meaning that there are larger numbers of fatalities and serious injuries and larger economic losses (everything else being equal) implies that the scenario is more serious. Accordingly, the single-attribute value functions were assumed to be consistent with Equation 2:

$$v_i(x_i) = \left(\frac{(x_i - x_{i,\min})}{(x_{i,\max} - x_{i,\min})} \right)^{z_i}, \tag{2}$$

where:

x_i = the level or category of attribute i
$v_i(x_i)$ = the value of the i-th attribute at level x_i, $x_{i,\min}$
$x_{i,\max}$ = the minimum and maximum level of attribute i
z_i = parameter larger than 0 describing the shape of the single-attribute value function and where $z_i = 1$ implies constant marginal values, $z_i > 1$ stands for increasing marginal values and $0 < z_i < 1$ implies diminishing marginal values.

Converting the categorical attribute *cause of the disaster* into a value function involved applying multiple regression analysis to the participants' holistic judgements of the seriousness of a scenario. The three categories of the *cause of the disaster* were coded using two dummy variables. We arbitrarily chose to consider natural cause as the baseline category, using one dummy variable to code for terrorism (1 if terrorism was the cause and 0 otherwise) and another dummy variable to code for an accident (1 if an accident was the cause and 0 otherwise). Regression coefficients that were estimated on the basis of a linear regression analysis, using the dummies as independent variables, could then be used to derive the value function through Equation 3:

$$v_c = \frac{b_c - b_{c,\min}}{b_{c,\max} - b_{c,\min}}, \tag{3}$$

where:

v_c = the 'value' of category c
b_c = the estimated regression coefficient of the dummy that coded category c (if a natural event was the cause, b_c was set to 0)
$b_{c,\min}$ and $b_{c,\max}$ = the minimum and maximum value of b_c.

2.5.2 Estimates of the relative weights

In the indirect method, the relative weights (w_i in Equation 1) were estimated using the linear multiple regression model, shown in Equation 4:

$$Score_j = \beta_0 + \sum_{i=1}^{4} \beta_i \cdot v_{ij} + \varepsilon_j, \tag{4}$$

where:

$Score_j$ = participant's 'seriousness score' for scenario j
β_0 = y-intercept[5]
β_i = regression coefficient for attribute *i*
v_{ij} = value of attribute *i* in scenario *j*
ε_j = error term for scenario *j*.

In the regression analysis, two assumptions regarding parameter z_i in Equation 2 were tested. First, z_i was assumed to be equal to 1 for each of the attributes, implying constant marginal values. Secondly, transformations of the quantitative attributes were tested by systematically varying the *z*-parameters to find the transformation that provided the best fit to the judgements made by each participant. The *z*-parameters were allowed to take on five levels: 0.3 (strongly marginally diminishing values), 0.7 (slightly marginally diminishing values), 1 (constant marginal values), 1.5 (slightly marginally increasing values) and 2 (strongly marginally increasing values). This involved testing 125 transformations for each participant and the evaluation of the goodness-of-fit of these transformations using the adjusted R^2 (Kutner *et al.*, 2004) as the criterion. Only the transformation with the highest adjusted R^2 was considered further. To obtain the relative weights (w_i in Equation 1) of the four attributes, the estimated regression coefficient b_i obtained from the regression analyses were normalised to sum to one. Thus, for each person, one set of relative weights was obtained in assuming constant marginal values and another set was obtained in relaxing that assumption and allowing for marginally 'changing' values.

Obtaining the relative weights using the direct method was straightforward. The weights were simply obtained by normalising the importance scores the participants provided for the four attributes so that they would sum to one.

3 Results

3.1 Value function for the attribute 'cause of the disaster'

The average values obtained for the three categories based on the separate assessments made for each participant are shown in Table 3. As can be seen, for more than half of the participants, terrorism was the cause considered having the strongest positive effect on the seriousness scores. In addition, the mean of the terrorism category is significantly higher than for natural cause and accidental cause: The results are as follows: Student's *t*-test: $t(160) = 4.65$, $p < 0.0001$ and $t(160) = 3.73$, $p = 0.00027$, respectively. There are also indications of accidental cause receiving, on average, higher seriousness scores than natural cause, though the difference is not statistically significant at $t(160) = 1.29$, $p = 0.20$.

Table 3 Values for the three categories of 'cause of the disaster'

	Percentage of participants involved			
$Cause_c$	$v_c = 1$	$0 < v_c < 1$	$v_c = 0$	$\bar{v}_c$
Natural	23.5	19.8	56.8	0.354
Accidental	21.0	58.0	21.0	0.440
Terrorism	55.6	22.2	22.2	0.680

3.2 Participants' preferences obtained by the indirect method

In the indirect method, the attributes were regressed on the seriousness scores of each participant, the coefficient of multiple determination (R^2) being used to assess how well the derived regression model describes the seriousness score of the sample of scenarios from which the model was derived. Low R^2 values can indicate either that there are marked inconsistencies in the participants' judgements or that a participant's preferences are not adequately described by the assumed regression model. Since R^2 only describes the fit of the model for the scenarios used to derive it, the cross-validated coefficient of multiple determination (R^2_{CV}) was calculated to determine how well the models describe the participants' preferences for the scenarios not included in the sample, but are still within the range of the attributes. This was done by using the 'leave-one-out' (or jack-knifing) procedure described in Cooksey (1996).[6]

3.2.1 Constant marginal values for quantitative attributes

When assuming constant marginal values for quantitative attributes, most participants have R^2 values that are fairly high, with three-fourths of the participants having an R^2 larger than 0.8. The results for a few of them with R^2 values between 0.5 and 0.6 can be considered outliers. The R^2_{CV} values are somewhat lower, of course, but still fairly high, with three-fourths of the participants having values larger than 0.7, suggesting that most of the regression models are reasonably valid for the scenarios not included in the sample from which the models were derived. The participants who could be regarded as outliers on the R^2 criterion can also be regarded as outliers on the R^2_{CV} criterion,

indicating that these participants either gave inconsistent responses or did not have preference models that conformed with the assumed additive value model involving constant marginal values.

In Table 4, the estimated regression coefficients (averaged over the participants) and the fraction of participants whose coefficients were statistically significant at varying levels are presented. The interpretation of the estimated regression coefficients is straightforward since all the attributes were normalised to a range of 0 to 1. The estimated regression coefficient connected to each attribute can, for each person separately, be interpreted as how much the seriousness score is affected when changing the value of the attribute from its most desirable to its least desirable level or category. Overall, the *number of fatalities* is clearly the attribute that has the largest impact on the seriousness scores. Interestingly, the *cause of a disaster* does appear to have an effect on the seriousness scores given by many of the participants, this effect being statistically significant (0.05 level) for almost a third of the participants. The differences between the average estimated regression coefficients are statistically significant ($p < 0.05$) for all pairs of attributes, except that of *economic loss* and *cause of a disaster*, $t(160) = 1.11$, $p = 0.27$.

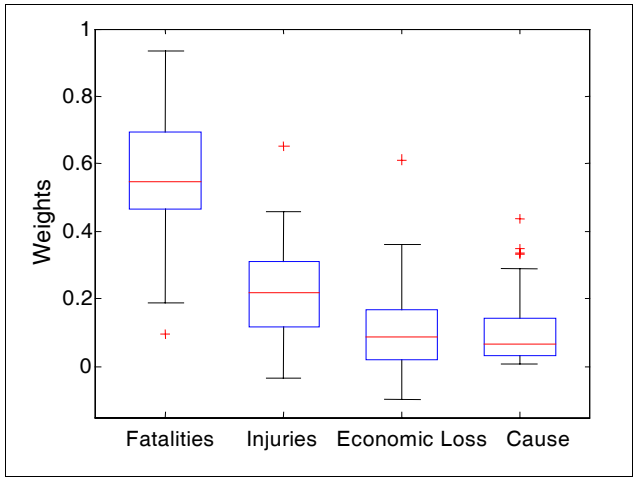
Table 4 Estimated regression coefficients averaged over the participants as a whole and the percentage of participants whose coefficients are statistically significant at the indicated levels, assuming constant marginal values

		Percentage of the participants for which the estimated regression coefficients (b_i) are significant at the indicated level			
Attribute, i	$\overline{b_i}$	*p < 0.1*	*p < 0.05*	*p < 0.01*	*p < 0.001*
Number of fatalities	53.9	98.8	98.8	98.8	96.3
Number of serious injuries	22.3	71.6	66.7	55.6	44.4
Economic loss	11.7	44.4	38.3	27.2	20.0
Cause of a disaster	9.8	34.6	29.6	18.5	14.8

In Figure 1, the distributions of the relative weights are presented for the participants as a whole. One can note that the relative weights vary a great deal among participants, yet if only the ordinal relationships between the relative weights are considered, the results across participants are quite consistent. For over 90% of the participants, the *number of fatalities* has the largest relative weight and either *economic loss* or *cause of a disaster* has the smallest relative weight.

Presenting the relative weights as an indicator of attribute importance has the drawback of its dependence on the range of the respective attributes, which may make interpretation somewhat difficult. To facilitate the interpretation, it is also possible to calculate the size of an increase in the levels of the attributes that have an equal effect on the seriousness scores, *e.g.*, how many additional serious injuries would be needed to increase the seriousness score as much as one additional fatality would do. The median[7] of these calculations, when assuming constant marginal values, is that of one additional fatality having an equal affect as about ten additional serious injuries (as the attribute is defined in Table 1), as well as an additional SEK 140 million (about $20 million) in economic loss.

Figure 1 The distributions of the relative weights obtained using the indirect method for the participants as a whole, assuming constant marginal values (see online version for colours)



3.2.2 *Transformed value functions of the quantitative attributes*

After finding the best transformation for each participant, the transformed value functions were regressed on the seriousness scores using multiple linear regression. The R^2 and R^2_{CV} values for each participant were calculated and both coefficients generally increased considerably when the assumption of constant marginal values was relaxed. For example, three-fourths of the participants have R^2 and R^2_{CV} values larger than 0.9 and 0.83, respectively. This suggests that the use of transformed value functions generally improved the regression models. There were still a couple of outliers involving low R^2 values, two of these from the same participants as when constant marginal values were assumed, implying that they had given rather ambiguous and inconsistent responses or conformed to preference models not accurately captured by a basic additive value model. The R^2 and R^2_{CV} values for the two other participants previously regarded as outliers had increased considerably, suggesting that their preferences can be described much better by using the transformed value functions.

The transformations involving the z-values contained in Equation 2 that provided the best possible fits are shown in Table 5. Only the z-values pertaining to the estimated regression coefficients that were statistically significant ($p < 0.05$) are included there, since if an attribute had no appreciable effect on a participant's judgements of seriousness, which a nonsignificant estimated regression coefficient would imply to be the case, the z-value for the attribute in question would contain no information regarding the shape of its single-attribute value function, but would instead reflect mere coincidence. As can be seen in the table, for most of the participants, the marginal values of both the *number of fatalities* and *number of serious injuries* are diminishing. This suggests that an event resulting in 1000 fatalities, for example, is not considered twice as serious as one resulting in 500 fatalities. Instead, such an event might be perceived, for example, as being 1.5 times as serious (the exact figure depending upon how strongly diminishing the marginal value is). The marginal values for *economic loss*,

on the other hand, are more varied across the participants. For over a third of the participants, they can in fact be classified as increasing. A possible explanation for this is that some participants only took account of this attribute when its level exceeded a certain threshold value which the assumed single-attribute value model (Equation 2) is not able to accurately capture.

Table 5 Best-fitted transformations of the quantitative attributes for participants as a whole

	Percentages of the participants for whom the marginal values of the best possible transformations were as follows:				
Attribute, i	*Strongly diminishing*[a]	*Slightly diminishing*[b]	*Constant*[c]	*Slightly increasing*[d]	*Strongly increasing*[e]
Number of fatalities	53.1	43.2	3.7	0	0
Number of serious injuries	33.3	55.1	10.3	0	1.3
Economic loss	14.3	24.5	22.4	8.2	30.6

Notes: [a] $z = 0.3$ [b] $z = 0.7$ [c] $z = 1$ [d] $z = 1.5$ [e] $z = 2$.

The estimated regression coefficients (averaged over the participants as a whole) and the percentages of participants whose coefficients were statistically significant at different levels are shown in Table 6. The distribution of the relative weights for all participants is presented in Figure 2. These results are very similar to the results obtained when assuming constant marginal values; however, the significance of the estimated regression coefficients have increased considerably. This especially applies to the *number of serious injuries*, where the estimated regression coefficient is now statistically significant at the 0.05 level for over 95% of the participants (in comparison to only about 65% when assuming constant marginal values).

Table 6 Estimated regression coefficients averaged over the participants as a whole and the percentages of the participants whose coefficients were statistically significant at the referred levels using transformed value functions

		Percentage of the participants for whom the estimated regression coefficients (b_i) were significant at the p-level			
Attribute, i	$\overline{b_i}$	$p < 0.1$	$p < 0.05$	$p < 0.01$	$p < 0.001$
Number of fatalities	58.9	100	100	98.8	98.8
Number of serious injuries	28.9	96.3	96.3	90.1	82.7
Economic loss	13.4	64.2	60.5	49.4	34.6
Cause of a disaster	9.7	48.1	38.3	29.6	22.2

3.3 Participants' preferences obtained by using the direct method

The distributions of relative weights obtained by using the direct method for the participants as a whole are presented in Figure 3. As can be seen there, the *number of fatalities* was generally regarded as the most important attribute, followed by the *number of serious injuries*, there being more than 90% of the participants who judged the *number of fatalities* to be the most important attribute (keeping in mind that attribute

importance is an effect of both the attribute *per se* and the ranges of the attributes). The least important attribute for most participants appears to be either *economic loss* or *cause of a disaster*. The relative weight for *cause of a disaster* appears to vary across participants more than the other attributes do, which is the opposite of what was found using the indirect method.

Figure 2 The relative weights based on the transformed value functions using the indirect method (see online version for colours)

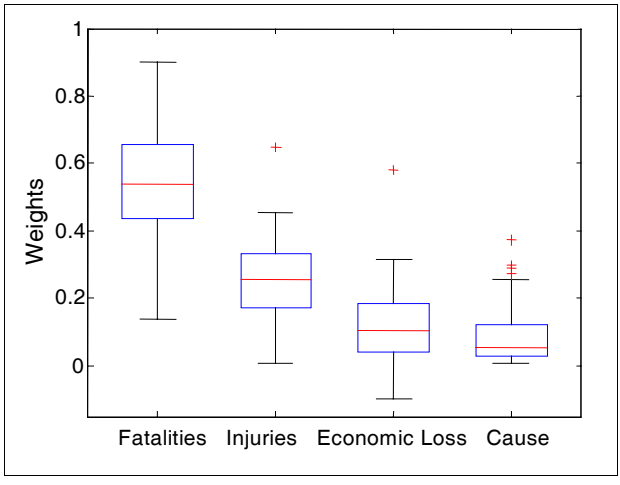
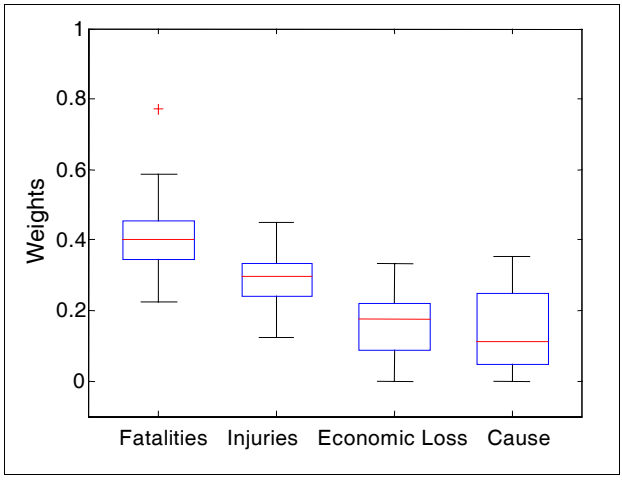


Figure 3 The distributions of relative weights obtained using the direct method (see online version for colours)



Based on the median of the relative weights obtained by using the direct method and assuming constant marginal values, one additional fatality would have an equal effect on the seriousness score as five additional serious injuries (as the attribute is defined in Table 1), as well as an additional SEK 100 million (about $14 million) in economic loss.

3.4 Comparison of the results obtained by using the two different methods

The relative weights that the two different methods provide are summarised in Table 7. As can be seen, on average, both methods provide the same rank ordering of the relative importance of the four attributes. The main difference between the results of the two methods is that the distribution of weights from the direct method is flatter, the difference between the largest and smallest weight there being less. This difference can be clearly seen in Table 7 or by comparing either Figure 1 or Figure 2 with Figure 3. The difference obtained in comparing the average difference between the largest and smallest weight that the indirect method provides (with the transformed value functions) and that provided by the direct method is also statistically significant, $t(160) = 6.81$, $p < 0.001$.

Table 7 Summary of the average relative weights obtained with the two different methods

Attributes	*Indirect method*		*Direct method*
	Constant values	*Transformed values*	
Number of fatalities	0.551	0.531	0.400
Number of serious injuries	0.228	0.261	0.320
Economic loss	0.120	0.121	0.160
Cause of a disaster	0.100	0.087	0.120

The results obtained with the two methods can also be compared by calculating the judged seriousness (Equation 1) of different disaster scenarios using the relative weights that the two methods provide and then correlating the respective scores obtained. This is a way to check the convergent validity of the two methods and thereby enable a more reliable conclusion to be drawn about the attribute weights. This was done by calculating the judged seriousness of 1000 random scenarios (involving random values for each of the quantitative attributes and a randomly chosen category for *cause of a disaster*) using the relative weights obtained for the transformed value functions in the indirect method. The sets of scores obtained were then correlated for each participant separately using Pearson's correlation coefficient. The correlations between the results obtained from the two methods are generally quite high. The median is almost 0.9 and only 5% of the participants have correlations lower than 0.83. This suggests a high consistency which, in turn, supports the validity of the weights obtained in the study and the judged seriousness that these weights imply.

4 Discussion

Although it was found, as expected, that the attributes related to physical harm (especially the *number of fatalities*) were regarded as being the most important (keeping the ranges of the attributes in mind), it was also shown that the cause of a disaster can affect judgements of its seriousness. This raises questions in connection with the use of utility theory as a normative basis for decisions, often being applied in terms of teleological decision rules, *i.e.*, that decisions should depend only on the consequences of available decision alternatives. We found, on the other hand, the attribute weights assigned to the *cause of a disaster* to indicate that for many of the participants, this could

be a factor influencing the seriousness of the disaster, implying that they use deontological decision rules as well. This is also supported by the fact that several participants explicitly stated in the questionnaire that the cause of the disaster affected their judgements. Previous research has also found that people may use deontological rules in making judgements. One example of such a rule is the "omission bias", which is "the tendency to be less concerned with harms caused by omission than with identical harms caused by action" (Ritov and Baron, 1999). Similarly, in a study of preferences for environmental losses, it was found that "judgments of seriousness appear to reflect not only the magnitude of the loss but also the reason for the loss" (Brown *et al.*, 2002).

However, drawing the conclusion that the participants in the present study use deontological rules is not unproblematic. In the questionnaire given at the end of the session, many of the subjects commented that they incorporated considerations other than the undesirability of the *specified* consequences into their judgements of the seriousness of a disaster. The comments provided by the participants implied the following:

- natural events are perceived as less serious because of a *belief* that it is difficult to prevent such events
- events that are impossible to prevent are perceived as more *acceptable* and, therefore, also less serious
- events caused by a malicious intent (*e.g.*, terrorist attacks) are perceived as more serious
- events wherein there is someone to blame, more prominent in connection with intentional and accidental events, are perceived as more serious
- terrorist attacks are perceived as more serious since successful attacks could encourage other terrorists to commit future acts of terrorism.

These comments imply that some persons made factual inferences that may have 'contaminated' the elicited preferences concerning disaster seriousness. For example, several participants appeared to assume that natural disastrous events and their consequences were impossible or at least very difficult to prevent and, therefore, perceived such events as less serious. Although these factual inferences may have some validity, it is clearly not the case that all natural events *and* their consequences are impossible to prevent or mitigate. Another example is that the participants may have inferred higher-order consequences based on the information given in the scenario descriptions, such as inferring that a successful terrorist attack may lead to increased border control, increased airport security and social tensions and also constitute a signal for future attacks. Scenario evaluations based on such factual inferences can be misleading.

Furthermore, even if the factual inferences would be valid, it is doubtful whether preventability, manageability, *etc.*, actually ought to affect the judgements of disaster *seriousness per se*. Is it really appropriate to, for example, assign a lower seriousness score to a scenario involving a large number of fatalities but where the countermeasures are extremely expensive compared to scenarios where countermeasures are relatively cheap, everything else being equal? Issues concerning manageability, *etc.*, would of course be a part of the decision-making process since in deciding which risk-reducing measures should be taken, a cheap measure would be preferable because it will entail a higher cost-effectiveness (given the same effect on the risk). When using

elicited preferences as prescriptive inputs to decision making, it is, therefore, highly important to consider whether these preferences may have been affected by unwanted considerations, such as by erroneous inferences about what is factually correct or that factors that should not really affect seriousness judgements have been taken into account. Further research concerning the extent to which the cause of a disaster affects its perceived seriousness is needed.

For most participants, the single-attribute value functions for the best transformations both for the obtained *number of fatalities* and *number of injuries* were marginally diminishing. This could involve, for example, an event that resulted in 1000 fatalities being regarded as *less* than twice as serious as an event that resulted in 500 fatalities. In an empirical study of people's preferences for the *number of fatalities*, Abrahamsson and Johansson (2006) obtained *utility* functions that were marginally diminishing, indicating the subjects to have shown risk-prone attitudes. These results are in line with prospect theory, which states that people tend to show a risk-prone behaviour concerning decisions that involve losses (Kahneman and Tversky, 1979). Keeney (1980) argued that the addition to the societal impact of a disaster which an additional fatality produces should decrease when the overall number of fatalities increases; this likewise implying risk proneness. Since a person's utility function is a combination of the "strength of preference he feels for the consequences" (his value function) and "his attitude towards risk taking" (Dyer and Sarin, 1982), it is possible that the shape of the utility functions that Johansson and Abrahamsson obtained and Keeney argued for is more an effect of people's strength of preference for different levels of the *number of fatalities* than their attitudes towards risk taking *per se*. People's relative risk attitude, as defined by Dyer and Sarin (1982),[8] towards the *number of fatalities* might then actually be neutral or even averse.

A question that arises in relation to the previous paragraph is whether marginally diminishing value functions are appropriate to use in evaluating the *number of fatalities* and *number of injuries* in societal decision making. What complicates matters and makes straightforward application of the elicited value functions difficult is the phenomenon of 'diminishing sensitivity' (also termed 'psychophysical numbing'). Research on this phenomenon has shown that an intervention to save lives is valued more when few lives are at risk rather than many, even if the absolute number of lives saved is the same in both cases (Fetherstonhaugh *et al.*, 1997). This can be explained by people who often seem to confuse relative and absolute quantities (Baron, 1997b) so that a proportionally large difference (*e.g.*, the difference between 1000 and 2000 fatalities) is perceived as being larger than a proportionally small difference (*e.g.*, the difference between 49 000 and 50 000 fatalities), also in an absolute sense. Diminishing sensitivity, applied to the problem studied in the present investigation, implies that an additional fatality is perceived as having a decreasing impact on the seriousness of a disaster as the number of fatalities increases, since this means that an additional fatality constitutes a smaller and smaller proportional difference. The problems connected with using the elicited value functions as prescriptive inputs to decision making have to do with these possibly being effects of human cognitive biases rather than a representation of the underlying values. Further research is needed to obtain a better understanding of the effects of diminishing sensitivity on people's judgements of the seriousness of a disaster.

Using more than one method to elicit attribute weights is a way to check the validity of the obtained weights. In this study, it was found that the weights obtained by the two methods differed in that the variability of the weights was significantly larger for indirect/holistic elicitation compared to direct elicitation. These findings are in line with studies that compared methods requiring holistic judgements and those requiring direct judgements of attribute importance (Weber and Borcherding, 1993; Baron, 1997a). The studies have found that since methods that require holistic judgements focus on alternatives and scenarios as a whole which are characterised by multiple attributes, the subjects tend to reduce the complexity of the judgements by overly concentrating on the most salient attributes (the *number of fatalities* in the present case), which leads to an unduly steep distribution of weights (Weber and Borcherding, 1993). In the direct elicitation of weights, on the other hand, subjects tend to spread the weights they assign too evenly, which results in a distribution of weights which is too flat. If both these matters are true, one could conclude that the 'correct' weights should lie somewhere between the weights elicited by the two methods. Furthermore, the two sets of weights obtained from the two methods can also be seen as indicating the degree of uncertainty present in the value judgements arrived at. Explicitly modelling this uncertainty in the decision-making process enables adequate conclusions to be drawn regarding the effect of these uncertainties on the decision.

The two methods were shown to have both strengths and weaknesses. The indirect method was found to be more time-consuming and more difficult. However, the indirect method allows certain information about the participants' preferences to be obtained that the direct method is unable to provide. First, the indirect method provides information about the consistency of the participants' responses, enabling the participants who gave highly inconsistent responses to be identified and the reasons for such an inconsistency to be sought. The participants can then be screened for further analysis if their inconsistencies are believed to stem from their being unfocused in performing tasks or their not taking the tasks seriously. Secondly, the indirect method provides information concerning the statistical significance of the obtained attributes, which allows conclusions regarding the confidence one can have in the relative weights to be drawn. The indirect method also provides information on the shapes of single-attribute value functions. Thus, overall, the indirect method gives more informative results; however, although using a single method to elicit values can provide valuable results, we would recommend that one should, if possible, utilise several different methods, since this can enable one to gain a deeper insight into people's preferences.

The types of preferences that were elicited here, which aim to be generic rather than specific to a particular decision, are especially applicable in small to medium-sized projects. This is because in such projects, unlike large-scale projects, value elicitations are rarely conducted on the population of interest due to budget constraints. It is nevertheless very important to take the value aspect of a decision into account. This can be done by using generic-type weights. Although the number of participants was somewhat limited and represented a rather homogeneous group, we argue that the principal findings of this study can be of value to societal decision making in this area. To gain a more adequate understanding of the values and preferences of the general public in such matters and check the generalisability of the obtained results, studies of other groups and involving other relevant attributes and ranges of attribute values are needed.

Eliciting values is not an easy task due to the vast number of methodological considerations and different types of biases that are, to a varying degree, inherent in all available techniques. However, we agree with Payne *et al.* (1992), who argued that the alternative of using some kind of intuitive approach or implicitly assuming weights is less appealing than using value elicitation methods, despite their being biased. The way forward, as we see it, is to do one's best to limit biases and elicit values as accurately as possible. Further studies of the basic type carried out here are clearly needed to gain a better understanding of people's preferences regarding potential disaster scenarios.

References

Abrahamsson, M. and Johansson, H. (2006) 'Risk preferences regarding multiple fatalities and some implications for societal decision making – an empirical study', *Journal of Risk Research*, Vol. 9, No. 7, pp.703–715.

Aiman-Smith, L., Scullen, S.E. and Barr, S.H. (2002) 'Conducting studies of decision making in organizational contexts: a tutorial for policy-capturing and other regression-based techniques', *Organizational Research Methods*, Vol. 5, No. 4, pp.388–414.

Baron, J. (1997a) 'Biases in the quantitative measurement of values for public decisions', *Psychological Bulletin*, Vol. 122, No. 1, pp.72–88.

Baron, J. (1997b) 'Confusion of relative and absolute risk in valuation', *Journal of Risk and Uncertainty*, Vol. 14, pp.301–309.

Borcherding, K., Eppel, T. and von Winterfeldt, D. (1991) 'Comparison of weighting judgments in multiattribute utility measurement', *Management Science*, Vol. 37, No. 12, pp.1603–1619.

Bottomley, P.A. and Doyle, J.R. (2001) 'A comparison of three weight elicitation methods: good better, and the best', *Omega*, Vol. 29, pp.553–560.

Brown, T.C., Nannini, D., Gorter, R.B., Bell, P.A. and Peterson, G.L. (2002) 'Judged seriousness of environmental losses: reliability and cause of loss', *Ecological Economics*, Vol. 42, pp.479–491.

Brown, T.C., Peterson, G.L., Brodersen, R.M., Ford, V. and Bell, P.A. (2005) 'The judged seriousness of an environmental loss is a matter of what caused it', *Journal of Environmental Psychology*', Vol. 25, pp.13–21.

Bulte, E., Gerking, S., List, J.A. and de Zeeuw, A. (2005) 'The effect of varying the causes of environmental problems on stated WTP values: evidence from a field study', *Journal of Environmental Economics and Management*, Vol. 49, pp.330–342.

Christen, P., Bohnenblust, H. and Seitz, S. (1994) 'A methodology for assessing catastrophic damage to the population and environment: a quantitative multi-attribute approach for risk analysis based on fuzzy set theory', *Process Safety Progress*, Vol. 13, No. 4, pp.234–238.

Clement, C.F. (1989) 'The characteristics of risks of major disasters', *Proceedings of the Royal Society of London*, Vol. 424, pp.439–459.

Cooksey, R.W. (1996) *Judgment Analysis: Theory, Methods, and Applications*, San Diego: Academia Press.

Coppola, D.P. (2007) *Introduction to International Disaster Management*, Amsterdam: Elsevier.

DeKay, M.L. and McClelland, G.H. (1996) 'Probability and utility components of endangered species preservation programs', *Journal of Experimental Psychology: Applied*, Vol. 2, No. 1, pp.60–83.

Dyer, J.S. and Sarin, R.K. (1982) 'Relative risk aversion', *Management Science*, Vol. 28, No. 8, pp.875–886.

Fetherstonhaugh, D., Slovic, P., Johnson, S.M. and Friedrich, J. (1997) 'Insensitivity to the value of human life: a study of psychophysical numbing', *Journal of Risk and Uncertainty*, Vol. 14, pp.283–300.

Fischer, G.W. (1979) 'Utility models for multiple objective decisions: do they accurately represent human preferences?', *Decision Sciences*, Vol. 10, No. 3, pp.451–479.

Fischer, G.W. (1995) 'Range sensitivity of attribute weights in multiattribute value models', *Organizational Behaviour and Human Decision Processes*, Vol. 62, No. 3, pp.252–266.

Fischer, G.W., Carmon, Z., Ariely, D. and Zimmerman, G. (1999) 'Goal-based construction of preferences: task goals and the prominence effect', *Management Science*, Vol. 45, No. 8, pp.1057–1075.

Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S. and Combs, B. (1978) 'How safe is safe enough? A psychometric study of attitudes toward technological risk and benefits', *Policy Sciences*, Vol. 9, pp.127–152.

Florig, H.K., Morgan, M.G., Morgan, K.M., Jenni, K.E., Fischhoff, B., Fischbeck, P.S. and DeKay, M.L. (2001) 'A deliberative method for ranking risks (I): overview and test bed development', *Risk Analysis*, Vol. 21, No. 5, pp.913–921.

Green, P.E. and Srinivasan, V. (1978) 'Conjoint analysis in consumer research: issues and outlook', *The Journal of Consumer Research*, Vol. 5, No. 2, pp.103–123.

Guidi, G., Ludovisi, G. and Mazzarotta, B. (2001) 'Methodological approach for the evaluation, in economic terms, of the risk from industrial plants subject to council directive 96/82/EC (Seveso II)', *ESREL International Conference*, Torino, Italy, 16–20 September.

Hershey, J.C., Kunreuther, H.C. and Schoemaker, P.J.H. (1982) 'Sources of bias in assessment procedures for utility functions', *Management Science*, Vol. 28, No. 8, pp.936–954.

Hubert, P., Barny, M.H. and Moatti, J.P. (1991) 'Elicitation of decision-makers' preferences for management of major hazards', *Risk Analysis*, Vol. 11, No. 2, pp.199–206.

Kahneman, D. and Ritov, I. (1994) 'Determinants of stated willingness to pay for public goods: a study of the headline method', *Journal of Risk and Uncertainty*, Vol. 9, pp.5–38.

Kahneman, D. and Tversky, A. (1979) 'Prospect theory: an analysis of decisions under risk', *Econometria*, Vol. 47, No. 2, pp.263–292.

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

Kaplan, S., Haimes, Y.Y. and Garrick, B.J. (2001) 'Fitting hierarchical holographic modeling into the theory of scenario structuring and a resulting refinement to the quantitative definition of risk', *Risk Analysis*, Vol. 21, No. 5, pp.807–819.

Karren, R.J. and Woodard Barringer, M. (2002) 'A review and analysis of the policy-capturing methodology in organizational research: guidelines for research and practice', *Organizational Research Methods*, Vol. 5, No. 4, pp.337–361.

Keeney, R.L. (1980) 'Evaluating alternatives involving potential fatalities', *Operations Research*, Vol. 28, No. 1, pp.188–205.

Keeney, R.L. (1992) *Value-Focused Thinking, A Path to Creative Decisionmaking*, Cambridge: Harvard University Press.

Keeney, R.L. (1994) 'Using values in operations research', *Operations Research*, Vol. 42, No. 5, pp.793–813.

Keller, A.Z., Meniconi, M., Al-Shammari, I. and Cassidy, K. (1997) 'Analysis of fatality, injury, evacuation and cost data using the Bradford disaster scale', *Disaster Prevention and Management*, Vol. 6, No. 1, pp.33–42.

Kutner, M.H., Nachtsheim, C.J. and Neter, J. (2004) *Applied Linear Regression Models*, New York: McGraw-Hill.

Miller, A.M. (1994) 'The magical number seven, plus or minus two: some limits on our capacity for processing information', *Psychological Review*, Vol. 101, No. 2, pp.343–352.

Morgan, K.M., DeKay, M.L., Fischbeck, P.S., Morgan, M.G., Fischhoff, B. and Florig, H.K. (2001) 'A deliberative method for ranking risks (ii): evaluation of validity and agreement among risk managers', *Risk Analysis*, Vol. 21, No. 5, pp.923–937.

Payne, J.W., Bettman, J.R. and Johnson, E.J. (1992) 'Behavioral decision research: a constructive processing approach', *Annual Reviews Psychology*, Vol. 43, pp.87–131.

Payne, J.W., Bettman, J.R. and Schkade, D.A. (1999) 'Measuring constructed preferences: towards a building code', *Journal of Risk and Uncertainty*, Vol. 19, Nos. 1–3, pp.243–270.

Pitz, G.F. and Sachs, N.J. (1984) 'Judgment and decision – theory and application', *Annual Review of Psychology*, Vol. 35, pp.139–163.

Renn, O. (2004) 'Perceptions of risks', *Toxicology Letters*, Vol. 149, pp.405–413.

Ritov, I. and Baron, J. (1999) 'Protected values and omission bias', *Organizational Behaviour and Human Decision Processes*, Vol. 79, No. 2, pp.79–94.

Slovic, P., Fischhoff, B. and Lichtenstein, S. (1980) 'Facts and fears: understanding perceived risk', in W.A. Albers Jr. (Ed.) *Societal Risk Assessment: How Safe is Safe Enough?*, New York: Plenum.

Slovic, P., Lichtenstein, S. and Fischhoff, B. (1984) 'Modeling the societal impact of fatal accidents', *Management Science*, Vol. 30, No. 4, pp.464–474.

Tversky, A. and Kahneman, D. (1981) 'The framing of decisions and the psychology of choice', *Science*, Vol. 211, No. 4481, pp.453–458.

Von Nitzsch, R. and Weber, M. (1993) 'The effect of attribute range on weights in multiattribute utility measurements', *Management Science*, Vol. 39, No. 8, pp.937–943.

Von Winterfeldt, D. (1992) 'Expert knowledge and public values in risk management: the role of decision analysis', in S. Krimsky and D. Golding (Eds.) *Social Theories of Risk*, Praeger, Westport Publishers.

Von Winterfeldt, D. and Edwards, W. (1986) *Decision Analysis and Behavioral Research*, Cambridge: Cambridge University Press.

Walker, M.E., Morera, O.F., Vining, J. and Orland, B. (1999) 'Disparate WTA-WTP disparities: the influences of human versus natural causes', *Journal of Behavioral Decision Making*, Vol. 12, pp.219–232.

Weber, M. and Borcherding, K. (1993) 'Behavioral influences on weight judgments in multiattribute decision making', *European Journal of Operational Research*, Vol. 67, pp.1–12.

Webler, T., Rakel, H., Renn, O. and Johnson, B. (1995) 'Eliciting and classifying concerns: a methodological critique', *Risk Analysis*, Vol. 15, No. 3, pp.421–436.

Willis, H.H., DeKay, M.L., Morgan, M.G., Florig, H.K. and Fischbeck, P. (2004) 'Ecological risk ranking: development and evaluation of a method for improving public participation in environmental decision making', *Risk Analysis*, Vol. 24, No. 2, pp.363–378.

Notes

1 Although there are numerous definitions of the disaster concept, many suggest that a disaster can be defined as an event that exceeds the coping capacity of an affected society due to widespread damage to human life, economic and environmental damages and serious disruption in the function of society (*e.g.*, Coppola, 2007).

2 EM-DAT is a database of disaster events maintained by the Centre for Research on the Epidemiology of Disasters (CRED), located at the Catholic University of Leuven.

3 Participants had an option to remain anonymous.

4 Requiring participants to make a large number of judgements may incur fatigue, which may distort the elicited preferences. When asked to which extent the participants were able to keep their concentration throughout the whole study, 58% said they were able to keep

their concentration fully or almost fully, 28% said they could keep their concentration moderately and the remaining participants had some to large difficulties in keeping their concentration. Although not ideal, in most cases, the effect of fatigue is believed to be acceptable. Of course, it would be possible to exclude data from participants who were not able to maintain their concentration.

5 Since we were only concerned with the relative importance of the four attributes, the y-intercept was of no interest in this study.

6 In this approach, a regression model is derived from all the scenarios except one, the model thus derived being used to predict the score of the excluded scenario. This procedure is employed repeatedly, one case being withheld and the residual obtained from the prediction being recorded in each case. A cross-validated coefficient of determination is finally computed as 1-PRESS/TSS, the Prediction Error Sum of Squares being abbreviated to PRESS and the Total Sum of Squares, TSS.

7 The median was chosen since some of the derived weights were very close to zero, which would have distorted the result if the average substitution rate had been calculated.

8 A relative risk attitude is defined as a person's risk attitude relative to the strength of his/her preferences. A person whose value and utility functions are identical, for example, has a relatively risk-neutral attitude.