LUND UNIVERSITY

Risk and Vulnerability Analysis of Complex Systems: a basis for proactive emergency management

Hassel, Henrik

2007

Risk and Vulnerability Analysis of Complex Systems

a basis for proactive emergency management

Henrik Jönsson

LUND UNIVERSITY

Licentiate thesis

Department of Fire Safety Engineering and Systems Safety
Faculty of Engineering

Lund 2007

Risk and Vulnerability Analysis of Complex Systems: a basis for proactive emergency management
Henrik Jönsson

Report 1038
ISSN: 1402-3504
ISRN: LUTVDG/TVBB-1038--SE

ISBN: 978-91-633-1614-2

Number of pages: 194
Illustrations and figures: Henrik Jönsson

Keywords: Risk and vulnerability analysis, complex systems, large-scale technical infrastructures, values, emergency response capabilities, operational definitions.

Sökord: Risk- och sårbarhetsanalys, komplexa system, storskaliga tekniska infrastrukturer, värderingar, krishanteringsförmåga, operationella definitioner.

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

Abstract

The present thesis concerns methods and knowledge that are useful when analysing the risks and vulnerabilities of complex systems in a societal emergency management context. Operational definitions of vulnerability and emergency response capabilities are suggested and two methods for analysing the vulnerability of critical infrastructure networks, based on the suggested definition, are presented. An empirical study of people's values and preferences regarding different attributes of potential disaster scenarios is also presented, since knowledge about values also is crucial for adequate risk and emergency management. It is concluded that the thesis provides important insight into some of the issues related to analysis of risks and vulnerabilities of complex systems, but that more research is needed to address this difficult and comprehensive task.

Acknowledgements

Almost three years have passed since I took my first explorative step into the world of risk and vulnerability research. Many are the people that have crossed my path on this journey and many are the persons that I owe the deepest debt of gratitude for their support. If it was not for them, I would definitively not have managed to write this thesis. When looking at the list of publications it is obvious that the research I have conducted is not a result of a single person – it is a result of team-work. Team-work does not only provide research with a higher degree of quality – it is so much more fun too! The ones I've had the pleasure of working closely together with is not merely my colleagues, they are also my friends. I would especially like to thank my three co-authors. Henrik Johansson: thank you for all your input, support and inspiration. I cannot imagine how I would have come as far as I have without your efforts. I hope I can repay the debt I feel somehow. Jonas Johansson: thank you for the great exchange and the fun (sometimes also frustrating) times we have had while writing our papers and developing the Matlab computer code. You have taught me so much about the complex world of electrical engineering and I hope I have given you a glimpse of the mysterious field of risk. Marcus Abrahamsson: thank you for our interesting and fruitful discussions. It is always a pleasure to work with you. I hope that the four of us will continue to develop the ideas and thoughts we have together.

I would also like to thank my supervisor, Professor Kurt Petersen, for his great feed-back and valuable comments on my papers and thesis. In having you as a source of knowledge and support I am positive that I will manage to get my PhD as well. Furthermore, I would thank all my co-workers at the Department of Fire Safety Engineering and Systems Safety. You make it fun to come to work each day! I also feel gratitude to all the people in, or in close proximity to, the FRIVA-group. The discussions we have always provide me with new perspectives and inputs.

The Swedish Emergency Management Agency (KBM) has financed this research. I hope we have transformed and will continue to transform these resources into a useful outcome of high quality.

Finally, I would also like to thank my family and friends – especially my "soon-to-be-wife" Rima. Without your support I would never have come this far – I love you! I hope you can endure another 2-2.5 years!

Lund, October 17, 2007
Henrik Jönsson

Summary

Today, the modern society is exposed to an array of hazards and threats that potentially can cause widespread damages and great losses to human values, such as damage to life and health, environmental damage and economic loss. These hazards include old ones, such as several natural phenomena, but also new and emerging ones, such as those stemming from technological development, globalisation, increased complexity of technological systems etc. When these hazards materialise, an emergency situation can arise where various needs, such as people's needs of medical care or food, have to be satisfied in a timely manner in order to avoid or reduce negative consequences. Many of the systems that are relevant here can be described as complex. The complexity stems from the fact that these systems consist of many factors and variables that interact in many different ways, and also from the fact that human actions are crucial for how the emergencies evolve. Due to this complexity and the large human values that are at stake, the risks in a society should be addressed proactively in a formal risk management framework.

One component of such a proactive risk management framework is to conduct risk and vulnerability analyses. In order to conduct appropriate risk and vulnerability analyses these should be based on methods that are appropriate for the purpose of a particular analysis. The present thesis, therefore, concerns developing methods and knowledge that can be useful when an actor is analysing risk and vulnerability in a societal emergency management context.

Two main classes of systems are of interest here; critical infrastructure networks and emergency response actors. Critical infrastructures play at least two important roles in emergencies. First, they can be the source of an emergency due to the fact that a disruption in the services of a critical infrastructure may lead to severe consequences for all systems that depend on them. Secondly, they can be critical for the response to an emergency, which has arisen due to another perturbation. A disruption of the services may severely hamper the emergency response. Furthermore, emergency response actors also play very important roles in emergencies, since they initiate a response in order to meet the needs that arise and thereby are able to reduce the negative consequences of the emergency. Examples of emergency response actors are the fire and rescue services, governmental agencies, NGOs and so on. The emergency response capabilities of these actors are what determine how well the needs can be met.

A good point of departure when developing methods, when evaluating methods, or when conducting analyses, is to base such work on operational definitions of the concepts of interest. An operational definition is roughly a definition that provides

an ideal procedure for how to measure or characterise a concept. Since many of the concepts in the present area of interest are quite vague, operational definitions can be very useful. In the research field, a commonly used operational definition of risk exists; however, no operational definition of vulnerability seems to exist, although this concept is common in the field. In the present thesis an operational definition of vulnerability is therefore suggested, which builds on the definition of risk. Vulnerability, then, can be seen as the answer to three questions: What can happen, given a specific perturbation? How likely is it, given that perturbation? If it does happen, what are the consequences?

In the present thesis, methods for analysing the vulnerability of critical infrastructure networks are suggested, which builds on the operational definition of vulnerability. Furthermore, the methods also build on previous research from the area of network analysis. It is argued that network analysis along with the suggested operational definition provide a good way of structuring the analysis of many large-scale and complex infrastructure system. Furthermore, the suggested methods have two different foci. The first method focus on the overall vulnerability of a system to a specific perturbation – here termed global vulnerability. The second method focus on identifying components that are critical, i.e. on local properties of systems. It is argued that these two perspectives complement each other.

An operational definition of emergency response capabilities is also suggested here, which emphasizes three main points. First, that capability needs to be related to specific tasks or activities, since what matters in an emergency is what different actors are doing. Secondly, concrete measures of how to determine what constitute a task being well performed need to be defined. Thirdly, how well an actor can perform a task depends on the context, such as which resources that are available, how other actors performs their tasks and so on. It is concluded that this definition can provide an analytic framework for studying emergency response capabilities.

In addition to appropriate methods for analysing risk and vulnerability in order to provide factual input to decisions, there is also a need for value-inputs. Values and preferences determine what should be counted as harm. Knowledge about values therefore needs to exist in order to know which variables are interesting to study in risk and vulnerability analyses, and also in order to evaluate risks or deciding on which risk reducing measures should be implemented. In the present thesis, therefore, an empirical study has been conducted which sought to elicit values and preferences regarding how people make trade-offs between different attributes of potential disaster scenarios. It is concluded that this study can provide important information to the risk management process, but that it needs to be complemented with other studies in order to investigate the generalizability of the results.

The overall conclusion of the present thesis is that there are great difficulties of analysing the risk and vulnerability of complex systems, such as the systems that are relevant from a societal emergency management perspective. The work presented here provides insight into some of the relevant issues, but more research is needed before risks and vulnerabilities can be analyses appropriately from a holistic perspective.

Sammanfattning (summary in Swedish)

Dagens moderna samhälle är exponerat för en rad olika hot och riskkällor. Många av dessa kan potentiellt leda till stora skador på sådant som människor värdesätter, såsom skador på människors hälsa, miljöskador och ekonomiska skador. Dessa hot är dels gamla hot, såsom många naturfenomen, dels nyare, såsom de som kan härledas till teknologisk utveckling, globalisering och den ökade komplexiteten i tekniska system. Då hoten exponerar ett samhälle uppstår nödlägen där hjälpbehov, såsom människors behov av akutsjukvård och mat, måste tillgodoses skyndsamt för att undvika eller reducera de negativa konsekvenser som krisen kan leda till. Många av de system som är viktiga i detta sammanhang är komplexa, eftersom de innehåller många komponenter och variabler som interagerar på många olika sätt. Dessutom beror komplexiteten på att mänskligt agerande spelar en stor roll för hur en kris utvecklas över tid. På grund av denna komplexitet och de mänskliga värden som står på spel bör riskerna i samhället hanteras proaktivt i en formell riskhanteringsprocess.

Ett element i proaktiv riskhantering är att genomföra risk- och sårbarhetsanalyser. För att dessa analyser ska vara adekvata bör de baseras på metoder som är lämpliga för det syfte analyserna har. Denna avhandling kommer därför att handla om att utveckla metoder och kunskap som ska kunna användas då risker och sårbarheter analyseras inom den samhälleliga krishanteringen.

Två huvudsakliga typer av system är av intresse i denna avhandling: kritiska infrastrukturnätverk och krishanteringsaktörer. Kritiska infrastrukturer spelar viktiga roller i kriser av åtminstone två orsaker. För det första kan de utgöra källan till att en kris uppstår, genom att serviceavbrott kan leda till allvarliga konsekvenser för dem som är beroende av denna service. För det andra är infrastrukturers service i många fall väldigt viktiga för i vilken utsträckning olika krishanteringsaktörer kan svara upp mot de hjälpbehov som uppstår i en kris, som är orsakad av en annan påfrestning. Ett avbrott då kan leda till en starkt försämrad hantering av krisen. Vidare spelar krishanteringsaktörer också viktiga roller för hur en kris utvecklar sig. Detta eftersom de strävar efter att möta upp de hjälpbehov som uppstår och på så sätt har en förmåga att reducera de negativa konsekvenser som krisen kan leda till. Exempel på sådana aktörer är räddningstjänst, statliga myndigheter, frivilliga organisationer etc. Dessa aktörers sammantagna krishanteringsförmåga är vad som avgör i vilken utsträckning hjälpbehoven kan tillgodoses.

Vid utveckling av metoder, utvärdering av metoder eller genomförande av analyser är det lämpligt att utgå från operationella definitioner av de begrepp som är av intresse. En operationell definition kan översiktligt beskrivas som en ideal procedur

för hur ett begrepp kan mätas eller karakteriseras för något specifikt system. Eftersom många av de begrepp som används inom detta forskningsområde ofta är vagt eller tvetydigt definierade kan operationella definitioner vara mycket effektiva. Inom riskområdet finns en relativt vanligt förekommande operationell definition av risk, men ingen sådan definition verkar finnas för begreppet sårbarhet, trots att också detta begrepp är vanligt förekommande. I denna avhandling föreslås därför en sådan definition som bygger på den operationella definitionen av risk. Sårbarhet kan då ses som svaret på tre frågor: Vad kan hända, givet en specifik påfrestning? Hur troligt är det, given den påfrestningen? Om det händer, vad blir konsekvenserna?

I denna avhandling föreslås metoder för sårbarhetsanalys av kritiska infrastrukturnätverk. Metoderna bygger på den föreslagna operationella definitionen av sårbarhet och även på tidigare forskning inom området nätverksanalys. Nätverksanalys tillsammans med den operationella definitionen av sårbarhet leder till en bra struktur för att analysera många storskaliga och komplexa infrastruktursystem. De metoder som föreslås har två olika fokus. Den ena metoden fokuserar på ett systems övergripande sårbarhet för olika påfrestningar – global sårbarhet. Den andra metoden syftar till att identifiera kritiska komponenter i systemet, d.v.s. den fokuserar på lokala egenskaper. Dessa två fokus kan sägas komplettera varandra.

En operationell definition av krishanteringsförmåga föreslås också i avhandlingen som betonar tre viktiga principer. För det första måste förmåga alltid relateras till specifika uppgifter eller aktiviteter, eftersom det som spelar någon roll i en kris är vad an aktör lyckas utföra. För det andra måste konkreta mått för vad som kännetecknar en väl utförd uppgift definieras. För det tredje påverkas en aktörs utförande av en uppgift av den kontext aktören befinner sig i. Kontexten kan ha att göra med huruvida alla nödvändiga resurser finns tillgängliga, hur andra aktörer lyckas med sina uppgifter etc. Slutsatsen som dras är att den föreslagna definitionen kan utgöra en bra grund för hur krishanteringsförmåga kan analyseras.

Förutom tillgång till lämpliga metoder för risk- och sårbarhetsanalys med syftet att ta fram att bra underlag för beslut, så är även kunskap om värderingar viktigt. Människors värderingar och preferenser avgör vad som överhuvudtaget bör räknas som en negativ konsekvens. Alltså måste det finnas kunskap om dessa värden för att överhuvudtaget veta vilka variabler som är intressanta att studera i en risk- och sårbarhetsanalys. Dessutom spelar naturligtvis värderingar en viktig roll då risker ska värderas och beslut fattas. I denna avhandling har därför en empirisk studie genomförts som syftade till att undersöka vilka avvägningar människor är villiga att göra mellan olika attribut som beskriver potentiella katastrofer. Slutsatsen som dras är att denna studie kan bidra med viktig information till riskhanteringsprocessen.

Dock bör resultaten kompletteras med resultaten från andra liknande studier för att undersöka generaliserbarheten.

Den övergripande slutsatsen av denna avhandling är att stora svårigheter föreligger då risk- och sårbarhetsanalyser ska utföras på komplexa system, såsom många av de system som är intressanta i ett samhälleligt krishanteringsperspektiv. Det arbete som presenteras här fokuserar på några relevanta områden, men ytterligare forskning behövs innan risker och sårbarheter kan analyseras ur ett helhets-perspektiv.

List of publications

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.

Jönsson, H., Johansson, J. and Johansson, H., "Identifying Critical Components in Technical Infrastructure Networks", Submitted to *Journal of Risk and Reliability* after invitation from the editor of ESREL 2007. Slightly adapted from Jönsson, H., Johansson, J. and Johansson, H. (2007), "Identifying Critical Components of Electric Power Systems: A Network Analytic Approach", *Risk, Reliability and Societal Safety* **1**:889-896, Proceedings of the European Safety and Reliability Conference 2007, Stavanger, Norway.

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., Johansson, H. and Abrahamsson, M. "Evaluating the Seriousness of Disasters: Implications for Societal Decision Making". (Manuscript.)

List of related publications

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

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

Table of contents

1 Introduction

Risk, broadly interpreted as the "probability and severity of adverse effects" (Haimes, 1998), is an inherent feature of basically every single human activity due to the fact that there are uncertainties associated with the outcome of most human actions and decisions. In driving a car, in walking down the street, in being dependent on power supply, etc., people are exposed to risks stemming from an array of hazards and threats. Risks are simply part of our everyday life – impossible to reduce to zero (Keeney, 1995). However, with the negative sides of risky activities often follows the positive; driving a car is more time-efficient than taking the bus, walking down the street is necessary to get to work, utilizing the power supply allows a person to cook, communicate and so on. In order to increase welfare and the quality-of-life we simply must accept the risks from some activities since they convey benefits that surpass the drawbacks introduced by the risks. In addition, risks posed by natural phenomena can not be avoided completely since humans are not fully able to control these phenomena. Risk is in general not something inherently negative but rather an "inevitably mixed phenomenon from which considerably good, as well as harm, is derived" (Wildavsky, 1988). Furthermore, although possible to reduce, some risks might not be worth reducing when for example considering their low probability of causing harm or the large costs associated with risk reductions.

The supposition that constitutes the foundation of the present thesis, and essentially the whole research field of risk analysis and management, is that the possibility to achieve a rational management of risks is increased if they are considered in a *formal* risk management framework. In such a framework, risks are addressed in a comprehensive and conscious manner, employing valid methods of inquiry and available scientific knowledge. The present thesis is about formal risk management carried out proactively in order to prevent, mitigate and/or prepare for emergencies and harmful events, that is, in order to reduce the risks facing the society. The focus is especially on those risks that have a potential of causing large-scale societal consequences.

An essential part of risk management is to gain knowledge of the systems of interest and their future behaviour so that the decisions and actions that are taken are well-founded. In order to gain such knowledge risk analyses are often conducted. More specifically, the purpose of a risk analysis is to gain knowledge of potential future scenarios in the system, their associated negative consequences and probabilities (Kaplan and Garrick, 1981; Aven, 2007). Such knowledge can then be used to inform and support the decision-making, for example regarding which actions to take, which risk reduction measures to implement or whether the risks can be

accepted or not. Risk analysis can be described as an essentially scientific, knowledge-acquiring endeavour – acquiring knowledge of observable variables by employing systematic methods. Complementing purposes of risk analyses have to do with the *process* of conducting the analyses, such as increasing the risk awareness of the ones participating in the analyses. Risk analyses can therefore sometimes also be seen as risk reducing activities in themselves.

In addition to science and factual knowledge, value input is essential to decision-making that concern risky activities, since values determine which ends and goals that should be pursued (Keeney, 1992). In risk and emergency management, the values determine which consequence dimensions are considered as good and bad, respectively, and also how different dimensions should be traded off against each other. Furthermore, value input is also needed to determine what can be regarded as an acceptable risk. Whose values to consider of course depend on the specific situation; however, for decisions of societal concern it is plausible to consider the citizens as "value consultants" (Webler, Rakel *et al.*, 1995), rather than for example groups of "experts". When conducting risk analyses and subsequently performing evaluations, in addition to having well-founded factual knowledge, it is thus also important to have good knowledge about stakeholder's values and preferences. The present thesis will address both these types of input to the risk management process.

Risk analysis has actually a rather long history, the first instance being possible to track to a group of people called the Aspiu, who acted as a rudimentary form of risk consultants in the Tigris/Euphrate-region around 3200 B.C. (Covello and Mumpower, 1985). The Aspiu was consulted when a person was faced with a difficult decision in which the outcomes of different alternatives where difficult to foresee and associated with large uncertainties. The Aspiu, then, made a systematic analysis of the possible ways of acting in order to find the alternative that appeared to be most favourable. Another predecessor to the modern risk analysis was the Athenians' approach to risky decisions around 400 B.C. Their approach was an early version of a qualitative risk analysis, where the consequences of different alternative actions were discussed and debated before decisions where taken (Aven, 2003). The foundation for the quantitative risk analysis, however, was laid in the 17th century with the emergence of probability theory (Covello and Mumpower, 1985). By use of probability theory it became possible to quantify risks and thus make it more mathematically and scientifically rigorous. More recent important developments of quantitative risk analysis can be tracked to the nuclear safety study sometimes referred to as the "Rasmussen Report" (Rasmussen, 1975). The Rasmussen report, issued by the U.S. Nuclear Regulatory Commission, was the first application of a modern version of quantitative or probabilistic risk assessment

to a large technological system and many of the methods developed within the scope of the Rasmussen report are still in use to this day (Apostolakis, 2004; Saleh and Marais, 2006).

1.1 The contemporary risk environment

The character of the risks that have exposed humans has varied over the history of mankind and also the attitudes towards risk management and control. The societal focus in many industrialized countries concerning events with potentially large-scale consequences was for a long period of time the threat of armed assault from external military forces; however, the end of the Cold War made this focus change to a greater concern for the vulnerability of the *civil* society (Olsen, Kruke *et al.*, 2007). In a broader perspective, it is the technical developments over the last centuries that have contributed the most to the changed nature of risk. Presently, there are several trends that contribute to the changing character of risks and emergencies that to some degree are interrelated and overlapping. These trends include globalisation, deregulation, the emerging threat of terrorism, tighter coupling and increased complexity of technical systems, development of information technology, increased interdependencies between critical infrastructure systems leading to a "system of systems view", increased societal dependencies upon infrastructure services, higher societal vulnerabilities to hazardous events, increased institutional fragmentation, more geographically dispersed events etc. (Perrow, 1984; Boin and Lagadec, 2000; 't Hart, 2001; Haimes and Longstaff, 2002; Boin, 2004; Leveson, 2004a; de Bruijne and van Eeten, 2007; Olsen, Kruke *et al.*, 2007). These trends all contribute to the changing risk environment and today many hazards, some natural and other man-made, have a potential of causing catastrophic harm to people and the environment, either due to sudden events or more gradual and creeping processes. Today, more hazards than ever have the potential to cause global and wide-spread harm which put demands on the emergency and risk management on all levels of society: local, regional, national and international.

In addition to changing trends regarding the nature of risks and hazards, there are also socio-cultural trends. A prominent example is the "greater insistence of citizens that they ought to be actively protected against disasters and crises" (Quarantelli, Lagadec *et al.*, 2007). This has, for example, in many countries led to new regulations in different societal sectors and jurisdictions. In Sweden, these regulations affect many different actors in the society, from municipalities and authorities to private companies and individuals. These demands include, for example, obligations for municipalities, county councils and authorities to perform risk and vulnerability analyses and to plan for contingencies and crises (SFS 2006:942; SFS 2006:544), obligations for certain chemical facilities to establish

safety reports, including risk analyses (SFS 1999:381 – Seveso II Directive), obligations for private power distribution companies to perform risk and vulnerability analyses (SFS 1997:857) and much more. The demands put forward in the regulations have in common a concern for managing and controlling the hazards and threats that expose the society in order to achieve a level of risk that can be deemed acceptable. The concerns both regard prevention of the hazards and mitigation and alleviation of the consequences of hazards that have materialised, for example by enhancing the society's capabilities to respond to and recover from hazardous events, reducing societal vulnerability and the vulnerability of critical infrastructure systems.

1.1.1 Increased focus on vulnerability

Over the last couple of decades the focus of risk and emergency management activities have been somewhat altered. Earlier, emergencies and disasters were seen to stem mainly from the triggering agent in isolation – often a geophysical hazard – thus leading to a "hazard-centric" focus (Dilley and Boudreau, 2001) which also was reflected in how the risks were managed (Weichselgartner, 2001; McEntire, 2005). However, in contemporary risk and emergency management, disasters are rather seen as stemming from the interactions between triggering agents and the *vulnerability* of the exposed systems (McEntire, 2001). Vulnerability thus should be interpreted as a system's susceptibility to the occurrence of a specific hazardous event or to a specific perturbation. For a highly vulnerable system that is exposed to a specific perturbation, the severity of the consequences is likely to be high. In a lesser vulnerable system, on the other hand, the severity of the consequences is likely to be less if the system is exposed to the same perturbation. Basically, we can for example not talk about natural disasters anymore, since the ultimate outcome of a naturally triggered emergency only to some degree depends on the natural phenomena per se (Alexander, 2002). A triggering event occurring in remote areas or in resilient societies will have different impacts than the same triggering event occurring in densely populated areas or in highly vulnerable societies. So instead of viewing the hazard (e.g. the natural event) as the disaster per se, it is more appropriate to view the disaster as human and socially constructed (Wisner, Blaikie *et al.*, 2004; Haque and Etkin, 2007). Factors that contribute to harm and disasters, besides the triggering events themselves, include for example the vulnerability of infrastructure systems, the capabilities of emergency response organisations, the affected population's social vulnerability, and much more. Researchers and risk and emergency practitioners have come to realise that in order to gain an as complete knowledge about risks as possible, and in doing so have a better possibility to make rational decisions, there is a need to address a broad array of different factors, which all contribute to shape the risk environment.

1.2 Complex socio-technical systems

The broad array of systems that are of interest to study in a societal risk and emergency management context can, in a broad sense, be said to be *socio-technical* and *complex*. These characteristics of systems pose great challenges to risk analysis and management. The fact that many systems are socio-technical implies that they contain or involve components and sub-systems of both technical (artefacts of different kinds) and social character (individuals, actors, groups, organisations). Ottens, Franssen *et al.* (2006) argue that what is significant for a socio-technical system is that it involves *social institutions* rather than only individuals that affect the functioning of the system. In the present thesis, the concept of socio-technical systems will be used to describe systems where social actors and institutions play an essential role for the functioning of the system. Examples include infrastructure systems, when including the institutions and organisations that manage the infrastructures, emergency response organisations, and of course a community or a society as a whole.

The exact meaning of complexity is somewhat ambiguous due to the fact that the concept is frequently being used in various scientific disciplines. In many definitions, though, a system is regarded as complex if it contains a large number of components that interact in many different ways (Simon, 1996; Axelrod and Cohen, 2000; Ottino, 2003). These characteristics describe many of the systems that are of interest in the present thesis quite well. A consequence of complexity is that *emergent system properties* arise from the elements of the system *and* their interactions. Emergent system properties are characterised by the fact that they have no meaningful interpretation at lower system levels. Mass, for example, is a *non*-emergent property since mass is possible to make sense of for all system levels, such as atoms, molecules, people, the universe etc. Group cohesion, on the other hand, is an emergent system property since it only makes sense when considering a set of persons and their internal relationships. Group cohesion for a single person or for the molecules in the body of a person does not make sense. The same argument can be applied to the atoms that humans or animals consist of. Although a living creature has the property of being *alive*, none of the atoms of the body can be said to be alive. Life is simply an emergent property.

As with complexity, there are also many diverging views regarding the nature and meaning of emergent properties. Emergence has actually been a topic of debate for a very long time and universal consensus is yet to be reached. The present discussion will certainly not provide an answer to this question; it will rather give insight into how the concept is being viewed here. Quite obvious is the fact that some macro level properties (i.e. emergent properties, such as life) have no

meaningful interpretation at a micro level (such as on the atom level); however, the contentious issue is to what extent such a macro level property can be *derived* from knowledge about the system's parts. The most extreme view of emergence is referred to as *strong emergence* (Pariès, 2006). According to this view it is impossible, *in principle*, to derive some macro-level properties from knowledge about the micro level. Many macro level properties that were believed to be impossible to derive from knowledge about the micro-level causality, however, have been proven to actually be derivable in the light of new scientific knowledge (Epstein, 1999). Therefore, a property that is "strongly emergent" in the light of today's scientific theories may very well prove not be strongly emergent in the future due to new scientific discoveries.

Another view of emergence is the one referred to as *weak emergence* (Pariès, 2006). According to this view macro level properties are possible to derive in principle from knowledge about the micro level; however, the number and comprehensiveness of the interactions between the system's components makes it impossible for a human being to work out the macro level property that corresponds to certain behaviour of the system's parts and their interactions. Instead, the only way to derive the macro level properties is to perform a "one-one simulation" (Pariès, 2006).

A complicating issue concerning the discussion about emergent properties, Epstein, (1999) argues, is that the distinction between *prediction* and *explanation* is often blurred. It makes perfectly sense that some phenomena are impossible, *in principle*, to predict, e.g. due to inherent stochasticity or chaos, but still being possible to explain or understand the underlying principles that govern the systems. In the present thesis, a pragmatic view of emergence will be used, which is proposed by Herbert Simon: "given the properties of the parts and the laws of their interaction, it is not a trivial matter to infer the properties of the whole" (Simon, 1996).

Emergence has implications regarding the causality in a system. In the traditional Newtonian worldview, all causation is upward, that is, higher level properties are completely determined by the behaviour of the parts. However, many researchers argue that a system with emergent properties has downward causation as well as upward causation (Lewin, 1999; Heylighen, 2003). What is meant with downward causation is that there are feedback loops from the higher level emergent properties to the interactions between the system's parts. Thus, the overall behaviour of a system with emergent properties is a mix of upward and downward causation.

Another characteristic that is commonly related to complex systems is that it shows *nonlinearities*, which is closely related to the concept of chaos. In systems with

nonlinearities, small causes might have large effects, and vice versa (Heylighen, 2003). Such systems might be very sensitive to the initial conditions, in that a small initial difference in input might lead to large differences in the subsequent output of a system (Lewin, 1999) – this is frequently referred to as deterministic chaos. Other effects of nonlinearities are that a system might exhibit *bifurcations* and *phase transitions*. Bifurcations imply that a given initial system state might lead to several different final states, impossible in principle to know in advance which of the states the system ends up in (Prigogine, 1997; Heylighen, 2003). Phase transitions implies that a system can be very insensitive to changes in system input over a range of different levels of the input, but once the level reaches a certain threshold the system is transformed into a completely different state. The effect of nonlinearities is that a system's future behaviour might be difficult or impossible to predict, even in principle, i.e. the system's future behaviour is undetermined and analyses of such systems are therefore challenging. A concrete example of phase transitions related to accidents and disasters is the theory of self-organized criticality (Bak and Paczuski, 1995) or the critical state (Buchanan, 2001) which it is also referred to. According to the theory some dynamical systems, many of them existing in nature, is organized into a critical state where only a minor perturbation can cause disastrous consequences. The standard example of such a system is the sand pile: at each time step a grain of sand is dropped on a surface. After some time the sand pile has grown in size and has organized into a state where only an additional grain of sand can cause massive slides – it is self-organized into a critical state. The resultant consequences from dropping an additional grain of sand can be described as a power-law distribution, which is characteristic for the critical state (Buchanan, 2001). A power-law distribution is characterised by a "heavy-tail", where the probability of extremely large effects can not be neglected. A somewhat competing theory for explaining this phenomenon when related to designed systems is called Highly Optimised Tolerance (Carlson and Doyle, 1999). According to this theory many systems are designed to be extremely robust against known perturbation, i.e. the ones that are known at the time of the design. The downside is that the system can become extremely fragile against perturbations it was not planned for to handle. Carlson and Doyle (1999) show that HOT can also give rise to power-law distributions similar to SOC, which means that the theories are competing for some systems. The point to make here, however, is only that for many systems of interest in the present thesis, the severity of the effects does not necessarily have to be linearly proportional to the magnitude of the causes.

So how are we supposed to make sense of complex systems? The 17th century philosopher René Descartes argued that "the thing to do with complexity was to break it up into component parts and tackle them separately" (Checkland, 1993), i.e. he argued for using reductionism to understand complex systems. That

approach has been significant for a large part of science, but underlying such a method is the assumption that "the components of the whole is the same when examined singly as when they are playing their part in the whole" (Checkland, 1993). However, as many researchers argue, such a method to acquire knowledge is not appropriate for studying complex systems, since a simple aggregation of separate parts does not yield a proper understanding of the system as a whole (Gell-Mann, 1997; Cook and Ferris, 2007). The reason is that the vast interactions and dependencies that exist in a complex system are distorted when breaking it down into isolated parts. Instead, approaches to make sense of complex systems must have a holistic/systemic orientation, where the interactions between the parts are also studied.

The fact that many systems of interest to study in a societal risk and emergency management context are complex and socio-technical clearly constitutes a challenge for any risk and vulnerability analysis. The issues are related to the characteristics described above, namely difficulties of prediction, the fact that there are several number of possible futures, the difficulties of analysing systems with many dependencies and interdependencies, problems associated with what to include in the system and what to leave out etc. There is a continuing need for developing methods and knowledge that can be used to better address and manage these issues. Research has already been conducted on these matters, but without doubt much more is needed. The present thesis aims to be one input to such matters.

1.3 Topics of interests

The main topic of interest in the present thesis is developing methods and knowledge that can be useful when an actor is analysing the risk and vulnerability of complex socio-technical systems, especially when this is done in a societal emergency management context. A good point of departure for any work that is concerned with developing methods, evaluating methods or conducting analyses is to start off from an *operational definition* of the concept of interest. In the field of risk analysis a quite well-established operational definition of risk exist that can be used as a basis for such work. However, in the context of societal emergency management other concepts are often discussed as well – two of the most relevant ones for the present thesis being *vulnerability* and *emergency response capabilities*. Of course there exist formal definitions in the literature of these concepts; however, these are generally not of operational type. A benefit of defining concepts operationally is that such definitions provide very precise and strict descriptions of what the concepts actually mean, something that is extremely important in the area of societal emergency management since different researchers and practitioners

often use the concepts with different meanings. Operational definition will therefore be a topic of interest in the present thesis.

Many systems that can be described as socio-technical and complex are relevant in a societal emergency management context. One class of systems that is a topic of interest in the present thesis is critical infrastructures, and especially electric distribution systems. Methods that can be used to analyse these large-scale infrastructure systems from a risk and vulnerability perspective are clearly needed. Furthermore, the present thesis will mainly be concerned with the critical infrastructures that can be described as "mainly technical", such as the electric distribution systems or water distribution systems, thus it will not deal with critical infrastructures such as banking and finance.

Finally, in addition to being concerned with analysis (basically being seen as a process for gaining objective knowledge about a system of interest) the present thesis will also be concerned with the "value-part" of the risk management process. As described earlier, scientific knowledge and facts about systems and system behaviour is not enough for making rational decisions. Knowledge about stakeholder's *values* and *preferences*, which are inherently subjective, are also essential for such decisions. More specifically, the topic of interest in the present thesis are values and preferences regarding *disaster scenarios*, i.e. trade-offs that people are willing to make regarding different characteristics of potential future disastrous outcomes.

1.4 An engineering research perspective

The topics of interest imply that the main perspective adopted in this paper is an engineering one, concerned with methods and knowledge development with the purpose of being of practical applicability. Since the engineering perspective differs somewhat from the traditional scientific one, there is a need to illuminate these differences and reflect upon which consequences this will have for the research approach and methodology chosen in the thesis.

1.4.1 Science and engineering

The overall purpose of traditional science is to gain knowledge and understanding by employing systematic and scientific methods of inquiry. This view is in accordance with Checkland's who argues that "science is a way of acquiring publicly testable knowledge of the world" (Checkland, 1999) and he furthermore claims that the traditional scientific method is characterised by reduction, repeatability and refutation. Engineering, technology, design and applied sciences are all research disciplines that stand in contrast to traditional science, in that the

purpose of the research is more practically oriented. The internal relationships between these four disciplines are not universally agreed upon in the research literature; however, the aim of the present section is not to clarify these relationships, but to show how the engineering perspective adopted here relates to the traditional scientific one. Here, engineering, technology, design and applied science can be regarded as partially overlapping disciplines and engineering will henceforward be used to label a practically oriented discipline with the aim to construct or design different types of artefacts corresponding to an "efficient accomplishment of a certain purpose" (Cook and Ferris, 2007).

Instead of the virtue of obtaining knowledge for the sake of the knowledge itself, which signifies science, the virtue of engineering is to identify and implement the best, most efficient or at least satisfactory means to pursue some predefined ends. As Bunge points out, science elicits change with the purpose of knowing whereas in technology (and engineering) one knows in order to elicit change (Bunge cited in Frey (1991)). Engineering thus has a normative feature – the concern "with how things ought to be" (Simon, 1996), which traditional science lacks. Historically, science and engineering have evolved largely independent of each other, however today the disciplines are much more converged and interwoven so that the disciplines sometimes might be difficult to separate (Gardner, 1994). According to Fromm (2005), "the distinction between engineering and science blurs increasingly for the engineering of complex and self-organizing systems, and both fields seem to converge more and more in this case", the reason being that in order to engineer complex systems, one must first understand them. However, Gardner argues that there are still differences between science and engineering regarding what is valued the most: knowing or doing.

In the literature it is not entirely clear whether engineering should be seen as a specific *scientific* discipline or whether it should be distinct from science (see for example Lewin (1983) and Poser (1998) for diverging views on the matter). What is clear, though, is that engineering *formally* is regarded as a science "since it has been located in the higher technical institutes and universities for a century" (Poser, 1998). Furthermore, in a discussion of design, Cross argues that "design science refers to an explicitly organised, rational and wholly systematic approach to design: not just the utilisation of scientific knowledge or artefacts, but design also in some sense as a scientific activity itself" (Cross, 1993). An analogue argument could be applied to engineering science. However, without taking a stance on the question whether engineering is a scientific discipline, which is essentially a conceptual question, it is argued that what is interesting is what can be characterised as "good" science and engineering, respectively. In the philosophy of science criteria for good science exist, however the philosophy of engineering is a much less

established topic (Lewin, 1983). Due to the differences between traditional science and engineering it is thus not entirely clear which criteria for "good" science that are applicable to engineering as well.

1.4.2 Scientific development of methods

As described earlier, engineering is normally about designing and constructing different types of physical artefacts or systems. The normal process of solving such an engineering problem can be described chronologically by problem definition, choice of objectives, creation of possible alternatives, analysis of potential alternatives, choice of best alternative, development of prototype and implementation (Lewin, 1983; Checkland, 1993). In the present thesis the concern will not be about constructing any physical systems; rather it will partly deal with creating or developing methods, which in turn can be used for example to design or analyse systems. According to Checkland (1993), however, a method is in fact also a type of system – a designed abstract system, which in contrast to designed physical systems only exists as a set of interrelated thoughts and concepts that aim to help solving a problem of a specific kind. The problem of developing methods is thus essentially a problem of design.

In the pursuit for an engineering philosophy, Lewin (1983) argues that there are similarities between the method of engineering and design, described above, and the method of science as it is proposed by Karl Popper in his paradigm of falsification. In Popper's paradigm, scientific hypotheses are never concluded to be true theories; they can only be false (if empirical observations falsify them) or corroborated (if empirical observations do not falsify them). According to Lewin both Popper's and the engineering method subject a "postulated solution to analysis and test in the light of experience and existing theory" (Lewin, 1983). In science this stage is about testing a *hypothesis* against empirical evidence with the subsequent falsification or corroboration, for example by conducting an experiment. In engineering, on the other hand, this stage is about "evaluation of a proposed design with respect to its specification" (Lewin, 1983). Both stages essentially concern whether the propositions, in some senses, are good enough. Thus, neither of the two methods of inquiry is about identifying a true or definite proposition since a better one always is possible to stipulate.

This line of reasoning can also be applied to development of methods, since development of methods also can be seen as an engineering or design problem. In that way it is possible to somewhat "imitate" the traditional scientific method when methods for risk and vulnerability analysis is being developed. In Figure 1-1 such a "scientific" process of methods development is presented. This process starts off with creating a method. The analogy to this step is theory or hypothesis

development in the traditional scientific method, which most often builds on previous research. In method development it is reasonable to create the new method based on previous methods and suggestions, i.e. not to "invent the wheel" again if not necessary. Of course, sometimes it is desirable to suggest a whole new approach to analysis. In the present thesis, however, the former approach is mainly adopted. The second step in the process is to apply the method in the context it is supposed to be applied. The analogy to this step is conducting experiments or making observations in order to find evidence for or against a hypothesis. The third step is to evaluate the application of the method. The analogy to this step is interpretation of the experiments and observations and the subsequent falsification or corroboration. Then the process of method development enters an iterative phase where the method is modified in the light of the evaluations previously made. The modified method is then yet again applied and the application is evaluated.

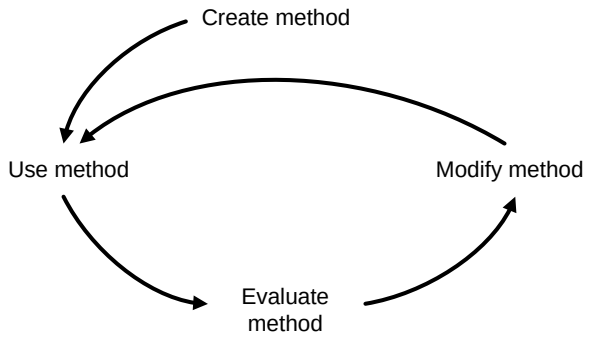


Figure 1-1. The process of developing methods, adapted from Checkland (1993)

In the standard engineering problem-solving method, described previously, different alternative designs are evaluated and the best one is chosen and subsequently implemented. The same basic principle of evaluation thus also holds for method development, the main difference being that often only a single method is being designed and evaluated in order to find out whether it is sufficiently good. So what characterises a method that is "good enough"? At the fundamental level, any designed system (including abstract ones such as methods) is developed for a certain *purpose*, or as Simon argues: "design is concerned…with devising artifacts to attain goals" (Simon, 1996). Thus, in order to be a satisfactory design, the designed system must meet certain *criteria* that are given on beforehand and which correspond to the pre-established purpose of the design. Before the development of a method is being initiated a number of criteria or axioms that the method must meet therefore should be established (ideally explicitly, but often

rather implicit). Evaluating the method can then be accomplished by investigating whether, or to what extent, the method actually meets the established criteria.

To summarise the discussions in this section, it is argued that the method development process can be made more or less scientific and an important step in this process is the conscious evaluation of a proposed method, in the light of its intended purpose, and the subsequent modification of that method. An issue is that this process is often very time consuming and the present thesis do not aim at coming to finalized methods, only to start the iterative and continuous process of developing them. In addition, developing methods can in many cases be seen as a joint venture between many research groups, where each group makes contributions to the development, e.g. evaluating each others suggestions. Of course, many other principles for good science is also possible to apply to engineering than the ones discussed in this section, however it is not the aim of the present thesis to clarify that.

1.5 Limitations and demarcations

Much could be said about the limitations of the research presented here. In this section however only a couple of points will be made. Limitations associated with specific details related to for example the methods and definitions that have been developed will be discussed in connection to the presentation of the methods and definitions since understanding these limitations require more in-depth knowledge.

A more general limitation of the methods, developed to analyse the vulnerability of critical infrastructures, are that they are only applicable to systems that are possible to model as networks. The reason for this was that many critical infrastructures, especially the ones that are mainly technical, are possible to model as networks, and the ambition was that the methods would be applicable to a broad class of infrastructure systems. However, there is often a trade-off between how generic the methods are and how useful they can be for specific type of systems. In focusing on infrastructures that are possible to model as networks it is believed that a plausible trade-off has been conducted. Furthermore, although the methods have been developed to be applicable to other systems, they have only been applied to analyse the electric power distribution system. In order to evaluate the applicability of the methods for other types of systems, case studies should be conducted on other types of systems as well.

Another limitation associated with the network-based methods is that interdependencies between different infrastructures not have been incorporated. The ambition has been to allow for the incorporation of interdependencies in the methods; however, this will be a matter for future research. A reason for making

use of network analysis is the belief that it could serve as an appropriate "common ground" between different types of infrastructure systems and thereby facilitate the future incorporation of interdependencies.

Due to the fact that the focus of the present thesis is mainly a normative one, no attempt to formulate scientific theories will be made. Scientific theories are traditionally aiming to describe or explain the workings or the behaviour of a real-existing system of interest, i.e. they are descriptive. Instead of formulating scientific theories, the concern will mainly be to suggest approaches, definitions and method that may be fruitful to adopt when studying certain classes of systems.

1.6 Thesis outline

The outline of the present thesis is as follows:

- In chapter 2 the aims and research objectives that emerge from the introductory chapter will be briefly stated.
- In chapter 3 the role of risk and vulnerability analysis in the context of societal emergency management will be discussed. A broad view of societal emergencies will also be sketched with the purpose of showing how the papers, of which the present thesis is based, relate to societal emergencies in general. Another purpose of describing societal emergencies is to show the complexities associated with them, and indirectly to indicate the challenges for risk and vulnerability analyses carried out in such a context.
- Due to the complexities associated with many of the systems related to societal emergencies there is a need to investigate different approaches for studying and analysing such system. In chapter 4, therefore, a number of approaches will be addressed and discussed. The three approaches described have been and continue to be influential to the research conducted by the author.
- In chapter 5 the central concepts of the present thesis, risk and vulnerability, will be discussed and explicitly defined. The definitions will be of operational type which is a particular concrete type of definition. The definition of risk will basically be a review of an existing definition, whereas vulnerability is an extension of the definition of risk which has been proposed by the research group of which the author is a part.
- In chapter 6, three research themes will be presented: vulnerability of critical infrastructure networks, emergency response capabilities and value input to risk analysis and decision-making. These themes are closely related to the

papers. After a presentation of the themes, these will be briefly evaluated and suggestions for future work will be given.

- In chapter 7, a number of concluding remarks will be given. In the end of this document the papers, of which this thesis is based, will be attached.

2 Aims and research objectives

From the general background provided by chapter 1, a number of aims and research objectives can be stated for the work in the present thesis. The first objective concerns *operational definitions*. As was said in the previous chapter, operational definitions can be very useful when developing methods, evaluating methods or conducting analyses in practice. For two concepts that are very interesting here, namely vulnerability and emergency response capabilities, no operational definitions appear to exist in the academic literature. The first research objective therefore is *to develop operational definitions of vulnerability and emergency response capabilities that can be useful in work concerning method development, methods evaluation or analyses in practice*.

The second and third research objectives concern methods for vulnerability analysis of large-scale technical infrastructures. To some extent methods that capture the effects of perturbations already exist; however, the effect of very large perturbations, which potentially can cause catastrophic consequences, is sometimes ignored in standard analyses of technical infrastructures. In general it is possible to separate between analyses that are concerned with *global* aspects of the systems, i.e. which aim to analyse the overall vulnerability of systems to specific perturbations, and *local* aspects of systems, i.e. which aim to identify the parts, components, or sub-systems that are critical to the system functioning. The present thesis is concerned with both of these types of methods. The second research objective is therefore *to develop methods for global vulnerability analysis of large-scale technical infrastructures that are able to take severe perturbations into account*, and the third research objective is *to develop methods for identifying critical components in large-scale technical infrastructures*.

The fourth research objective concerns the *"value-part"* of risk-informed decision making. As was described in chapter 1, values are intrinsic to any risk or vulnerability analysis and decision regarding risks, since the very motivation for conducting the analyses in the first place is to investigate the likelihood and severity of different future scenarios that may harm human values. Many applications of risk analyses focuses on single dimensions of harm; however, often this approach has been assumed without deeper analysis of the underlying values. Here, the interest relates to events with a potential for causing disastrous consequences. The fourth research objective is therefore *to investigate how people are willing to make trade-offs between multiple consequence attributes.*

3 Risk and vulnerability analysis in the context of emergency management

Risk and vulnerability analyses already play important roles in the emergency management process in many countries. As was mentioned previously, according to the Swedish legislation, for example, it is mandatory for municipalities, county councils and authorities to conduct risk and vulnerability analyses. This chapter aims to give an overview of emergencies and the role that risk and vulnerability analyses play, or potentially can play, in an emergency management context. The chapter ends with presenting a model that aims to provide a very generic picture of emergencies in order to illustrate what factors influence the occurrence of emergencies, how emergencies evolve and the final outcome of them. Implicitly, thus, the model gives insight regarding what risk and vulnerability analyses need to take into account in order to provide an as complete picture as possible.

3.1 Some notes on the concepts of accidents, emergencies, crises, disasters and catastrophes

In the research literature, there are several different concepts that relates to the broad class of events in which harm to life, health, environment, property or other human values, of various severities take place. The five most prominent ones are accident, emergency, crisis, disaster and catastrophe; however, there is in general no universal consensus in the academic literature regarding the interpretation of them and the relations between them (Quarantelli, Lagadec *et al.*, 2007). Therefore, there is a need to show how they are being used in the present thesis.

Catastrophe is probably the concept, of the five, that is being used least frequently in the academic discourse. A common view is that catastrophes are *qualitatively* different from for example disasters and emergencies in that the social life is *completely* disrupted and the community can not function in any meaningful way (Quarantelli, 1997). Although a disaster is defined as having a major impact on the society, in terms of large-scale negative consequences, there are still several societal activities that continue to function. Quarantelli also argues that a qualitative difference also exists between disasters and emergencies, in that emergencies can be handled by local resources and personnel while disasters require assistance from external actors (Quarantelli, 1998). Alexander (2005), on the other hand, has another view, which is broader than the one proposed by Quarantelli, where emergencies include events of a variety of impact magnitudes from small disruptive accidents to disasters and catastrophes.

The concept of accidents is closely akin to the concept of emergencies; however, still quite distinct from it. Hollnagel defines an accident as "a short, sudden, and unexpected event or occurrence that results in an unwanted or undesirable outcome" (Hollnagel, 2004). Although the concept of accidents and the area of accident investigation and analysis can provide important insight to emergency management it is somewhat to narrow in scope to be directly applicable here. First, an accident is *always* seen as an effect of human activities rather than the occurrence of for example a natural event. Secondly, it is clear that in the area of accident modelling and analysis the greatest interest is devoted to identifying the causes and conditions leading up to the occurrence of some critical/accidental event, such as the release of hazardous materials. The interest is not as much with the response to the release, such as how emergency response agencies is acting or how the general public behaves, which is often of interest in crisis and emergency management. So while accident modelling and analysis can provide important insight to emergency management research and practice, it only covers a part of what is interesting for emergency management. Thus, what accident modelling do not generally aim to capture, but which is of great interest in the present thesis, is the fact that the ultimate outcome of a hazardous event, such as the accidental release of toxic gas, in many cases to a large extent is determined by how the event is responded to.

The concept of crises is also common in the academic literature. A crisis is often said to refer to "a serious threat to the basic structures or the fundamental values and norms of a social system, which – under time pressure and highly uncertain circumstances – necessitates making critical decisions" (Boin, 2004). Thus, in order for a crisis to arise three conditions have to be met: there has to be an imminent *threat* to core values, there has to be large *uncertainties* associated with possible actions and there has to be a sense of *urgency* associated with actions[1] (McConnell and Drennan, 2006; Boin and 't Hart, 2007). Disaster, on the other hand, predominantly refers to the devastating outcome of an event, rather than to the dynamic *processes* being referred to in the concept of crises. A crisis does not have to develop into a disaster or a catastrophe, since if it is managed successfully it could develop into only a minor incident. A disaster can therefore be said to be a "crisis with a bad ending" (Boin and McConnell, 2007).

[1] A crisis can be said to differ from the broader concepts of threats and hazards in that a crisis has entered an "acute phase", requiring very quick actions, i.e. a crisis is a hazard or threat that has materialised or is very soon about to materialise. This view is also brought forward by Quarantelli, Lagadec et al. (2007).

The relation between crisis and emergency management is most difficult to clarify. In many cases the concepts are treated as synonyms and most often they are at least grossly overlapping. However, subtle differences between the concepts can sometimes be discerned, see for example CCMD (2004). Responding to an emergency often involves prompt actions to try to minimise the harm on people and/or the environment (i.e. a physical harm). It often deals with rather concrete threats and consequences and do not necessarily involve a great deal of uncertainties. Crisis management on the other hand involves a higher degree of subjectivity: if it is perceived, for example by the public or by decision-makers, that core values are seriously threatened then there is a crisis; or as Boin and 't Hart argue: "[p]hysical facts, numbers, and other seemingly objective indicators are important factors, but they are not decisive" (Boin and 't Hart, 2007). In addition, often crisis management deals with vaguer types of consequences, such as lack of trust in social institutions, and the uncertainties are always high. To give a concrete example of the difference between emergencies and crises, consider the Estonia disaster that occurred in the Baltic Sea in 1994. Due to the capsizing of the ship an *emergency response* was initiated in order to save as many human lives as possible. However, after the acute phase of the emergency had ended, i.e. where no more lives could be saved, a *crisis* emanated from the fact that there where doubts regarding whether investigations where carried out appropriately or whether facts where hidden from the public. As such, an emergency can escalate into a crisis.

Although, the qualitative and quantitative differences between emergencies, accidents, disasters, crises and catastrophes proposed by many researchers are acknowledged in the present thesis, it is argued that it is often difficult to draw any clear-cut distinctions regarding which events and phenomena that fall into the respective category – and often an event fits into several of the categories. What is needed in the present thesis is a concept that provides a broad view of the processes that lead to harm and the activities that is focussed on preventing the harm from occurring or alleviating it. Alexander's view of emergencies, referred to above, is believed to provide such a broad view. In what follows, therefore, the term *emergency management* will be used to refer to the activities taken prior to, during and after the occurrence of emergencies, that is concerned with mitigation of, preparedness for, response to and recovery from emergencies.

3.2 A framework for the emergency management process

A widely used framework for describing the emergency management process contains the four phases stated in the previous section, i.e. mitigation[2], preparedness, response and recovery (McLoughlin, 1985), see Figure 3-1. The framework, which has been labelled "Comprehensive Emergency Management", emerged in the end of the 1970s and acknowledges both the wide array of possible hazards that societies potentially have to respond to and the great functional similarities among different events (McEntire, Fuller *et al.*, 2002). Furthermore, it emphasizes that the emergency management process not only is about the acute phase of an emergency, but also about the activities that are performed before and after an emergency has occurred. In the framework, the mitigation phase consists of any activities that aim to reduce the probability of emergencies and disasters and activities that aim to reduce long-term risks, such as land-use management and disaster insurance. The preparedness phase consists of activities that aim to increase the capabilities of responding to emergencies, such as installing early warning systems and establishing emergency plans. The response phase consists of any activities that are performed in close proximity in time of the emergency, such as immediately before (after warnings have been obtained), during (evacuation, acute medical aid, information distribution) and immediately after (such as sanitation, restoring critical infrastructure service) the event in order to meet any acute needs. Finally, the recovery phase consists of both short-term and long-term activities that aim to restore any vital functions and make the system return to the "normal" state. Sometimes a fifth phase is added to the framework, namely a learning phase in which measures to reduce any vulnerabilities that were revealed in the emergencies should be taken. As such, the learning phase can be seen as the beginning of "the next" emergency and thereby "connects" the recovery phase with the mitigation and preparedness phases. Of course, learning can also occur in an organisation without it having to experience any actual emergency, for example from studying other organisations, conducting risk and vulnerability analyses or simulating crises.

[2] In some versions of the model the mitigation phase is replaced with prevention, although without a significant change in meaning.

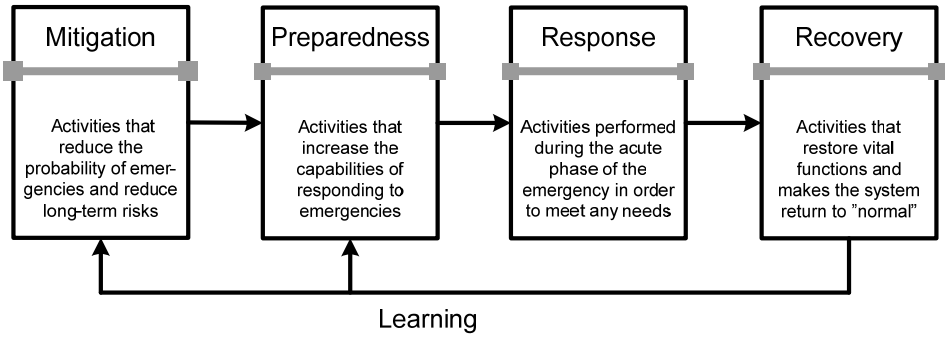


Figure 3-1. The MPRR-model – a widely used framework for the emergency management process labelled the Comprehensive Emergency Management approach.

The framework described above has received some criticism. Cronstedt (2002) argues that the framework builds artificial barriers between the four phases – barriers that do not exist in reality. He further argues that this leads to an unnecessary large effort being allocated to discussions of which element various activities are best described as. He also argues that the temporal order of the elements implied by the framework potentially can hamper the treatment of emergencies. In addition, McEntire, Fuller *et al.* (2002) argue that the Comprehensive Emergency Management approach has been overly concerned with the hazards, downplaying the importance of vulnerabilities and also that it has been too reactive.

Although the criticism mentioned above to some part is acknowledged in the present thesis, the framework is believed to constitute a satisfactory model for emergency management that can be used to relate different emergency management and research activities to, especially the role that risk and vulnerability analysis play. Of course, making use of models that separate different activities from a temporal perspective render a possibility that the same activity is interpreted as part of different phases by different people. For example, how proximate in time after an emergency must an activity be carried out in order for it to be classified as a response activity? Certainly there is not a single clear answer to this, but it is not really the purpose of the model to have clear-cut answers to such questions. Instead the purpose is to provide a broad perspective on emergency management, illuminating the fact that it is not only a single phase that is important for adequate emergency management. Emergency management activities need to address all phases.

A problem in connection to the temporal phases of emergency management is that in classifying different emergency management activities as preventive or responsive

and so on, one anchors the classification on a specific event. If something aims at breaking the causal chain leading up to that event it is called a preventive measure, whereas if something is done to break the consequence chain following that event it is called a responsive measure. However, it is not always obvious which event that is being anchored on. Whether a measure is classified as preventive or responsive is thus not a characteristic of the measure itself but rather a relation between the measure and the event being anchored upon. In some sense, all measures that aim at reducing risks can be said to be preventive, even the actions taken during an emergency, since they aim to reduce the probabilities or consequences of future events. Therefore, it is important to be clear about which events that are being anchored on when classifying measures as preventive, preparatory, responsive, and so on.

3.3 The dual role of risk and vulnerability analysis in emergency management

Risk and vulnerability analyses can potentially play important roles in both the mitigation and preparedness phase of an emergency (see Figure 3-1). Conducting risk and vulnerability analyses, then, is one component (of many) in a proactive approach towards emergency management and safety. The purpose of the analysis has large influences on how it will and should be carried out. Available resources, the competence of the analysts and much more will and should affect the choice of method, the comprehensiveness of the study and so on. In the present thesis, a distinction is made between two overriding purposes, or roles, that risk and vulnerability analyses can have: a *decision-oriented* and a *process-oriented* role (see Figure 3-2).

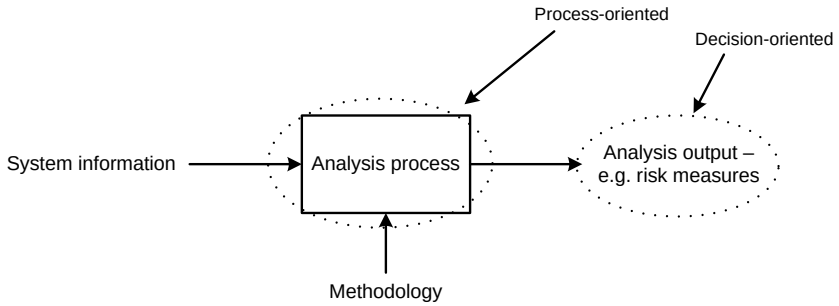


Figure 3-2. Illustration of the analysis process and whether the focus of an analysis that has been carried out is on the process itself or the output of the process, adapted from Rouvroye and van den Bliek (2002).

A purely decision-oriented approach is only concerned with what the analysis is able to produce, for example in terms of quantification of risk by use of some risk

measure. The actions performed during the analysis process are only important to ensure the quality and validity of the analysis output. Many contemporary applications of risk analysis (especially in engineering) are directed toward providing input to decision-making, such as investigating whether a certain activity is acceptable from a risk perspective or which actions are most cost-effective in reducing a risk. An example of a decision-oriented approach is put forward by Cox when describing traditional Quantitative Risk Assessment (QRA) as "providing a logical framework and a systematic procedure for organizing and applying scientific and engineering knowledge to improve "rational" (consequence-driven) decision making when the consequences of alternative decisions are uncertain" (Cox, 2007). Thus, ensuring that the best available knowledge is used as input to decision-making will help make the decisions as "rational" and good as possible.

A purely process-oriented approach is not concerned with what the analysis will produce, for example in terms of risk estimations; instead the focus is on the activities that are performed during the analysis process per se. Most often a process-oriented analysis is conducted by people that themselves are part of the "system" being analysed. Conducting risk analyses are then believed to enhance people's risk awareness and encourage them to reflect upon their actions and change those actions that may contribute to the overall risk. Furthermore, in many cases the people that participate in the analysis process play an essential role in shaping the risk in the system, for example by acting as responders in the acute phase of an emergency or as operators in the control room of a chemical plant. Conducting risk analyses with these people can function as a catalyst for building trust and friendship ties among the participants leading to better preconditions for adequate communication and coordination prior to and during an emergency. In addition, common mental models about risks and emergencies can be created, which also can lead to positive effects.

Process-oriented approaches can for example be found in emergency preparedness and planning. Many researchers argue that the value of emergency planning does not lie in the generation of an outcome in terms of a written plan, but in the *processes* of producing the plan (Quarantelli, 1997; Perry and Lindell, 2003). According to McLoughlin this is because "the officials who are responsible for emergency operations have spent time determining which official will do what and how operations will be coordinated" (McLoughlin, 1985). Thus, the emergency planning in itself is a means of reducing the overall risk for the system in question, by increasing the capabilities to respond to perturbations. The same can be said about conducting risk analyses with a process-oriented approach – the analysis process is believed to reduce the level of risk by increasing the risk awareness and the response capabilities of the people "in the system".

In conducting interviews with people participating in risk analysis processes, Busby and Hughes (2006) found that many persons were actually sceptical about the ability of risk assessment methods to produce valid, objective risk measures; instead they argued that the value of the risk analysis "lay in helping people who generate the risk, or find themselves responsible for risk, reflect on their practices". Increased focus on the analysis processes per se is likely to be preferred as systems become more complex. A parallel can be drawn to Peter Checkland's distinction between hard and soft systems (Checkland, 1993). In hard systems problems are well-defined and there is a general agreement on which objectives to pursue. The problem then dwells down to choosing the best possible future strategy. In softer systems, on the other hand, problems are ill-defined and it is not even clear which objectives that should be pursued. Checkland argues that in such circumstances the purpose of making use of methods to perform various types of analyses rather is to structure a discussion about the problems (in the context of this thesis these problems concern risky activities) than to generate any concrete input to decision-making. The line of reasoning can be applied to risk analyses as well; as systems become "softer" and more complex it is increasingly difficult to generate valid and objective measures of risk as input to concrete decisions. Instead, the analyses in themselves are seen as risk reducing activities.

Risk and vulnerability analyses that are carried out in practice can rarely be classified as either a purely decision-oriented or a purely process-oriented approach. Instead, they often involve a mix of the two types of purposes, although the purpose is often leaning towards the one or the other. For example, in the guidelines published by the Swedish Emergency Management Agency (SEMA) regarding risk and vulnerability analyses that Swedish authorities, municipalities and county councils are obliged to conduct, both purposes are stressed (SEMA 2006a; 2006b). On the one hand, the risk and vulnerability analysis is the tool for knowledge attainment that subsequently can be used for deciding which risk and vulnerability reducing measures are most effective, or at least effective "enough" to implement. On the other hand it is stressed that in conducting the analyses the aim is to increase the risk awareness of the participants and to create and maintain a safety culture in the organisations. A type of risk analysis where the decision-oriented purpose is much accentuated is the risk analyses conducted in the context of the Swedish land-use planning process. In the Swedish Plan and Building Act one (of many) requirements is that when someone is to exploit land for housing, offices or other activities, planning must be carried out with regards to people's health (SFS 1987:10). Often this requirement is interpreted in the sense that a risk analysis has to show that the risk for the plan area, exposed by surrounding hazards, is acceptably low. To show risk acceptance, external risk experts are usually

consulted who conduct quantitative risk analyses that can be compared to established acceptance criteria and a decision regarding the suitability of the proposed land exploitation can be taken. When a decision has been taken the risk analytic effort ends, i.e. no continuing process is initiated with the purpose of for example increasing the safety culture of the involved actors.

The demands one can put on an analysis and the method used for the analysis are dependent on where on the continuum, shaped by the two extreme roles, a specific analysis can be positioned. The validity of the method, in terms of the correspondence between any estimations and reality, is not equally crucial if the analysis is very process-oriented rather than decision-oriented. A process-oriented analysis must instead ensure that discussion and deliberations throughout the analysis promote the purpose of the analysis, e.g. if the purpose is to increase trust relations among people having a role in the emergency response, it is important that the "right" people participate in the analysis.

In the context of emergency management both roles of risk and vulnerability analysis are often very important. In Swedish municipalities, for example, it is common, but not always the case, that the ones conducting the analyses are also acting in the response phase of an emergency. Therefore, analyses can constitute a way for these to interact and create trust relations among themselves. At the same time there is a clear need to make decision regarding which resources and skills are needed, whether the municipality should start cooperating with neighbouring municipalities, whether structural mitigation measures should be implemented and so on. Of course, such a decision can be made without formal analysis; however, the possibility to make a rational decision is definitely increased if a properly made analysis is used as input to the decision.

The methods being developed in the present thesis primarily aims to provide concrete input to decision-making. It is thus important that the analysis method ensures that the outcome, given that the analysis is performed appropriately, is of high quality and validity. However, this as a primary aim does not exclude the methods from being useful from a process-oriented perspective as well.

3.4 Strategies for risk reduction: anticipation and resilience

Risk analyses often provide input to how risks can be controlled or reduced. Many different types of strategies for risk control and reductions exist and also many ways of classifying them. The present thesis does not aim at discussing these issues in depth, only to briefly comment on two general and contrasting types of strategies

for risk reduction that often are discussed in the research literature; anticipation and resilience. Aaron Wildavsky, in his book "Searching for Safety" Wildavsky (1988) argued that anticipation include the "efforts made to predict and prevent potential dangers before damage is done", whereas resilience involves the "capacity to cope with unanticipated dangers after they have become manifest, learning to bounce back". Wildavsky further argued that both type of strategies are needed and that a balancing between the two must be attained; focusing too much on resilience will lead to systems being exposed to unnecessary stresses and perturbations. Focusing too much on anticipation (interpreted roughly as mitigation/prevention), on the other hand, will lead to reduced resilience/increased vulnerability since people, organizations etc. are so rarely "put to the test". Unfortunately, anticipation can never be "complete", which means that on some rare occasions hazards will materialise even though large resources are devoted to prevention. Then, even a small perturbation may lead to a catastrophe. This phenomenon is sometimes referred to as the vulnerability paradox ('t Hart, 1997, 2001). The phenomenon can also be related to the reliability and resilience of critical infrastructure systems. These have over the years in general become more reliable; however, this has also led to that the society is increasing its dependency on the systems and thereby also increasing its vulnerability to service disruptions (Boin, 2004). The main problem with anticipatory strategies, Wildavsky argues, is that very detailed knowledge is needed in order to reduce risks and the barriers and functions implemented for risk reduction are only effective for specific hazards. In developing resilience and generalized capabilities, on the other hand, one is protecting the system to a wide array of hazards and perturbation; detailed knowledge about the hazards is simply not needed, he argues.

Wildavsky's strict differentiation between the two types of strategies is not the only view in the academic literature. Resilience, for example, is frequently being used with a broader scope – see Manyena (2006) for a review of definitions. Instead of only viewing resilience as the ability to withstand, respond to and recover from unanticipated hazards and perturbations, it is sometimes argued that resilience also include the ability to foresee and prevent hazards and perturbations. This is the case in the relatively new safety paradigm called "Resilience Engineering" (Hollnagel, Woods *et al.*, 2006) and this view leads to the fact that anticipation and resilience to some extent overlap, i.e. being resilient also means being able to anticipate, a connotation Wildavsky seemingly do not assign to resilience.

Issues also arise in trying to define anticipation. In Wildavsky's view anticipatory strategies are only possible when considerable knowledge regarding the hazards in question exists and where it is possible to predict how actions will affect future behaviour; however, here it is argued that such a view restricts the concept too

much. Anticipation can be carried out without only focusing on how to prevent the hazard from materialising; it can also be carried out to find out which demands are likely to be put on emergency response actors when a hazard manifests, for example which resources, skills etc. are needed. In many cases there are great functional similarities between hazards so without knowing the exact details of them, anticipation can be used to prepare for a wide array of emergencies and disasters – i.e. anticipation can be used to build resilience and generalized capabilities. For example, in anticipating which resources are "generalizable", detailed knowledge of hazards, causes of hazards and such are often not required; or as Marais, Dulac and Leveson argues: "it is not necessary to predict all potential causes of a ship sinking in order to provide life boats and other emergency measures" (Marais, Dulac *et al.*, 2004). By employing anticipatory strategies, for example by conducing risk, vulnerability and capability assessments it is possible to identify measures that increase the resilience of a system to perturbations. In fact, aren't all activities that are consciously carried out in order to increase resilience or capability a type of anticipatory strategy? This is because they try to anticipate which qualities, characteristics, skills etc. will make a system better at foreseeing, withstanding, responding to, recovering from etc. future occurrences of hazards and perturbations. For example, one can anticipate that increasing the flexibility of an organisation will increase the organisations ability to cope with unexpected crises. We do not need to know anything in particular about the characteristics of the crises, only that there exists a positive correlation between flexibility and ability to cope with unexpected events.

3.5 A general "model" of societal emergencies

Many applications of risk analysis mainly focus on modelling how a hazard exposes a particular system of interest. In an emergency management context, however, the response to an emergency often is an important factor for how the emergency evolves and which consequences the emergency will give rise to. In this section a general model of the response phase of emergencies is outlined. The purpose of describing such a model is primarily to provide a frame of reference when thinking about emergencies. This model, thus, plays a similar role as accident models do in the area of accident analysis and investigation. Hollnagel argues that an accident model "determines how we view an accident" which means that it provides "a stereotypical way of thinking" (Hollnagel, 2004). Therefore, such models both have advantages and disadvantages since they may structure but at the same time constrain ones thinking. The benefits, however, is believed to outweigh the drawbacks since a model enables a common understanding of a phenomenon. An underlying intention of the model is to illuminate what needs to be considered in risk and vulnerability analyses that are applied in a context where the acute phase of emergencies play an important role for the final outcome of the emergency. It is

admittedly a rather simplified model of emergencies; however, that is the intention since it strives to be general in the sense that it aims to cover all, or at least a wide array of, emergencies.

The fundamental aspect of emergencies, disregarding their "magnitude", is that some people, industries, organisations, etc., that are being affected by a *hazard agent* or *perturbation* are not able to satisfy some of their *needs*. That is, they need some type of assistance by other actors to meet these needs. The hazards can be of different nature, such as man-made, natural, accidental, and intentional and so on. Although these hazards to a large extent differ, there are many similarities regarding how they affect a community. Therefore, much can be gained if an all-hazards approach is adopted, which is done in the present thesis. Furthermore, unless the needs that arise are not met in a specific time frame, depending on the need in question, *negative consequences* will arise. The severity of the consequences depends on the type of need in question. For example, if the assistance need is related to physiological needs (the first step in the well-known Maslow hierarchy (Maslow, 1954)), such as the need for water and food, the severity of the negative consequences will be high if the needs are unmet. As was the case in the definition of risk (section 5.1), a negative consequences is defined as a harm to something that human's value. The overall goal of emergency management is thus to protect this value system by designing or performing appropriate mitigation, preparedness, response and recovery activities.

At the very heart of the model is therefore the *value system*. Human values are socio-cultural constructions which mean that the values that are important to protect are likely to vary across different cultures. In addition, it is likely that values also vary over time. There is no absolute value system, instead the values have to be monitored and the activities performed, in for example a municipality, must be adapted to the situation at hand. In the research group of which the author is a part a six dimensional value system has been elaborated with (Abrahamsson, Johansson *et al.*, 2007). This proposal has not been established together with citizens or representatives from the public, which could be argued to have been preferable. However, it has been found to be a satisfactory value system by municipality officials who have been participating in analysis activities arranged by the research group. The six dimensions are human life and health, the environment, the economy, continuation of daily life and normal functions, constitutional value structures[3], and demands of societal resources for response.

[3] Constitutional value structures are about whether democratic principles are violated, and whether laws and regulations are not adhered to. Human rights, such as freedom of speech

Without claiming to be complete or optimal, these six dimensions provide an example of how to operationalize the value system in a specific context.

In the society there exist many different sources of "amplification" and "attenuation"[4] of the impacts that a specific perturbation have on the value system. It is the way these amplifiers and attenuators act on the specific perturbation that determines the seriousness of the negative consequences. This model will make a separation between five different types of attenuators and amplifiers; however, the boundaries between these categories can be somewhat fuzzy since there are large interactions and dependencies among them. The amplifiers in the model are social vulnerability, organizational and institutional vulnerability and infrastructural vulnerability, and the attenuators in the model are structural barriers and emergency response capabilities. The amplifiers above are labelled amplifiers since a higher "score", e.g. a higher social vulnerability, will lead to larger impacts on the value system, everything else being equal. The attenuators, then, of course implies an opposite relation to the impacts[5].

Social vulnerability is a concept frequently being used in the emergency management literature and several definitions and interpretations exist. In its broadest interpretation social vulnerability coincides with what can be termed *societal* or *community* vulnerability, i.e. a measure of the overall susceptibility of a society or community to withstand, respond to and recover from perturbations; however, in this model it is being used in a somewhat more restricted sense. Here it is about people's, households' and different social groups' ability to withstand, respond to and recover from the occurrence of a specific perturbation. *Organizational and institutional vulnerability*, then, is similar to social vulnerability except being applied to different types of profit and non-profit organisations, such as companies, governmental agencies and so on. Assistance needs will arise on those occasions where the exposed people, households, organisations etc. do not have

and equality before the law, that are violated are examples of harm to constitutional value structures.

[4] The two concepts are analogies drawn from the theory in the field of risk perception termed "social amplification of risk" (Kasperson, Renn *et al.*, 1988). According to the theory "risk events interact with psychological, social and cultural processes in ways that can heighten or attenuate public perception of risk and related risk behaviour". In the present thesis, instead of relating the concept to *perception of risk*, attenuators and amplifiers are rather seen as processes that either amplify or attenuate the damages on the value system caused by the occurrence of a perturbation.

[5] Of course, it is possible to formulate the attenuators as amplifiers by negating the meaning of the terms, i.e. lack of vulnerability etc. Above the most frequently used concepts were chosen.

enough capacity and capability themselves to withstand, respond to, or recover from the perturbation, such as lacking resources, skills, or knowledge. Different parts of the society, such as different social groups, are likely to exhibit different assistance needs of various magnitudes during an emergency since the vulnerabilities of groups and organisations vary. Research concerning social vulnerability often focuses on finding the root causes of social vulnerability and how it is possible to anticipate which needs that are likely to arise and which social groups are especially likely to require assistance (Morrow, 1999; Cutter, 2003; Cutter, Boruff *et al.*, 2003; Wisner, Blaikie *et al.*, 2004). Such knowledge is crucial for effective emergency management and for facilitating risk reductions.

Structural barriers are "more-or-less" static barriers built into the society with the purpose of reducing the impact a certain perturbation has on various systems that needs to be protected, such as social, institutional and infrastructural systems. The structural barriers thus try to mitigate the perturbation so that the intensity of it is less when the system to be protected is exposed. Such structural barriers include for example levees for flooding mitigation, and building codes with the purpose of ensuring the robustness of buildings to earthquakes and much more.

In order to meet the assistance needs that arise in an emergency or to prevent any future assistance needs to arise, various *emergency response actors* (governments, public or private organisations, NGO:s etc.) initiate responses in regards to the emergency. The assistance needs of an emergency thus put *demands* on the emergency response actors. Some scholars classify different types of demands into two categories; *agent-generated demands* and *response-generated demands* (Dynes, 1994). Agent-generated demands are demands that are direct effects of the specific hazard agent or perturbation that initiated the emergency. Response-generated demands, on the other hand, are those demands that stem from activities carried out by the emergency response actors to minimise the consequences of the disaster. To give an example, consider the Tsunami that struck South East Asia on Boxer Day 2005. Agent-generated demands included search and rescue operations, acute medical treatment, evacuation of populations, and so on. Response-generated demands included communication and coordination between the response actors, mobilisation of resources, establishing functions for situational data acquisition, and so on. The latter types of demands are often generic to all types of emergencies, while many of the agent-generated demands are specific to certain hazard agents. In the end, however, the success of the overall emergency response has to do with how well the agent-generated demands are met since these are related to the protection of human values. How well the response generated demands are met will of course have a large influence on how well the agent-generated demands are met.

In order to meet the demands, emergency response actors have to carry out a wide variety of *tasks*[6]. Some of these tasks are directly related to assistance needs, whereas others are more indirectly related, such as facilitation of the performance of other tasks or anticipation of future needs and subsequent prevention of these needs. How well or to which extent these activities and tasks can be performed depend on the *emergency response capabilities* of the emergency response actors. Often there are several *preconditions* that have to be met in order for an actor to perform a specific task. An example can be that another task needs to be performed before a specific task can be performed. As such, it is clear that there are large dependencies between the performances of different tasks; it is impossible to determine how well a certain task can be performed without considering the *context* of the task. Furthermore, to be able to perform a task, emergency response actors also have to have access to certain *resources*, such as having access to competent personnel or water to distinguish a fire, and the service of *critical infrastructures*, such as having electric power supply.

Critical infrastructures, broadly defined as large-scale socio-technical systems providing services to the society that are essential for its proper functioning, play important roles in the context of societal emergencies. It is important to note that "[a]lthough it may be the hardware…that is the initial focus of discussions of infrastructures, it is actually the services that these systems provide that are of real value to the public" (Little, 2002). Critical infrastructures can have at least two crucial roles in an emergency. First, they can be seen as attenuators that reduce the impact of perturbations on the value system. This is done by continuing to provide their services so that effective responses can be initiated and performed. Secondly, they can be seen as amplifiers by contributing to or even constituting the perturbation to the society if disruptions of the essential services arise. These arise either due to an inability to withstand external hazards (that may only expose the infrastructures or expose both the infrastructures and other systems), or due to internal failures. Assistance needs, then, arise from the fact that the "normal" services that people, organisations etc. rely on are disrupted. Furthermore, emergency response actors that perform tasks and activities to meet assistance needs are often also dependent on these services, which mean that the response to an emergency may be severely hampered. An issue is of course that the critical infrastructures can be affected by the same perturbation as the perturbation causing the assistance needs to arise. Consider a flooding situation, for example, leading to

[6] In the present thesis, a task is used to label something being done in an emergency. Other closely related concepts are for example activities and functions, which are taken to be synonymous to tasks.

the assistance need of evacuating certain affected areas. In order to do this emergency response actors need road access to the area; however, roads are possibly not accessible causing emergency response actors to be forced to choose other strategies for evacuation, possibly not as effective and efficient as evacuation by roads. Thus, the capabilities of the emergency response actors to perform tasks and activities can be severely degraded if they do not have access to the services and resources that they normally have access to. Assuming the resources and the services of CIs to be unaffected by hazards and perturbations when planning for emergencies can therefore lead to an underestimation of the efforts needed to respond to the emergency and an overestimation of the emergency response capabilities.

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 service they provide by making them more complex and interdependent" (Zimmerman, 2001). Dependencies and interdependencies between the critical infrastructures mean that disruptions in one CI can cascade to other infrastructures, causing secondary, tertiary and even higher-order effects, and in addition, effects can cascade back to the system where the disruption originated. The interdependencies can be of various types. Rinaldi, Peerenboom *et al.* (2001), for example, classifies interdependencies into four separate categories: physical (mutual dependencies among the material output exist between two systems), cyber (the state of an infrastructure depends on information transmitted through an information infrastructure, such as a SCADA system), geographical (the state of several infrastructures can be affected by the same event in their local environment), and logical (other types of interdependencies which especially are related to human behaviour, for example overload of the mobile communication infrastructure when there are disruptions in the telephone network). The complexity of this "system of systems" constitutes a serious challenge for risk and vulnerability analysis. Haimes and Longstaff (2002), for example, argue that it is not possible to understand cascading adverse effects on an ad hoc basis or using brainstorming-like methods. Rather, they argue, "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". An issue is that there are generally no actors in the society that have an overview of these critical infrastructures, neither is there anyone that has this responsibility (Amin, 2000). Furthermore, the ownership and operation of these infrastructures are increasingly distributed over a wide array of public and

private (national and international) organisations, leading to great challenges for analysing them from a holistic point of view. Several research initiatives exist with the purpose of modelling critical infrastructures from a holistic perspective, e.g. Haimes (2001), Dudenhoeffer, Permann *et al.* (2002), Brown , Beyler *et al.* (2004), Lee, Mitchell *et al.* (2004), Newman, Nkei *et al.* (2005), Min, Beyler *et al.* (2007); however, overall the state-of-the-art is still in a quite rudimentary stage (Little, 2002; Rinaldi, 2004).

It is important to note that the model described and discussed above is a crude representation of a real emergency. A more detailed model would for example divide the response to an emergency into different temporal phases, such as detection, reaction, mobilization etc. However, as mentioned earlier, the crude representation is intentional since the purpose of the model was to represent emergencies generally and capture the most important characteristics of these.

3.6 Reflections on the model: implications for risk and vulnerability analysis

The intention of the model presented above was to illustrate the fact that there are many factors that need to be accounted for in a risk and vulnerability analysis in an emergency management context, since there are many factors that influence the unfolding of the risk scenarios. Especially interesting is the double-edged role critical infrastructures play in an emergency, that is, they provide indispensable services to the society thus facilitating the response, while at the same time pose a serious threat to the ones dependent upon their services if disruption would occur.

A problem with the model is that the identified factors are very much intertwined and it can be difficult to make distinct separations between them. For example, in many cases different people, households and social groups have different access to the services of infrastructures. So although social groups with a low access to the service of an infrastructure (such as a less reliable access) are not necessarily more vulnerable to infrastructure disruptions per se than other social groups, disruptions are more likely for such social groups – leading to greater impacts there – given the manifestation of a hazard. The infrastructural vulnerability will thus cascade into a type of social vulnerability that will vary among different groups in the society. This also shows the importance to study the relations and interactions between the different amplifiers and attenuators, not just each in isolation. Different factors may for example compensate for weaknesses in other factors, e.g. the lack of structural barriers to certain threats may be compensated by well developed emergency response capabilities of the response actors. In order to gain a complete

picture of the risks and vulnerabilities in a community, all these factors and interactions therefore need to be studied.

The complexity of an emergency situation constitutes great challenges to risk and vulnerability analyses. There are two main reasons for this: the many dependencies and interdependencies, and the importance of human actions and responses. The fact that there are many dependencies and interdependencies implies that it is difficult to partition an analysis into sub-analyses. For example, analysing emergency response capabilities and assistance needs separately may lead to misleading results. This is because the two factors are not independent, since if the emergency response actors can satisfy the assistance needs in a timely manner, they may prevent future ones from arising. On the other hand, if the emergency response actors are not able to satisfy assistance needs, new needs may be created. There are of course pragmatic reasons for separating analyses into several sub-analyses, such as separating analyses of individual infrastructures, analyses of social vulnerability and assistance needs, analyses of demands on emergency response actors, analyses of emergency response capabilities, and analyses of structural barriers, since analysing "everything at the same time" may be a too arduous task. However, then the interactions between the different units of analyses must also be studied in order to integrate the findings into an overall picture of the risks and vulnerabilities.

The other reason for the great complexity is the fact that human actions and behaviour play such an important role in emergencies. In the traditional technical risk analyses, human behaviour basically did not have a role in the analyses; it was rather only the technical aspects of the systems that were studied in the analyses. More recently, quantitative risk analyses started to incorporate human aspects and behaviours into the analyses, but only in terms of the behaviour of operators in for example nuclear power plants. The field of Human Reliability became a great contributor to risk analysis by first providing methods for estimating probabilities of human errors, and later to investigate how the performance conditions and the context affect human actions (Fujita and Hollnagel, 2004). However, still the main focus is on avoiding the occurrence of accidental events, not so much on studying how these events subsequently are responded to by affected systems and emergency response actors.

In taking a broader view of emergencies it is clear that human and organisational behaviour play important roles for emergency management, not primarily as sources of errors, but as sources of resilience and capability to minimise impacts, i.e. people and organisations act as attenuators during an emergency. Descriptive studies of emergencies and crises, such as case studies, can provide important

insight into which characteristics people and organisation should attain in order to initiate and maintain a good response to emergencies. Often these studies emphasize the importance of factors such as adaptability, flexibility, improvisation and creativity, since in many cases things do no not develop according to what was expected on beforehand. Findings from the emergency management field, therefore, can provide vital input to risk and vulnerability analyses by helping the analyst to understand how different characteristics of people and organisations affect performance during a response.

To conclude this chapter, it is clear that taking a broader view of emergencies and accounting for more factors in risk and vulnerability analyses will lead to a higher degree of complexity. Human actions and performance are often difficult to predict, meaning that it is difficult on beforehand to know how an emergency will evolve. Another feature that adds to the complexity is that in an emergency situation there are often several value dimensions that are relevant, e.g. number of fatalities is often not the only dimension of concern. In attaining a complete picture of risk, therefore, one must model how all relevant value dimensions are affected in an emergency, clearly requiring a greater modelling effort. Much research is definitely needed in order to satisfy these research demands.

4 Approaches to understand, model and analyse complex systems

The present thesis is essentially about the problem of analysing risks in and vulnerabilities of complex systems. In order to do that, we must explore different ways of making sense of such systems. In the research literature there are several approaches and suggestions available. In this section an overview of three general and broad approaches will be given, which have been influential to the research presented here. The three approaches are:

- Systems theory and the systems movement,
- Complexity theory and the theory of complex adaptive systems,
- Network theory and analysis.

4.1 Systems theory and the systems movement

Systems theory, and the systems movement as it is sometimes broadly referred to, is a set of interrelated and somewhat overlapping disciplines with the attempt to "explore the consequences of holistic rather than reductionist thinking" (Checkland, 1993), that is, to focus "on systems taken as a whole, not on their parts taken separately". What is especially interesting to study are systems that display organized complexity, i.e. too much complexity to allow for analytic approaches and too much regularity to allow for statistical approaches (Weinberg, 1975). Ashby argues that when concerned with simple systems, the traditional scientific approach of isolating factors and "varying the factors one at a time" is possible, but not when concerned with more complex systems, since changing one factor cascades into changes in other factors too (Ashby, 1957). This fact is in the centre of the systems approach and is referred to as the "strong connection law" by Weinberg (1975).

The modern version of systems theory evolved in the aftermath of the Second World War, where pioneers such as Norbert Wiener and Ludwig van Bertalanffy conducted research on Cybernetics and General Systems Theory, respectively. These researchers observed that different scientific disciplines became increasingly specialised which made communication among the disciplines increasingly difficult. What system theoreticians tried to do was to promote the "unity of science" by developing a meta-discipline that sought to facilitate the communication between different specialists by developing a common language. Boulding, for example, argued that "General Systems Theory is the skeleton of science in the sense that it aims to provide a framework or structure of systems on which to hang the flesh and blood of particular disciplines and particular subject

matters in an orderly and coherent corpus of knowledge" (Boulding, 1956). What was also observed by the "systems pioneers" was the high degree of isomorphism between different scientific disciplines. In systems theory, therefore, some researchers try to identify "universal" laws which are applicable to many different disciplines. The utility of such laws is that they can provide hypotheses about phenomena in disciplines other than from which the laws were derived. The "laws" thus can give suggestions of how to study phenomena and where to look for the answers (Ashby, 1957); however, they do not "give" the answers since they are based on inductive inferences (Weinberg, 1975). Making such analogies between different types of disciplines or systems is one fundamental aspect of systems theory.

Another part of systems theory, perhaps the most significant, is the discipline that is concerned with applying systems thinking to practical problem-solving, labelled "systems practice" by Checkland (1993). What are of interest to "system practitioners" are problems in the real-word with all its complexity. Since the concern is problem-solving, systems practice is very close akin to engineering in general. In the field of systems practice, methodologies, frameworks and guidelines have been developed in order to facilitate problem-solving. Systems engineering, systems analysis, systems dynamics and decision aids from decision theory are examples of developments in this field. Furthermore, methods and techniques for performing risk and reliability analyses can also be said to be a part of the development in the field of systems practice, and have largely been influenced by systems theory, which will be seen in chapter 5 where the foundations of risk and vulnerability analysis is addressed.

4.1.1 Distinguishing the real-world system and the system model

Central to systems theory is the existence of a real world system of some type (e.g. technological, socio-technical, biological) that someone wants to make sense of, or solve a problem with regards to, e.g. an electric power distribution system or a municipality. Prima facie it might be easy to conclude that the system is 'the thing in reality that is being studied'. However, as Ashby points out, there are fundamental disadvantages with such an approach, because "every material object contains no less than an infinity of variables and therefore of possible systems" (Ashby, 1957). It is impossible to include all facts and aspects of the real phenomena when studying it. The pragmatic (the only!) way to proceed, which is adopted in systems theory and in the present thesis, is that the investigator selects the factors that are relevant in a certain situation and "those which are relevant may change with changes in the purpose of the research" (Ackoff, 1971). The chosen

factors, variables and properties are then incorporate in the "system" being studied, as such, a system is essentially a "human-made model" (Ropohl, 1999). The models can be specified in various ways, from formal mathematical or logical models to graphical representations of the real system of interest. But these models have in common that they stem from a mental representation of the real system of interest (Cook and Ferris, 2007). Due to the fact that the system is a model of the 'real thing' the system definition and description is somewhat dependent on the person making the description; the investigator chooses the factors to include and which factors that are relevant in a specific context depends on the purpose of making the description. This characteristic is captured by Weinberg when he defines a system as "a point of view" (Weinberg, 1975). However, although the system definition is somewhat subjective it is not relative in the sense that it is impossible to judge the appropriateness of the description, only that there might exist many definitions that are equally valid in the sense that they define the real phenomenon from different perspectives. This view is also supported by Haimes when talking about models in risk analysis: "more than one mathematical or conceptual model is likely to emerge; each of these focus on a specific aspect of the system, yet all may be regarded as acceptable representations of the system" (Haimes, 1998). As a rough guideline regarding which factors to include in the system description, Weinberg's rule of thumb can be used: "simplicity is what determines the right set of factors " (Weinberg, 1975).

In the simplest form, a system can be defined as "a set of elements and a set of relations between these elements" (Ropohl, 1999). In this interpretation, a system is a structural concept; however, Ropohl argues that it is also possible to interpret a system as a functional concept, where the system transforms some input to some output. In practice, these interpretations complement each other. The former interprets the system concept as a "white box" where the internal elements and relations can be studied, while the latter interprets the system concept as a "black box", where the inputs, functions and outputs are of interest. In the present thesis, these two definitions are amalgamated and a system is therefore seen as a set of element, their internal relations that taken together perform specific functions by transforming some inputs to some outputs.

4.1.2 Some systems concepts

In any application of systems concepts it is important to clarify which elements that the system is comprised of. This can be done by specifying the *system boundaries*, i.e. distinguishing between what is part of the system and part of the *environment*. Indirectly the system boundaries can be specified by "listing the variables that are to be taken into account" (Ashby, 1957), which is Ashby's suggestion of how to define the system. Ackoff argues that the "system's

environment consists of all variables which can affect its state" (Ackoff, 1971). Simon makes the same distinction between a system and its environment but uses the words inner and outer environment (Simon, 1996). Systems can have different relationships to their environment and consequently be classified as *open*, *closed* or *isolated*. Open systems are systems that interact with (receive input from and yield output to) their environment (Skyttner, 1996). A closed system only exchanges energy with its environment, whereas isolated systems are hermetically closed, i.e. they have no environment. The systems that are of interest here are predominantly open systems, which imply that it is not sufficient to only consider the system, it is also important to study its context.

Another important concept in systems theory is *state variables*. A state variable[7], u, is used to describe different elements of the system. If considering a human being, for example, the state variables can be body temperature, heart rate, breath rate etc. Each of these variables can take on different states, which often vary over time; the heart rate, for example, naturally increases when a person is exercising. The system's overall state, U, can then be defined as the states of each of the variables (u_1, u_2…., u_n) of which the system is composed (Ashby, 1957). *All* possible states of a system can be represented in the *state space*[8] of the system, thus each point in a state space corresponds to a unique system state, U. Furthermore, in order to represent a system's dynamical behaviour, the concept of *trajectories* can be used. A trajectory can be defined as the succession of states that a system is taking on over time (U_1, U_2…., U_k) when *transformations* are taking place in the system. All these concepts will be relevant for the subsequent discussion of risk and vulnerability in chapter 5.

4.2 Complexity theory and the theory of complex adaptive systems

Complexity theory, including the somewhat narrower theory of complex adaptive systems, is an emerging field with many features that are similar to systems theory; however, much of the literature in systems theory is "virtually unacknowledged in the complexity literature" (Phelan, 1999). Both fields were essentially products of the discontent related to the traditional reductionistic method of inquiry, which were argued not to be possible to use when studying complex systems and as a consequence both fields urge the importance of also studying the interactions

[7] The choice of notation is arbitrary; however, in order to avoid confusion with subsequent notations the letter u was chosen to represent a state variable

[8] Sometimes the term *"phase space"* is used instead of state space, but with the same meaning.

between different parts of systems. Both fields also express an ambition to discover general and universal laws that govern many types of systems. Gell-Mann argues that complexity scientists are beginning to find such universal laws, or rather, universal principles that are applicable to a wide range of complex systems (Gell-Mann, 1997). Furthermore, complexity theory and systems theory share similar terminology, such as concepts like emergence, systems, dynamics, and hierarchy and so on (Phelan, 1999).

On closer inspection, though, there are significant differences between complexity theory and systems theory. First, the attitudes towards complexity are different in the two fields. A hallmark of complexity theory is the belief, or assumption, that complex global patterns (emergent properties) arise from simple underlying rules (Epstein, 1999; Lewin, 1999; Phelan, 1999; Axelrod and Cohen, 2000; Phelan, 2001). Thus, according to complexity theory, complexity may actually be ostensible, which is elegantly captured in the Murray Gell-Mann's phrase: "surface complexity arising out of deep simplicity" (Gell-Mann, 1997). Systems theory sometimes has the totally opposite belief: that apparently simple causes in fact are of a more complex nature (Phelan, 2001).

This belief has consequence for the approach that complexity scientists use to understand complex systems. Instead of trying to understand a system by identifying positive and negative feedback loops between variables that might themselves be systemic properties, which is sometimes done in systems theory (e.g. in systems dynamics) (Anderson, 1999), complexity theorists "drops down a level to explain the rules that govern the interactions between lower-order elements that in the aggregate create emergent properties in higher-level systems" (Phelan, 2001). The difference thus lies in whether systemic properties are explained by casual drivers on the same level of analysis or on a lower level of analysis (Anderson, 1999). To model a complex system, complexity theorists therefore, in contrast to systems theorists, often use bottom-up, agent-based approaches, where emergent global structures arise from the interactions among the agents. Furthermore, complexity theorists argue that the emergent structures often affect the interactions among the agents thus leading to top-down causality as well (Lewin, 1999). The goal of an agent-based simulation is to identify the rules that the agents follow on a local level, such as how they interact with other agents, so that the global emergent properties resemble with what is actually observed in the real world system of interest. Epstein uses the term "generative laws" to label the local rules (the micro-specification) of the agents that are sufficient to generate the observed macroscopic behaviour of the system (Epstein, 1999).

4.2.1 The theory of complex adaptive systems

The theory of complex adaptive systems (CAS) can be said to be a subset of complexity theory in that it is about a special type of complex systems, namely systems "where many players are all adapting to each other and where the emerging future is extremely hard to predict" (Axelrod and Cohen, 2000). Axelrod and Cohen claim that the theory of CAS is not really a theory in the sense that it is possible to falsify; it is rather "a way of looking at the world" (Axelrod and Cohen, 2000). Central to this way of looking at the world are *agents*[9]. Agents have abilities to interact with its environment, such as with other agents. What an agent corresponds to in the real world is dependent on the real world system that is studied and the level of detail that is chosen by an observer or an analyst. In a social system, agents can correspond to a person, a married couple, an organizational division, an organization and so on. Significant for agents is also that they have *purposes* and *goals* that they try to pursue by using various *strategies*. By changing the strategies, i.e. trying to *adapt*, an agent can increase its *fitness* (more effective goal achievement). Furthermore, agents often have memories and a location, which might affect how the agent acts in a certain situation. The strategies dictate an agent's actions based on his perception of the environment and his believes about how his goals are to be pursued. Strategies can thus be said to be constituted by a set of decision rules. It is important to note that agents only have access to the information in his local environment, thus no agents have access to complete information (Anderson, 1999). Furthermore, the strategies can evolve over time due to the fact that they can observe the effectiveness of their strategies through some *measure of success*. In addition to agents, *artefacts* may also exist. Artefacts are similar to agents in that they have capabilities to affect its environment and locations; however, they do not have any goals of their own but are used by agents. Typical artefacts are man-made objects and material resources of various kinds.

In cybernetics (a branch of systems theory), the behaviour of designed systems (such as robots) are often controlled by stipulating an internal model for how the system should act when it obtains information from its sensory components, i.e. defining the system's strategies, for example using feedback loops to create a reaction to various stimuli. The difference between a cybernetic system and a CAS is that the model used by the system to react to its environment is fixed, whereas a CAS learns from its actions and tries to adapt in order to find better ways of acting in regards to its environment (Gell-Mann, 1997). However, as Gell-Mann also points out, if we where to include broader aspects of the cybernetic system, such as human designers and such, in the system description it would be regarded as a CAS

[9] The central components of a complex adaptive system described in this section are mainly based on the framework suggested by Axelrod and Cohen (2001).

since human designers have the ability of modifying the internal model of the cybernetic system in order to develop its abilities.

4.3 Network theory and network analysis

Network theory contains a body of knowledge that can be used to describe, analyse and understand complex systems (Amaral and Ottino, 2004). Network theory stems from graph theory, a branch of discrete mathematics, which was founded by Euler in the 18th century. In the first half of the 20th century sociologists started to use networks, or sociograms which is a synonym sometimes used by sociologists, as a representation of different types of relations between individuals and groups. This branch of sociology came to be referred to as social network analysis (Scott, 2000). In the mid 20th century the two mathematicians Erdös and Renyi started to study random networks, a specific type of theoretical network model, which allowed for a statistical approach towards understanding such networks. Over the last couple of years, however, the interest in using network theory and network analysis to study real, complex systems has increased rapidly. Instead of only focusing on the properties of random networks, researchers have found other types of theoretical network models that can be used to represent or approximate, and subsequently understand, many types of complex systems, e.g. small world networks (Watts and Strogatz, 1998) and scale free networks (Barabási and Albert, 1999). Albert and Barabási (2002) argue that there are four main reasons for the increased interest in network theory. First, the computerization enables the collection of data regarding large-scale systems. Secondly, the increased computing power makes it possible to address questions that where previously impossible to address. Thirdly, researchers have found that there are generic properties of complex networks. Finally, there has been an advocacy of moving beyond reductionist approaches and instead try to understand the systems as wholes.

In network theory a system is represented as a network composed of nodes and edges. Depending on which types of system (e.g. technological, social, biological, informational) that is modelled, the nodes and edges are representing different things. In a social network a node can be an individual or a group of individuals, whereas an edge is a relation between individuals, such as a friendship tie or a family relation. In a road network a node can be a junction and the edge can be the road that connects different junctions. The main reason for studying the network representation of complex systems is that "structure always affects function" (Strogatz, 2001). So by studying the structure of a system and of how different parts of the system interact, it is possible to "understand and explain the workings of systems built upon those networks" (Newman, 2003). Over the years, network theorists have developed many measures that can be used to describe and subsequently understand a specific network. These properties are either local, e.g.

the number of other nodes a specific node is connected to, or global, e.g. the average number of other nodes that the nodes in a network are connected to. The purpose of this section is not, however, to give a review of these measures so the interested reader is directed to any of the following references: Albert and Barabási (2002), Barabási (2002), Dorogovtsev and Mendes (2002), Newman (2003), Holme (2004) and Watts (2004).

Holme, Kim *et al.* (2002) argue that there are three main interests in current network studies. First, studies concerned with developing algorithms that regenerate the real-world network structures. Such regeneration makes it possible to understand the processes that underlie the evolution of different types of networks. The work presented in Watts and Strogatz (1998) and Barabási and Albert (1999) are two pioneering examples of studies in this category. Secondly, studies concerned with the effect of the network structure on the dynamics of the system. Thirdly, studies concerned with how restrictions imposed on the networks affect network performance. In the present thesis the major interest is in the last mentioned category; to which extent disturbances and perturbations to a system negatively affect the function of the system and subsequently to what extent the loss of function lead to harm on the underlying value system.

To be able to interpret the various network measures and characteristics that can be derived, theories of course has to exist regarding the relation between the structure and function of a specific network. A common way to calculated network performance is by measuring the connectedness of the network, for example whether there exist paths between all nodes to all other nodes or the average geodesic length[10] between all pairs of nodes in the network. Such measures might be relevant to some systems, but less relevant to other. In a technical infrastructure network, for example, there has to exist a path between nodes which customers are connected to and the nodes that generate, or feed in, the specific commodity provided by the infrastructure system. Whether there exist paths between *all* pairs of nodes is less relevant in such systems. The point here is that performance measures that are being employed have to be adapted to the specific system of interest, since the relation between structure and function differs for different types of systems.

[10] A geodesic length is the length of the shortest path between two nodes in a network. With length in this case is meant the number of edges that need to be traversed before reaching the other node.

4.4 Reflections related to risk and vulnerability analysis

The overarching purpose of this chapter has been to give a brief overview of a couple of general approaches to study complex systems, which have been influential to the research presented in the present thesis. It was very difficult to keep the overview brief due to the fact that the "paradigms", systems theory in particular, are very broad. In addition, there are often diverging views regarding the content of the paradigms and this review is not claiming to address all relevant characteristics and diverging claims about them. What is especially important to note is that these disciplines not should be seen as mutually exclusive approaches to understand and analyse complex systems. On the contrary, many principles are acknowledged by all disciplines and in many senses the disciplines overlap or complement each others and can be used in conjunction. The clearest commonality between the disciplines is the migration from reductionistic thinking to holistic thinking. All disciplines can be said to follow the "systemic principle" which "emphasises the understanding of the interactions between agents [or components] and looks for the nature of the relationships between them, instead of decomposing the system into parts, to study them independently (Le Coze, 2005).

With the concern of holistic thinking, common to the three disciplines, comes a concern of capturing emergent behaviours; however, what differs between the approaches is the means of capturing these behaviours. In systems dynamics, for example, top-down approaches are used, where causal relationships between variables on the same system level are investigated and modelled. In agent-based simulations, on the other hand, bottom-up approaches are used where units and relationships between units at a lower system level are specified in order to come at conclusions about emergent, system-level properties. Proponents of the two different approaches sometimes argue that using the opposing approach inhibits the possibilities of capturing emergent properties. An "always preferable" approach is however not believed to exist; instead the appropriateness of an approach must be decided on in the context of the particular situation and problem at hand; however, using both approaches in parallel when analysing a complex system may very well provide complementing insight into the system's function.

The field of risk and safety engineering is already today largely influenced by the systems movement and can be seen as a branch of systems engineering (Haimes, 1998). However, the focus in this field has not always been on *system-level* properties. Earlier the focus of risk management and related paradigm was on reliability and risk for *individual components* and *devices* (Saleh and Marais, 2006). Saleh and Marais argue that it was during the 1970s that system-level safety,

reliability etc. became the foci of the studies. Much of the developments took place in the oil, gas, chemical and nuclear industries and where the Rasmussen report (Rasmussen, 1975), mentioned in chapter 1, was one of the pioneering efforts. Still, however, there are researchers who argue that many of the methods for risk analysis are not able to capture "systemic accidents". Hollnagel, for example, argues that systemic models of accidents, which has implications for risk analysis as well, go beyond causal chains and try to describe system performance as a whole, i.e. it views safety as an emergent property, where "the steps and stages on the way [to an accident] are seen as parts of a whole rather than as distinct events" (Hollnagel, 2004). It is not only interesting to model the events that lead to the occurrence of an accident, which is done in for example event and fault trees, but also to capture the array of factors at different system levels that contribute to the occurrence of these events. Such as factors stemming from the local workplace, factors on management, company, regulatory or governmental level and finally also factors associated with social norms and morals. The main point of the systems-oriented approach to accidents, which is also acknowledged by Leveson (2004a), is that a single factor is seldom the only "cause" of an accident; it is more common that the "cause" stems from a complex set of factors and their interactions.

As a conclusion of this chapter it is argued that all three general approaches, described previously, can be seen as frameworks for understanding and analysing complex systems. The systems of interest in the field of risk and emergency management often involve elements and sub-systems of various types, such as social, technical, natural, organisational, biological, and so on. Any approach used for analysis in such a context needs to be able to incorporate these multidisciplinary aspects of risks and emergencies. The described approaches, taken separately or used in conjunction, provide methods, tools, concepts, and a vocabulary for addressing such systems and they have been an important source of influence to the present thesis, which will be seen in the following chapters. Furthermore, it is very clear today that we need to make use of well developed and appropriate methods in order to gain insight into system with extensive interactions among its components. Our abilities to use "pure brainstorming" and intuition alone for analysing risks and vulnerabilities of such complex systems are simply not sufficient, because even a small amount of feedback loops, dependencies and interdependencies make it difficult to grasp how a system's behaviour will change over time.

5 Operational definitions of risk and vulnerability

The concepts of risk and vulnerability are central to the present thesis; however, since these are applied over a wide range of research disciplines and professions the interpretations of them often vary. Efforts initiated to try to develop standard, "universal" definitions of such concepts seldom succeed. An example is the effort initiated by the Society for Risk Analysis to define risk, where a committee labored with the concept for 4 years before it gave up, concluding that "maybe it's better not to define risk. Let each author define it in his own way, only please each should explain clearly what that way is" (Kaplan, 1997). Not clearly defining the concepts when they are being used can potentially be a serious problem. This chapter therefore aims at providing such clarifications by presenting definitions of both risk and vulnerability. It is not claimed that the proposed definitions are the only ones possible or the best ones in every situation. However, experience with use of the definitions, gained by the research group in which the author is part, has been successful. In addition, the definition of risk that will be described has been frequently used in the risk field for more than two decades.

Primarily this chapter will give a review of how the concepts of risk and vulnerability commonly are being used in the fields of risk and emergency management. In addition to reviewing the concepts, the chapter will describe how the concepts, especially vulnerability, have been developed in the research group in which the author has been a part. The development mainly stems from a perceived need for developing and operationalizing the concept of vulnerability and to clarify the important role played by values in defining, analysing and evaluating risks and vulnerabilities.

The definitions given in this chapter are of operational type. An operational definition is a special type of definition that has its roots in the methodological position advocated by Percy Bridgman in the beginning of the 20th century (Ennis, 1964). What characterises an operational definition is that it provides an operation, procedure or method that can be used to measure (if quantitative) or characterise the concept (if qualitative) of interest. In the social sciences operational definitions are common, since concepts that are investigated there are often quite abstract, such as the psychological states of happiness or distress or the distributions of power in groups. In such cases and in many other cases as well, it is important be specific about the concepts and as Ennis argues; "concreteness is one of the virtues of operational definitions" (Ennis, 1964). Furthermore, defining concepts in an operational way provides a means for other scholars to understand them and how

they are being employed in a particular study. The possibility for an external researcher to critically review scientific work is also enhanced if abstract concepts are operationalized, which in turn will increase the quality of a scientific discipline in the long-run. Operational definitions also exist in the hard sciences, such as in physics, where elementary entities such as length and mass can be defined in operational terms. Since many of the concepts used in the field of risk and vulnerability analysis are not straightforward, operational definitions are very useful there too. This is because they can guide the work of developing methods for measuring/characterising a concept, guide the work of measuring/characterising a concept for a specific system of interest, or guide the work of evaluating an existing method for measuring/characterising a concept.

It is important to note that in this thesis a distinction is made between a method for measuring risk or vulnerability and an operational definition, in that the operational definition provides an ideal or theoretical way of measuring the concept, whereas a method provides a practical way to comply with the operational definition, at least approximately. In practice, there are many aspects that affect the appropriateness of using different methods for complying with the operational definition, such as the resources available, the analysts' competence, the scientific knowledge available about the system of interest etc. Which method to choose, if there are several methods available that all comply with the operational definition, is thus contingent on the particular situation and system being studied.

5.1 The concept of risk

The concept of risk is used in many scientific disciplines and is also a frequently used word in daily life. As a consequence the word has many different meanings, some quite dissimilar, while other only subtly different. There are different views of where the word risk originally can be derived from. One suggestion is that it stems from the Greek word *rhiza* which refers to the "hazards of sailing around a cliff" (Covello and Mumpower, 1985). Another suggestion is that it stems from the early Italian word *risicare* meaning "to dare" (Aven, 2003). From these basic denotations the concept has been transferred to English with the meaning somewhat altered; however still referring essentially to the same basic concept – uncertainties about future outcomes and potential for damages. In the present thesis, a distinction will be made between three different interpretations of the concept of risk (the reader is directed to Hansson (2004) and Rosing (2003) for a more thorough overview of different perspectives on the meaning of risk):

- Risk as a probability or frequency. When the concept of risk is used in this way it is often explicitly posited what the probability relates to in terms of

negative consequences. Examples are "the risk of dying in a car accident is 1% per year" and "the risk of catching a cold is high".

- Risk as a circumstance that increase the likelihood or consequence (or both) of adverse events. The circumstance can either be physical, e.g. the existence of flammable liquids near ignition sources, or an activity, e.g. driving the car in a high speed.
- Risk as a combination of the probability and the negative consequences of adverse events.

The two first interpretations of risk are quite common in everyday expressions, whereas the latter way of interpreting risk is the more common in the field of risk research. In what follows, risk will therefore predominantly be used with this interpretation in mind.

Two main features exist in all, or at least most, definitions of risk; a distinction between possibility and reality (Renn, 1998). This implies that in order for a risk to "exist", there has to be *uncertainties* regarding the future outcomes of a system and there has to be a potential that some observable variables (variables representing states of "the world") of interest take on adverse values (Kaplan and Garrick, 1981; Aven, 2007). In essence, risk (when defined in this way) exists in almost every activity or in every aspect of human life. Furthermore, it is important to point out that risk can be defined either *generically* or *specifically*. Risk, as it is referred to above, complies with a generic definition; however, when risk is to be used in a specific situation, what is regarded as the negative consequences, i.e. the observable variables of interest, have to be specified, thus transforming the generic definition into a specific one.

When defining risk in a specific situation, it will *always* express "someone's views regarding the importance of different adverse effects" (Fischhoff, Watson *et al.*, 1984). The phrase "someone's views" in the citation refers to the values basis for the specific analysis. A generic definition of risk that is in accordance with this view is proposed by Ortwin Renn, who argues that risk should be defined as the "possibility that human actions or events lead to consequences that affect what humans value" (Renn, 1998). Clarifying the value basis that is used is an essential first step before any risk analysis can be carried out, since it is otherwise impossible to know which observable variables of the system that should be studied. Commonly, the value basis for a risk analysis is implicit, in that it is not explicitly stated which values are used but it is possible to derive these values by identifying which observable variables are of interest in the analysis. In many cases, though, the value basis is not analysed in detail, but rather represents the analyst's values or his/her preconceived notions about the relevant stakeholders' values. In any case,

the value basis should be made explicit in an analysis, since this facilitates a critical review of the analysis.

Often distinctions are made between the concepts of risk, hazard and threat. In most distinctions hazards and threats are seen as underlying sources of danger (Kaplan and Garrick, 1981; Aven, 2007), i.e. something that has the potential for causing harm to the system of interest, being either internal or external to the system. Any risk reduction measure aims to either prevent the hazard from materialising in the first place or to reduce the harm on the system caused by the occurrence of the hazard. In the present thesis, the concept of hazard and threat are used interchangeably, however note that in the research literature these concepts are sometimes separated by viewing threats as stemming from an intentional source, such as a terrorist cell or a saboteur, whereas hazards are seen as non-intentional, such as natural phenomenon or accidental sources of danger (Haimes, 2006).

5.1.1 Models in risk analysis

In order to conduct a risk analysis a model of the real-world system has to be constructed. By subsequently analysing the model, knowledge regarding potential future unwanted consequences can be gained (Nilsen and Aven, 2003). How to construct the model of course depends on many factors, such as the type of real-world system that is of interest, the resources available in conducting the analysis, the consequence dimensions of interest, and the available input data and so on. There is, however, a fundamental trade-off between the accuracy of the model and the practical applicability of it (Aven and Kristensen, 2005). Aven and Kristenesen argue that the main task of the risk analyst is to achieve a proper balance between simplicity and accuracy and this balance must be related to the purpose of the analysis. For some purposes there is a need for great accuracy, whereas for other purposes a very rough system representation might be enough. This is nicely captured by Nilsen and Aven (2003), who argue that in defining the system model, a risk analyst must "provide satisfactory representation of the system under study against the simplicity required for analysis purposes".

In many methods for risk analysis, however, the analyses are conducted without necessarily explicitly defining the system, i.e. analyses are carried out on people's mental representations (Leveson, 2004b). Not defining systems explicitly can potentially imply that people involved in the risk analysis process are talking about "different systems", causing communication problems, controversies regarding which aspects of the real system that should be incorporated in the analysis and so on. If the systems instead are explicitly defined at an early stage of the risk analysis, discrepancies in the mental models between different people can be overcome or at

least made explicit and discussed. Explicitly defining the system of interest is especially important for highly uncertain situations with high stakes, since it is especially likely that different stakeholders may have different views of the system. Hatfield and Hipel (2002), in describing an actual case involving three stakeholders each conducting a risk analysis on the same underlying system, argue that "[e]ach party brought to their assessment a unique perspective, which was manifested as a different definition of the system during the problem formulation". In addition, since neither of the parties was aware of the fact that their views on the system definition differed from the other parties' views, the arguments put forward by a party did not make any sense to the other parties. Explicitly defining the system is therefore an important step of a risk analysis, in order to overcome controversies at an early stage, or at least make the analysis transparent and possible to critically scrutinize.

5.1.2 The quantitative definition of risk: scenarios and the set of risk triplets

In the early 1980s, Stanley Kaplan and John Garrick published their view of how to define risk (Kaplan and Garrick, 1981). They referred to this definition as "the quantitative definition of risk" and the definition they proposed was of operational type. The original definition was later somewhat modified and refined (Kaplan, 1997; Kaplan, Visnepolchi *et al.*, 1999; Kaplan, Haimes *et al.*, 2001). In the field of risk analysis, this definition has been used extensively and it will be briefly reviewed in what follows.

Central to the quantitative definition of risk is the notion of scenarios. A scenario expresses a possible way that a system can behave in the future and more formally it can be "viewed as a trajectory in the state space of a system" (Kaplan, 1997). Thus, a scenario can be described as a succession of system states over time (U_1, U_2…, U_k) as illustrated in Figure 5-1. Since there are uncertainties regarding the future behaviour of the systems of interest to risk analysis, there exist many possible scenarios. The type of scenarios of interest for risk analysis is referred to as *risk scenarios*, S_α. A risk scenario is a special type of scenario in that it deviates from the "success scenario", S_0, or the as-planned scenario which it is also called. The success scenario defines the ideal state of the system over time, i.e. when everything works according to the plan, when it is not exposed to any perturbations etc. The first step in a risk analysis is therefore commonly to define the success scenario since this will simplify the identification of risk scenarios.

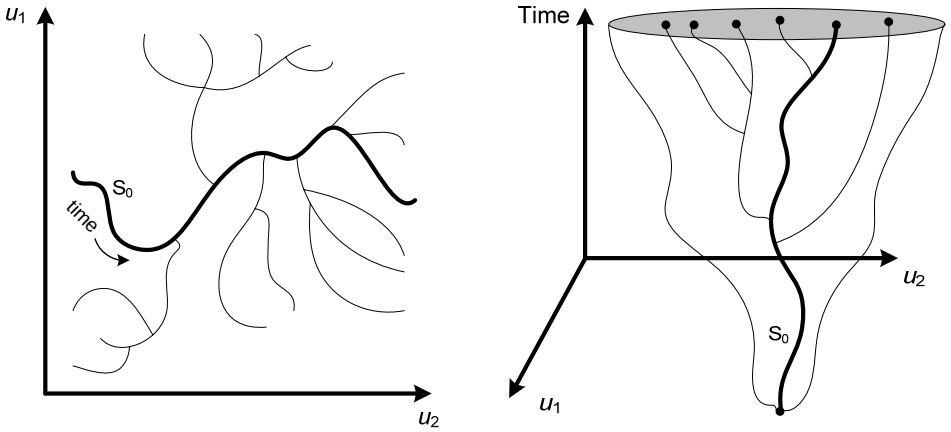


Figure 5-1. Illustration of risk scenarios (deviations from the success scenario) by use of a geometrical state space representation. To the left is a two-dimensional representation and to the right is a three-dimensional representation of a state-space. The difference between the two representations is that in the 3-dimensioal representation time is explicitly represented on the z-axis, whereas for the 2-dimensional representation time is represented along the trajectories.

What characterizes a risk scenario is that it can lead to negative consequences, X_α. From the definition of risk proposed by Renn (section 5.1) a negative consequence is something that harms what is of value to humans. What is of value to a specific person might not be of value to another person, since values are inherently subjective. Due to this fact, any estimation of risk is fundamentally subjective in the sense that it expresses someone's view of what should be regarded as negative consequences. As Hansson argues, when the tourist talks about rain as a negative outcome, the farmer talks about it as a blessing (Hansson, 2005). Objective or absolute risks, in this sense, simply do not exist. Furthermore, in most cases several dimensions of consequences are relevant to accurately capture the adverse effects of a potential event. This can be expressed by a vector composed by different consequence attributes (X_1, X_2….X_n), e.g. number of fatalities, number of serious injuries, number of minor injuries. In order to, for example, facilitate the comparison between risks, these attributes might be aggregated into an overall "hybrid measure" by expressing the trade-offs between the attributes. Methods from multi-attribute utility and value theory are often useful for such purposes, e.g. Keeney and Raiffa (1976), von Winterfeldt and Edwards (1986).

In addition to the negative consequences of a scenario, it can also be characterized by a probability, L_α, of occurring. In the quantitative definition of risk probability should be interpreted in the Bayesian tradition, where probabilities are subjective

in the sense that they express a "degree of belief" regarding the events of interest. The contrasting paradigm is sometimes called the "frequentist" paradigm and in that paradigm probabilities represent objective quantities that exist in "the world". In the context of this thesis, probability therefore is "a measure of expressing uncertainty about the world….seen through the eyes of the assessor and based on some background information and knowledge" (Aven and Kristensen, 2005). In order for a risk analysis to be as good as possible, it is of course important that the best available knowledge is employed, or in the words of Kaplan (1997): "Let the evidence speak!"

The three concepts that have been discussed above, i.e. risk scenarios, negative consequences and probabilities, are the building blocks of the quantitative definition of risk. According to this definition, a risk analysis involves answering three questions:

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

A single answer to each of these questions is called a *risk triplet*, $<S_\alpha, L_\alpha, X_\alpha>$, and includes a description of a risk scenario (answer to question 1), the probability that it will occur (answer to question 2) and the negative consequences given that the scenario occurs (answer to question 3). However, since there are uncertainties regarding the future behaviour of the systems of interest in a risk analysis, there are many answers to these questions. These answers can thus be expressed as a set of answers, namely as a *set of risk triplets*, $\{<S_\alpha, L_\alpha, X_\alpha>\}$. Risk can then be *defined* as the *complete*, *c*, set of triplets (equation 1). This definition of risk, however, will only be applicable *in theory*; the reason being that in reality there is an *infinite* number of possible risk scenarios, since it is always possible to give a more detailed description of any stated risk scenario. In equation 1 below, α is therefore an index that ranges over a set A that is infinite and non-denumerable.

$$R = \{< S_\alpha, L_\alpha, X_\alpha >\}_c, \alpha \in A \quad (1)$$

A, above, can be thought of as the set of points on a plane, see Figure 5-2, and each point on that plane, α, represents a single risk scenario, S_α. The set of all possible points can be seen as representing the set of all possible risk scenarios, denoted S_A (also referred to as the *risk space*), which thus is comprised of an infinite number of risk scenarios, S_α. In practice, then, all scenario descriptions that are expressed with a finite number of words (i.e. *all* scenario descriptions in practice) are in fact

representing a *set* of underlying risk scenarios (each scenario in this set of course also in turn representing a set of underlying scenarios). In order to distinguish the latter types of scenarios (the ones representing a set of underlying scenarios) from the ideal, infinitely detailed, scenarios labelled as S_α, these are labelled S_i. The difference between S_i and S_α is illustrated geometrically in Figure 5-2.

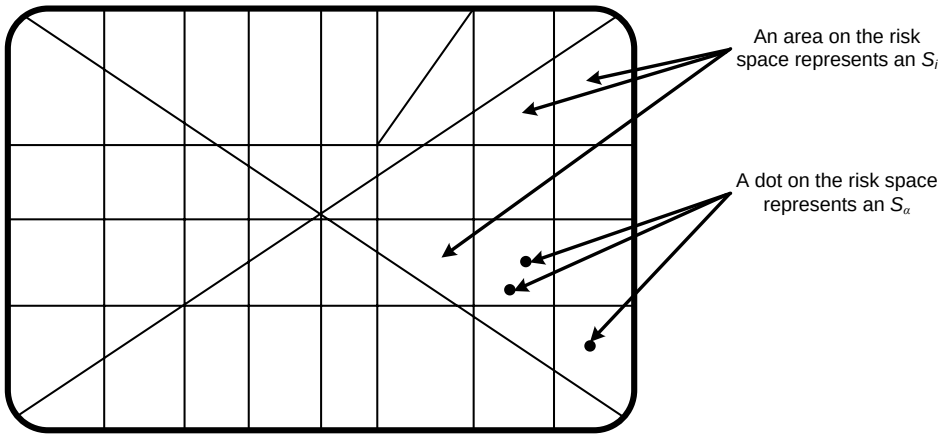


Figure 5-2. A geometrical representation of the risk space, S_A, where the difference between S_i and S_α is presented. S_α can be represented by a point on the risk space, whereas S_i can be represented by an area or a box on the risk space.

In any practical application of risk analysis, the only feasible way to proceed is to find an *approximation* of the underlying risk space, S_A, by identifying a *partitioning*, *P*, of this space. By partitioning S_A, one thus strives toward identifying a finite set of scenarios (of type S_i) that *covers* the whole underlying risk space. Covering all possible risk scenarios does thus not mean that all possible scenarios (S_α) must be described in detail in the risk analysis, only that all scenarios must be *represented* by some scenario description, S_i (and its associated consequence, X_i , and probability, L_i). The "theoretical" definition of risk proposed in equation 1 can thus be modified in order to be applicable in practice. This modification is presented in equation 2.

$$R_P = \{< S_i, L_i, X_i >\}_P, \tag{2}$$

where R_P is an approximation of R (given in equation 1) and is contingent on the particular partitioning *P*. How to make this partitioning 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, Visnepolchi *et al.*, 1999). The method proposed by Haimes, Kaplan *et al.* (2002) is an example of how different scenarios can be ranked and filtered in order to find the most important ones in need for a more detailed analysis.

There are two other requirements of the partitioning of the underlying risk space: that the scenarios should be finite and disjoint. The first requirement is of practical reasons since no practical application of risk analysis can deal with infinite numbers. The second requirement has to do with the fact that no pairs of S_i are allowed to overlap, in the sense that both cover the same underlying scenarios. To exemplify this, assume that the risk associated with pumping chlorine gas between two tanks is being analysed. A potentially hazardous event is that the pipe connecting the two tanks ruptures causing a gas release. Assume that the diameter of the hole can vary from 2 mm to a total rupture (20 mm) and in the risk analysis one wants to cover the whole spectrum of possible sizes of holes. A disjoint partitioning of the underlying risk space would be to, for example, identify 3 scenarios; 2-8 mm (a small leak), 8-16 mm (a large leak) and 16-20 mm (a total rupture) holes. In this case there is no overlap between the identified scenarios; however, if the diameters of the holes would instead be assumed to be 2-10 mm, 5-15 mm, and 15-20 mm, respectively, the partitioning would not be disjoint, since holes of sizes ranging from 5 to 10 mm are covered by two different scenarios. If these scenarios are then aggregated into an overall estimate of the risk, such estimates would be misleading since some scenarios are accounted for several times – leading to an overestimation of the risk. Violation of this requirement, however, is not as serious if there is no attempt to estimate the overall risk, by aggregating the probabilities and consequences of different risk scenarios in a system. Haimes, for example, has developed a method that intentionally generates scenarios that to some degree overlap (Haimes, 1998). His method is called Hierarchical Holographic Modelling (HHM) and aims at finding an as complete picture of the system as possible by viewing the real system of interest from different perspectives.

In connection to the quantitative definition of risk, two other relevant concepts need to be introduced; these are *Initiating events* and *End states* (see Figure 5-3). Since the focus of a risk analysis is the possible risk scenarios that can occur, i.e. the deviations from the success scenario, there has to be a "point of departure" from the success scenario. This point of departure is called an initiating event (IE). After an initiating event has occurred the system continues to evolve over time and once it is possible to determine the consequences of the risk scenario, the system has

reached an end state (ES). Thus, depending on the consequences of interest in a specific analysis, the end state can be reached at different moments in time. For example, if the consequence of interest is the number of fatalities that arise as a direct effect of an accident, the end state are probably reached quite soon in time after the initiating event occurred, whereas it may take "longer" if the consequence of interest is the indirect socio-economic effect of the accident. Since it is the consequences of interest that determines when the end state is reached it is very important that these are clearly defined and possible to determine.

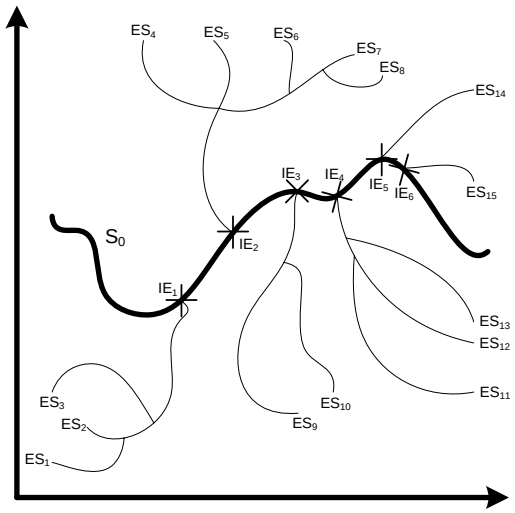


Figure 5-3. State space representation of a system where the concepts of initiating events (IE), and end states (ES) are illustrated.

5.1.3 Risk measures

To sum up the previous section, a risk analysis can be said to aim at generating a set of risk scenarios, and determine their respective probability and consequence. The risk scenarios are generated by partitioning the risk space appropriately with regards to the purpose of the analysis. The most important scenarios to include are the ones that contribute the most to the overall risk in the system, whereas less significant scenarios can be lumped together into more coarse classes of scenarios. The set of risk triplet that is generated in the 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). However, such a list may be difficult to interpret and make use of straightforwardly. Therefore, it is common to derive various risk measures from this set. The most common of these is probably *expected*

risk, which can be derived by multiplying the probability and consequence of each scenario and then summing these products. In the literature, risk is sometimes *defined* as the expected value of the risk (as it is defined here); however, that way of viewing risk can lead to highly misleading results, since frequent but small accidents and infrequent but disastrous events (both contributing equally much to the expected risk) are not possible to distinguish. In only considering the expected value of risk, much important information may therefore be lost.

Other common risk measures are F-N curves, individual risk contours, and individual risk profiles (CCPS, 2000). F-N curves are measures of the societal risk associated with some risky activity and express the cumulative frequency versus the severity of the consequences (often expressed in terms of number of fatalities). The individual risk contours consist of "isorisk" lines in a geographic representation of a hazardous area. The values of these lines are applicable to the risk that exposes a hypothetical person who is constantly present at a certain location during a whole year. The individual risk curves are very similar to the contour, but instead of a geographic presentation of individual risk, the curves present the risk as a function of the distance from the hazardous activity.

In essence, risk measures are developed to facilitate the comprehension of the risk in a system. Another reason is for enabling an easier risk evaluation, which is often done by comparing the risk in a system, expressed using some risk measure, with an acceptance criterion. This, however, is beyond the scope of the present thesis.

5.1.4 Critique against the traditional engineering interpretation

The perspective of risk that has been presented on the previous couple of pages is common in the engineering risk literature. However, moving on into the field of emergency management, risk is sometimes used with another meaning, which should be noted in order to avoid confusion. Dilley and Boudreau (2001) argue that sometimes risk only refers to hazards and external events, not the negative consequences in the system of interest. An example of this view of risk is used by Cutter, Boruff *et al.* (2003) who claims risk to be "an objective measure of the likelihood of a hazard event". In this definition, risk is not related to the subsequent negative consequences due to the occurrence of the hazard. David McEntire, an emergency management scholar, argues that "risk is a result of proximity or exposure to triggering agents, which increase the probability of disaster and the potential for human or material losses" (McEntire, 2001). McEntire's view of risk is closer to the definition of risk that has been presented in the present thesis than compared to Cutter's and her colleagues; however,

according to the view adopted here, proximity to a triggering agent is only a factor that *contributes* to the risk in the system of interest. There are many other factors (attenuators and amplifiers) that determine which negative consequences that will arise from the occurrence of a hazardous event, as was described in chapter 3.

The traditional application of risk analysis, sometimes referred to as technical risk analysis (Renn, 1992), has received considerable criticism over the years. Often it is claimed that risk analyses are too "hazard-centric" not taking the exposed system's capabilities to withstand exposures into account (Dilley and Boudreau, 2001) and focus overly on physical impacts (McEntire, 2005). Others claim that the focus of the risk analyses is too narrow in that they only focus on single dimensions of the negative consequences (Keeney, 1991; Renn, 1998), not matching up with most people's risk perceptions and preferences which have been shown to be much more multi-faceted and comprehensive, e.g. Kasperson, Renn *et al.* (1988), Slovic (1999) and that the only consequences of interest is the immediate impacts of the events (Einarsson and Rausand, 1998). Furthermore, it has been argued that risk is usually defined as the product of consequences and probabilities, implying that low consequence/high probability events are equally risky as high consequence/low probability events, which is often not in accordance with people's risk perception (Kasperson, Renn *et al.*, 1988). In order to extend the applicability of risk analysis several suggestions have been made with the aim of complementing the "standard" risk attributes, such as expected number of fatalities, expected economic losses, with dimensions able to capture psychological aspects of risk, social concern and such, e.g. Florig, Morgan *et al.* (2001), Morgan, DeKay *et al.* (2001), Klinke and Renn (2002), Kristensen, Aven *et al.* (2006). Such dimensions include delay effects, reversibility of consequences, violation of equity etc.

The critique against the traditional engineering approach, however, addresses the traditional *application* of risk analysis, not the underlying definition of risk presented previously. Actually, nothing in the definition of risk, presented here, prohibits an analyst from complying with the critique put forward above. In defining the consequence dimensions of risk one decides what should be seen as constituting a risk. For example, if fatalities occurring with a temporal delay are perceived as more serious than immediate fatalities, it is possible to capture this by defining two consequences dimensions of risk; *immediate fatalities* and *delayed fatalities*. Many of the dimensions that sometimes are said not to be captured in risk analyses is about "consequences of consequences", such as the reversibility of impacts or social upheaval; however, since these dimensions are still different types of *consequences* they are possible to capture in the operational definition of risk. Of course, defining observable variables that represent such dimensions are sometimes

not straightforward and it can also be difficult to gain knowledge regarding the future states of these variables.

5.2 The concept of vulnerability

The concept of vulnerability is defined in a variety of ways in the research literature, and the interpretation of it is highly ambiguous (Cutter, Mitchell *et al.*, 2000; Brooks, 2003; Haimes, 2006), even more so than the concept of risk. The etymological origin of vulnerability is the Latin work *vulnerare* with the meaning "to wound" (Dilley and Boudreau, 2001). The application of the concept 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). 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 the systems. Previously, the disaster was basically equated with the physical hazard that triggered the disastrous course of events; however the critiques argued that disasters do not take place in nature, but in society (Weichselgartner, 2001). So instead of viewing the hazard (e.g. the natural event) as the disaster per se, it is more appropriate to view the disaster as human and socially constructed (Wisner, Blaikie *et al.*, 2004; Haque and Etkin, 2007), that is, produced by the *interactions* between *triggering agents* and an array of *processes* taking place in the exposed systems. In section 3.5, these processes were termed attenuators and amplifiers of consequences depending on which effect a specific process has on the negative consequences. The triggering agents can thus be seen as "external risk factors", whereas vulnerability can be seen as "internal risk factors" (Cardona, 2003).

In the research literature it is possible to distinguish two subtly different but interrelated ways of interpreting the concept of vulnerability; vulnerability as a *characteristic of the system as a whole* and vulnerability as a *feature, state or aspect of a system* rendering it more susceptible to hazards. The first of these views, predominately used in the present thesis, treats vulnerability as an emergent system property that determines the effect a specific hazardous event[11] or perturbation has

[11] Earlier in the chapter a hazard was described as a potential for causing harm, meaning that if the hazard is materialised (e.g. the volcano, which is a hazard, erupts), there exist at least one risk scenario associated with a negative consequence. In discussions of vulnerability it is assumed that the hazard of interest has been materialised in some particular way, causing a *perturbation* on the system. In the present thesis, therefore, the notion of perturbations will be used to denote materialised hazards that expose a system of interest in some particular way. The source of the perturbation can be either internal to the system or external.

on the variables of the system that relate to the negative consequences. As such, "vulnerability is the crucial modifier of consequences" (Salter, 1997). In this view, then, the "relationship between the hazards to which they [the systems] are exposed and their vulnerability to those specific hazards is what creates risks of a specified negative outcome" (Dilley and Boudreau, 2001), a view supported by several scholars in the field, e.g. Salter (1997), Dilley and Boudreau (2001), Brooks (2003), Cardona (2003), Wisner, Blaikie *et al.* (2004), Haimes (2006) and Aven (2007). In order to be able to talk about the vulnerability of a system, the vulnerability has to be related to specific perturbations. A system may be highly vulnerable to certain perturbations whereas less vulnerable to other. Vulnerability, then, does not exist independent of the hazards that may expose the system. In many cases, "generic determinants of vulnerability" (Brooks, Adger *et al.*, 2005) may exist, in the sense that they contribute to a higher or lower vulnerability to an array of different hazards. Such factors, of course, are the most important ones to identify and deal with since they are relevant in regards to many different hazards.

The view that treats vulnerability as features, states or aspects of systems is for example proposed by Einarsson and Rausand (1998; Wisner, Blaikie *et al.*, 2004; Apostolakis and Lemon, 2005; Haimes, 2006; 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 interpreted as a system property). This view is basically analogous to the view that sees risk as a "circumstance that increase the likelihood or consequence (or both) of adverse events" (bullet 2 in the beginning of this chapter). 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). 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. Although I agree that the concept of vulnerability can be interpreted as a feature or state of a system, it will be avoided in the present thesis to avoid confusion. Instead, as will be seen later in this thesis, concepts such as *critical component* or *weaknesses* will be used to refer to features or aspects of a system that leads to an increased vulnerability.

5.2.1 Operational definition of vulnerability

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[12]. In fact, only some slight modifications have to be done in order to operationally define vulnerability. The modifications have to do with the fact that vulnerability has to be related to a specific perturbation or type of perturbation. What is interesting in this case is how the system withstands a perturbation, or recovers from it given that the system has been damaged. Of interest is thus how the state of the system changes over time, i.e. which the possible risk scenarios are, *given* the realisation of a hazard. The fact that there exists at least one risk scenario is obvious since this is what characterizes a hazard, that is, hazards per definition imply a potential for harm otherwise they would not be hazards. 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 that 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. To give a simple example, consider a building located in an area with low seismic activity compared to a building located in a high-seismic area. In the high-seismic area it is likely that buildings are built with the earthquake hazard in mind; so assume it can withstand a magnitude 7 earthquake. The building located in the low seismic area, on the other hand, is likely to ignore the earthquake hazard, so assume it can only withstand a magnitude 5 earthquake. The latter building is clearly more vulnerable (as vulnerability is defined here) to the earthquake threat, since *given* a magnitude 6 earthquake it will collapse, whereas the building in the high-seismic area would withstand the same perturbation. However, the *risk* for the building in the high-seismic area may be larger since the probability that an earthquake of magnitude 7 or more occurs may be larger than the probability that an earthquake of magnitude 5 or more occurs in the low-seismic area.

[12] 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 systemperspektiv" (Methods for risk and vulnerability analysis from a systems perspective) (Johansson and Jönssson 2007). The report is a result of the research conducted in the research programme of which the author of this thesis is a part.

In a vulnerability analysis the interest is to investigate how a system will be affected by different types of perturbations. It is not of interest to study the causes of those perturbations and how they could be prevented. In many cases there may be several different types of hazards and events that may perturb a system in a similar way. For example both ice storms and hurricanes can cause three power lines in an electric distribution system to malfunction. Both these events, although stemming from different types of underlying phenomena, can in this case be said to constitute an equivalent perturbation to the system, since they affect the system in a similar way.

The perturbation per se 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 systems 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, since the dynamics have to be captured. The perturbation, however, will only *constrain* or *determine* the state of some specific state variables in the system of interest. For example, the perturbation "a hurricane" will only constrain the state of the variable "wind speed" in the system of interest (such as in a municipality)[13]. 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 depend on the system's degree of vulnerability in regards to the specific perturbation. Thus, the perturbation is not defined as a completely determined trajectory through the state space of the system; instead it is defined as a partially determined trajectory through state space, i.e. *a partially determined risk scenario*, which constitutes a deviation from the success scenario S_0.

The partially determined risk scenario that represents a perturbation, S_p, consists of a succession of *partially determined states of the system*:

$$S_p = \left(U_{p,1}, U_{p,2} \ldots U_{p,n}\right), \tag{3}$$

[13] 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.

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 $u_{p,1}$, $u_{p,2} \ldots u_{p,k}$.[14] A partially determined state of the system, U_p, that correspond to the perturbation can then be defined as:

$$U_p = \left(u_{p,1}, u_{p,2} \ldots u_{p,k}, \#_1, \#_2 \ldots \#_j\right) \tag{4}$$

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 of course 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 5-4. Furthermore, S_p can be thought of as a part of all possible risk scenarios, i.e. as a part of the risk space (S_A), namely as that part which is constrained by the perturbation. However, since S_A is non-denumerable and infinite, any fraction of S_A (including S_p) is also non-denumerable. To conduct vulnerability analysis *in practice* one therefore has to partition the *constrained risk space* into a finite and manageable number of scenarios that cover the constrained risk space.

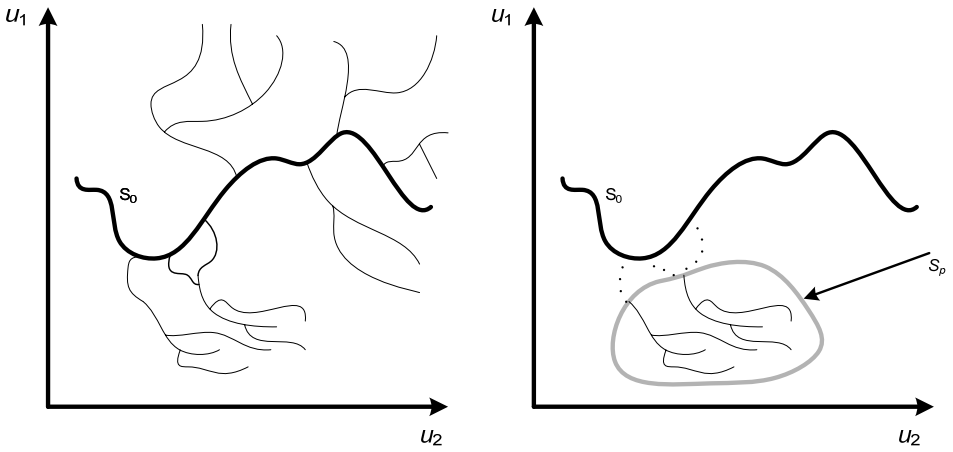


Figure 5-4. The difference between risk (to the left) and vulnerability (to the right) by use of state space representation.

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

The conceptual differences between vulnerability and risk can now be applied to Equation 2 in order 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 done 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 5 below.

$$V_P = \{< S_i, L_i, X_i >\}_P : S_i \in S_p \tag{5}$$

In essence, the vulnerability of a system to a certain perturbation can be expressed as a set of triplets – analogous to risk. To generate the set of triplets, the analyst must make an appropriate partitioning of the constrained risk space (constrained by the specific perturbation) into a manageable set of scenarios and determine their respective probability and consequence. Additionally, similar to risk it is possible to derive vulnerability measures from the set of triplets, such as the expected value or the probabilities that the consequences will exceed certain levels (cumulative probability curves). Such measures can facilitate the understanding of the vulnerability of a system considerably and also make comparisons of various kinds easier.

5.2.2 Bridging the concepts of risk and vulnerability by use of bow-tie representation

Common ways to represent accident and risk scenarios are by use of bow-ties, which are cause-consequence models basically integrating fault-trees and events trees (Hale, 2006). This is done by connecting the top-event of a fault tree with the initiating event of an event tree, see Figure 5-5. Located in the centre of the bow-tie is the undesirable, accidental or critical event that may lead to a negative outcome, and both on the left side (causes) and right side (consequences) of the central event a variety of safety barriers operate to break the chain of events that otherwise may lead to negative consequences. That is, a "barrier is something that either can prevent an event from taking place or protect against its consequences" (Hollnagel, 2004). These barriers can be of various types, such as passive hardware barriers, active hardware barriers and human intervention barriers (Bellamy, Ale *et al.*, 2007) and so on.

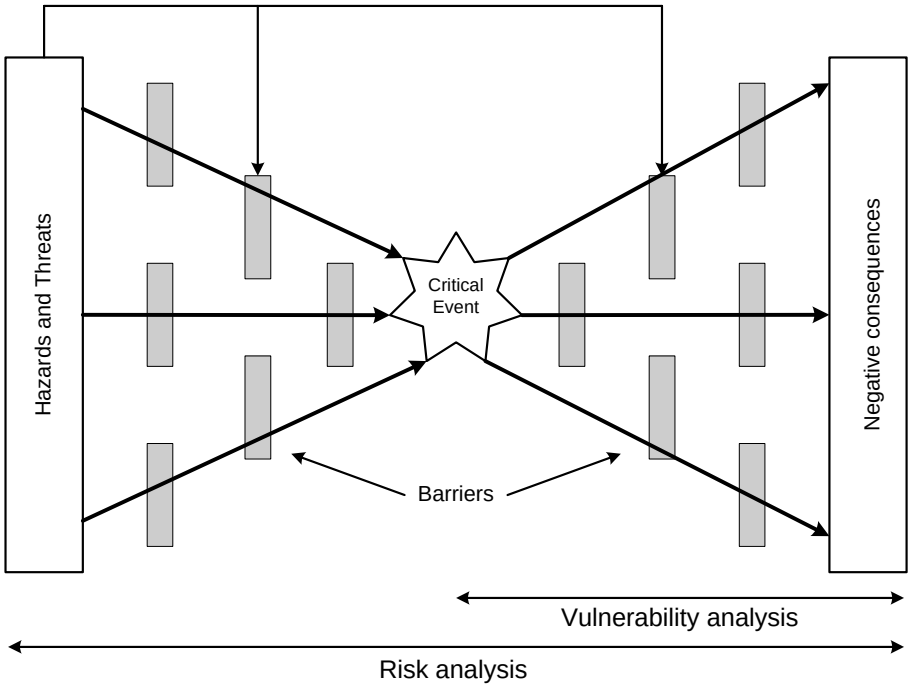


Figure 5-5. Bow-tie representation of an accident or risk scenario, and clarification of the relation between a risk and vulnerability analysis, adapted from (Hale, 2006).

The bow-tie representation can also be used to clarify the definition of vulnerability, suggested above, and its relation to risk, as is seen in Figure 5-5. To do this the central "event" of the bow-tie is seen as the "starting point" of the perturbation, i.e. the first state in S_p, to which the vulnerability of the system is studied. What is of interest to study, then, is only the right side of the bow-tie, i.e. which possible negative consequences that the perturbation may lead to and the barriers that operate to avoid negative consequences to arise. Note that the perturbation also can affect the function of the barriers, which is illustrated in the figure. The left side of the bow-tie is simply not part of the vulnerability analysis, since it is assumed that the barriers that may exist on that side have been unsuccessful in breaking the chain of events leading up to the critical event. In a risk analysis, on the other hand, the interest is in both the cause *and* the consequence sides.

Note that this view of the relation between risk and vulnerability is not shared by all scholars. Einarsson and Rausand (1998), for example, argue that both risk and vulnerability analyses have interest in both the right and the left side of the central

event. Risk, however, extends more to the left, whereas vulnerability extends more to the right. The definitions of risk and vulnerability that have been suggested in the present thesis thus do not support Einarsson's and Rausand's view; however, pragmatic reasons may to some extent explain this discrepancy: in a vulnerability analysis the scope is considerably smaller than in a risk analysis since in a vulnerability analysis there is an interest in only a limited part of the risk space for the system in question, namely that part which is constrained by the perturbation of interest. Of practical reasons, therefore, a vulnerability analysis has the potential to gain deeper insight into the constrained part of the risk space than compared to a risk analysis that tries to cover the whole risk space – given the same time spent. So in practice it is likely that a vulnerability analysis is more detailed in regards to the consequences of the perturbation than a risk analysis, but in principle there is no difference between the definitions of risk and vulnerability that would make a vulnerability analysis be more concerned with consequences.

Another issue in relation to the bow-tie representation is that the event in the centre of the bow-tie, i.e. in this case the perturbation, is not an obvious choice. In fact, no choice of the central event can be said to be the "true" choice. It can only be said that the choice is more or less appropriate in regards to the purpose of an analysis (Bellamy, Ale *et al.*, 2007). However, in defining this event it is determined which barriers that are to be considered in the vulnerability analysis. To give an example, consider the threat posed by avian influenza to the Swedish society. If the perturbation is assumed to be "large-scale outbreak of avian influenza in an Asian country", barriers to consider in the analysis are for example the Asian country's ability to contain the virus inside its borders, the ability of the Swedish border control to prevent infected persons to enter the country, the ability of the Swedish health services to contain the virus given that people in Sweden have been infected and so on. On the other hand, if the perturbation is assumed to be an "outbreak of avian influenza in a Swedish city (stemming from a preceding outbreak in Asia)", the barrier consisting of the ability of the Asian country to contain the virus is not really relevant since it is assumed that the virus is already inside the Swedish borders. The point of the example is that appropriateness of choosing a certain event has to do with the purpose of the analysis. To continue the example, assume that it is an organisation within the Swedish health services with the responsibility of responding to an outbreak of avian influenza in Sweden that are conducting a vulnerability analysis regarding the threat posed by the avian influenza. Assuming the central event to be a "large-scale outbreak of avian influenza in an Asian country" would not be appropriate since even though problems associated with the ability of the Asian country to contain the virus had been identified it would be outside the sphere of influence of the Swedish health services. A more appropriate choice of central event would convey that only those

barriers that are within the sphere of influence of the Swedish health services are included in the analysis.

5.3 The meaning of risk and vulnerability analyses

In the present thesis the phrase "risk and vulnerability analysis" has been used and will be used in what follows. But what does the phrase really mean? Unfortunately this is not entirely clear. The obvious problem is that in the phrase, two somewhat ambiguous concepts are combined leading to an even more ambiguous combination of concepts.

The phrase is frequently used in Sweden in connection to emergency management and sometimes also in the research literature. The Swedish Emergency Management Agency (SEMA) seems to use the phrase in order to put an increased emphasis on the consequence dimension of risk, and especially the long-term consequences (SEMA, 2006b). A risk and vulnerability analysis, according to SEMA, starts with a rather coarse risk analysis (similar to a preliminary hazards analysis) including semi-quantitative estimations of probabilities and consequences of different scenarios, followed by a more detailed analysis of a small number of scenarios. The more detailed analyses are concerned with different actors' capabilities to respond to the scenarios. Of course, since the response capabilities of the actors in for example a municipality affect the risk in the municipality (since the actors affect the probability and consequence of the risk scenarios) the preliminary hazards analysis involves methodological issues - how are the capabilities to be taken into account when estimating the probabilities and consequences of different scenarios in the preliminary hazards analysis? Is it possible to disregard response capabilities when estimating the risk in the PHA? While these methodological considerations make the approach less appealing, the underlying assumption of the approach is acknowledged in the present thesis, namely that in studying a small number of scenarios in detail, it is believed that generic insight often can be gained regarding the response capabilities for the involved actors.

As the concepts have been operationally defined in the previous sections, it is clear that vulnerability as it is being used here is part of risk. So a risk and vulnerability analysis should in fact be the same as a risk analysis in the same way as fixing the car and fixing the engine of the car is the same as fixing the car. What differs the two phrases though is that the emphasis on vulnerability is increased. This view is suggested by Aven (2007) 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, then, uses the concept vulnerability to refer to a feature or aspect of a system

rendering it more susceptible to hazards. 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).

In expanding an analysis from potential for harm to probability for 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 always should strive to expand a vulnerability analysis into a risk analysis. However, on some occasions it can be very difficult to determine the probability of a perturbation accurately due to lack of knowledge and data regarding the phenomena – for example the threat of terrorism. In addition, available statistics may indicate that the probability of a perturbation is low, for example when using generic probabilities and assume failure independence, but where there are possibilities of common cause failures not taken into account in the probability estimations. In merging very uncertain probability estimations with vulnerability estimations that are associated with quite small uncertainties one renders a risk of making the analysis less useful.

Hansson argues that "[s]afety does not mean measures only against those hazards that are known and quantified, but also as far as possible, against those that are unknown and unexpected" (Hansson, 2005). A similar claim is suggested by Hollnagel and Woods who argue that safety is not achieved by only keeping failure probabilities below certain values; the system also need to have "the ability to recover from irregular variations and disruptions and degradation of expected working conditions" (Hollnagel and Woods, 2006). Vulnerability analyses can therefore be used to gain knowledge of a how well a system can withstand and recover from certain perturbations, without having to consider the probability of the perturbation explicitly. Very high vulnerabilities can merit measures to be taken although existing knowledge regarding the probability of the perturbation points to it being very low, but this of course depends on the uncertainties associated with the probability estimations. If in fact there are large amount of representative data supporting the claim that the probability is low, then high vulnerabilities probably do not merit measures to be taken. However, if there is a lack of data, which is often the case in the context of emergency management, then high vulnerabilities may merit reductions.

6 Presentation of research, evaluation and future work

The model of societal emergencies, presented in chapter 3.5, showed that in order to provide a complete picture of risks and vulnerabilities, many factors, systems etc. and their interactions need to be considered. The present thesis does not aim to address all these factors in detail, but rather to start addressing some of the relevant issues. A long-term goal for the research community as a whole, however, should be to try to find ways to take all relevant factors and systems, and their interactions, into consideration when analysing risks and vulnerabilities.

This chapter aims to *present the research* conducted by the author which is related to some of the factors that are relevant in a societal emergency management context. The presentation closely relates to, and somewhat overlaps with, the papers attached in the end of the thesis. However, mainly this chapter is intended to provide background and additional information of special interest, such as how the operational definitions suggested in the previous section relates to the papers. In order to gain a deeper insight into the conducted research, the reader is directed to the attached papers. After the presentation, brief *evaluations* and *reflections* will be made in connection to the presented research. This is because evaluations are important in the process of developing methods and knowledge intended for practical application, as was argued in chapter 1.4. Finally, suggestions of *future work* will also be given.

The chapter will be oriented around three themes, which relates to the research aims and objectives presented in chapter 2. All three themes are related to the operational definition of risk and vulnerability presented in the previous chapter, which will be evident in what follows. The three themes are:

- Methods for vulnerability analysis of critical infrastructure networks (Paper 1 and 2),
- Emergency response capabilities (Paper 3),
- Value input to risk analysis and decision-making (Paper 4).

6.1 Presentation of three research themes

6.1.1 Methods for vulnerability analysis of critical infrastructure networks

The vulnerability and robustness of critical infrastructures are very important factors from a societal emergency management perspective, as was described in chapter 3.5. Critical infrastructures are large-scale systems, often described as complex and it can be difficult to analyse these systems adequately. One possible way to create a structure for how to approach this problem, which is done here, is to use an operational definition as a point of departure. In the previous chapter, vulnerability was defined as the answer to the three questions: What can happen, given a specific perturbation? How likely is it, given that perturbation? If it does happen, what are the consequences? The result of these questions is a list of risk scenarios, and their corresponding probabilities and consequences, which are contingent on the occurrence of the specific perturbation. An important question is how it is possible to identify all relevant risk scenarios, and where this set of scenarios meet the criteria of being complete and disjoint (at least approximately). When concerned with a large-scale critical infrastructure it is likely that a certain perturbation can lead to a large number of possible risk scenarios, since it is often not known exactly how the perturbation will expose the system or how the system will withstand the perturbation – i.e. uncertainties exist. What is needed, therefore, is a *methodological approach* that can create a structure for partitioning the underlying risk space (conditioned on the occurrence of a specific perturbation) and thus capture the relevant risk scenarios.

The methodological approach called *network analysis* (see chapter 4.3) was found to provide such a structure for analysing the vulnerability of critical infrastructure networks. Using network analysis as a point of departure is reasonable since a feature that unifies many critical infrastructures is their *network structures*. Examples include the electric power system, water distribution systems, transportation systems, telecommunication systems and so on. In addition, literature studies showed that network analysis previously had been used to study the robustness and vulnerability of complex networks, e.g. Albert, Jeong *et al.* (2000), Holme and Kim (2002), Holme, Kim *et al.* (2002), Motter and Lai (2002), Crucitti, Latora *et al.* (2004a, b). These studies are mainly concerned with the vulnerability of *theoretical models* of networks, such as scale-free, random or small-world networks (see Albert and Barabási (2002) for an overview of theoretical network models). However, it is often difficult to relate real existing networks to these theoretical models and therefore another group of network analytic studies is concerned with analysing the vulnerability of the network

representations of *real systems*, e.g. Albert, Albert *et al.* (2004), Crucitti, Latora *et al.* 2004c, 2005), Kinney, Crucitti *et al.* (2005), Holmgren (2006).

Before describing the details of the network analytic approach to vulnerability analysis and its relation to the operational definition of vulnerability, a distinction between the structural model (*network model*) and the functional model (*physical model*) of a critical infrastructure system will be made, see Figure 6-1, as is done in Johansson (2007). Taken together these two models constitute the model of the real system of interest. The structural model is a model of the system's components and how they are connected to each other, i.e. the structural model is a set of nodes and edges. The functional model, on the other hand, describes the extent to which the system is able to provide its intended services (i.e. its performance), *given* the structure of the system and other input regarding the behaviour of the system.

In network analysis the structural model is exposed to a perturbation. The perturbation is modelled as a *removal* of nodes/edges which thus leads to a modification of the structural model. The performance drop due to the perturbation, i.e. the negative consequence, is then estimated by use of the functional model. In addition, there may also be a feed-back loop from the functional to the structural model if the functional model can account for cascading failures, such as edge overload, see Figure 6-1.

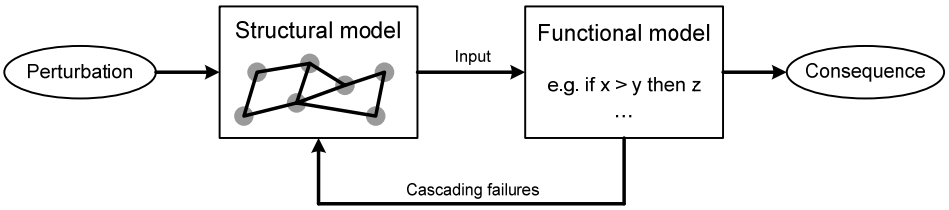


Figure 6-1. Differentiation between the structural and functional model of a system, adapted from Johansson (2007).

In separating the two types of models it can be seen that the network analytic approach basically is consistent with any type of functional model, i.e. the approach is essentially *model agnostic*. For example, in Paper 1 (Johansson, Jönsson *et al.*, 2007), which was concerned with electric distribution systems, the functional model used was quite rudimentary: a distribution substation was assumed to be supplied with power as long as at least one unbroken path connected it to an in-feed node. In Paper 2 (Jönsson, Johansson *et al.*, 2007), on the other hand, a somewhat more refined functional model was employed, where the loads of the distribution substations and the capacities of the in-feed nodes were taken into account. Further refinements of the functional model are possible by taking

account of capacity constraints in nodes and edges, thus capturing cascading failures. Still, such a functional model is a quite coarse representation of the electrical flow in power lines and cables; of course even more refined models exist (e.g. power flow). When adopting a more detailed modelling approach, however, practical issues associated with computation time and requirements of input data arise. The models are likely to become more accurate, which of course is an advantage, but performing the vast number of calculations that are required may not be feasible. In any case, by separating the structural and functional models the approach becomes more flexible in regards to which functional model is being used. The generalisation of the approach to other types of technical infrastructures is then also facilitated, since only the functional model used need to be adapted to better represent the function of the specific system of interest.

It is possible to distinguish between two different foci of methods for vulnerability analysis. The first focus is on the *global vulnerability*[15] of critical infrastructure networks to perturbations of various kinds. The other focus is on *critical components* of an infrastructure network, i.e. components that can cause large negative consequences if they are unavailable. Such information of local properties of a system can complement analyses of global vulnerability by pointing out possible reasons for systems to be vulnerable. The methods that have been developed and which are presented here cover both these foci and will in turn be described and discussed below.

Global vulnerability analysis

Paper 1 is concerned with global vulnerability analysis based on a network analytic approach. In network analysis, as mentioned earlier, the general approach for conducting global vulnerability analysis is to expose the network (structural) model of a system to different types of *attack strategies* and then study how the system performance deteriorates. Attack strategies are specific ways of removing nodes and/or edges from the network and are used to represent different *types* of perturbations. Two common attack strategies, which are used in Paper 1, are random removal (all nodes and/or edges has an equal probability of being removed) and removal in some directed manner, e.g. removing the node with highest degree (the node that have most edges).

The network analytic approach can be related to the operational definition of vulnerability. As defined in chapter 5.2.1, vulnerability *is* a list of risk scenarios and

[15] The term global is here being used to emphasize that vulnerability in this case should be interpreted as a system property, i.e. a global property, in accordance with the operational definition presented in section 5.2.1.

their corresponding probabilities and negative consequences, *given a specific perturbation*. A *specific* perturbation in this case can be described by an attack strategy *and* the fraction (or number) of removed components. An example of such a perturbation is "1% randomly removed nodes". Since these nodes are removed in a purely random fashion, any combination of 1% removed nodes can constitute a perturbation to the system. Each possible combination of removed nodes thus constitutes an answer to the question: "what can happen, given a specific perturbation?", i.e. each combination constitutes a risk scenario. Furthermore, since the removal here was random, each combination has an equal probability of occurring, which answers the question: "how likely is it, given that perturbation?". Finally, by estimating the negative consequences (by use of a functional model as described in the previous section and Figure 6-1), *given* the occurrence of a specific risk scenario, the last question in the operational definition of vulnerability: "if it does happen, what are the consequences?" is also answered. In the present context, however, network analysis is applied to study large-scale infrastructure systems. The effect of this is that the number of possible risk scenarios, i.e. the number of possible combinations of removed components, *given* a specific perturbation is often enormous, especially if several components are removed simultaneously. This fact makes it practically impossible to estimate the consequences of *all* possible combinations. Instead, a computer-based Monte-Carlo simulation can be employed, where a sample[16] of all possible risk scenarios is drawn and the consequences of each estimated[17]. The Monte-Carlo simulation therefore can be said to partition the underlying risk space by finding a sample of representative risk scenarios. The result, when following these procedures, is a list of risk scenarios (the number being equal to the size of the sample), and their corresponding probabilities and negative consequences, which *is* the vulnerability of the system to the specific perturbation in question.

This list of scenarios may be very difficult to make sense of in the same sense as it may be difficult to make sense of a large set of scenarios in a risk analysis. Therefore, *vulnerability measures* need to be established in order to facilitate the comprehension. The most common measure is to calculate the expected consequences due to the perturbation in question. This is done in basically all application of network analysis and also Paper 1. Something that seemingly is ignored, however, is the fact that a *distribution* of possible consequences underlies the expected consequence, i.e. there exist uncertainties regarding the impact of a perturbation. Knowledge about this may actually be very important when for

[16] The sample has to be sufficiently large to provide statistically stable results.
[17] A computer software used for simulation, a program called NetCalc, was developed by the research group using the Microsoft .NET framework.

example making decisions concerning vulnerability. Therefore, curves that are analogue to the standard FN-curves, frequently used in risk analyses, with the exception that the curves are contingent on the occurrence of a specific perturbation, can be presented.

In the previous paragraphs the vulnerability of a system was considered in relation to a *specific fraction* of removed components (using a specific type of attack strategy), however, network analytic studies normally consider the expected negative consequences as *a function* of an *increased fraction* of removed components. Thus, when presenting the expected consequences, *vulnerability curves* are generated, such as those presented in Paper 1, rather than a point estimate. In the standard vulnerability curves, however, no information about the distribution of the negative consequences that underlie the expected consequences is provided. Here, two ways of presenting such information will be mentioned. The first way is to present *percentile plots*. In a percentile plot arbitrary percentiles can be chosen to illustrate the distribution of possible consequences (the uncertainties regarding the consequences). The 2.5% and 97.5% percentiles can for example be chosen to illustrate an interval that covers the consequences of 95% of the underlying risk scenarios. The second way is to present *fragility curves*. These curves illustrate the probability that the negative consequences exceed some specified levels (such as 5%, 50%, and 100% performance drop) as a function of an increased fraction of removed components. Fragility curves were originally developed in the area of seismic hazards; however, they can serve as a good way of presenting information about vulnerability in other areas as well, as is illustrated by Simpson, Rockaway *et al.* (2005).

The previous paragraphs show that the relation between the network analytic approach and the operational definition of vulnerability is quite straightforward. Taken together, network analysis and the operational definition clearly has the potential of providing the structure that is needed for analysing large-scale infrastructure systems. In Paper 1 these principles were applied to analyse electric power distribution systems. Previous network analytic efforts had a number of limitations if they were to be applied in this area. First, the performance measures commonly used are often very general, i.e. they are not adapted to the specific system of interest. As such, the appropriateness of using these when analysing the vulnerability of a specific type of system, such as the electric power distribution system, could be questioned. Several of the suggested approaches do not distinguish between different types of nodes. However, in most technological infrastructures components are highly heterogeneous: some feed a commodity into the network, whereas others directly supply customers and so on. Furthermore, none of the suggested approaches are essentially interested in modelling the

consequences to the societal system to which the infrastructures provide their services; instead, the focus is mainly on the technological system per se. Finally, none of the suggested approaches aim to model the distribution level of the power system. Performance measures developed to suit other levels therefore needed to be evaluated in regards to how well they suit the distribution level, and adapted if necessary.

The considerations described above led to a network analytic method for vulnerability analysis being proposed in Paper 1 which distinguishes between three types of nodes: in-feed nodes, transmission nodes and distribution substations. As long as a distribution substation had an unbroken path to an in-feed node, it is assumed that the customers connected to the substation have power supply. In order to capture the societal consequences of disruptions a concept called Customer Equivalents (CE) was introduced. Each distribution substation is given a CE-value which is meant to reflect the severity of societal consequences if that substation were to loose its power supply. The assignment of CE-values should reflect the underlying value system in the particular analysis, which means that the choice of CE depends somewhat on who is conducting the analysis. In Paper 1, a simple assumption was made that the CE of each substation was proportional to the number of customers connected to that station; however, more detailed approaches are possible as well, e.g. see Koonce, Apostolakis *et al.* (2006), Michaud and Apostolakis (2006). The negative consequence due to a perturbation is estimated as the number of CE that have lost their power supply. In addition, two vulnerability measures were introduced which can facilitate comparisons between systems. The conclusion of Paper 1 is that the suggested methods and measures can increase the value of using a network analytic approach to analyse the vulnerability of critical infrastructure networks.

Identifying critical components

The previous section referred to the system's overall vulnerability; however, another focus of methods for vulnerability analysis is on *local properties* (properties of components or groups of components). One such focus is on identifying and ranking critical components in a system. Therefore, the focus of Paper 2 (Jönsson, Johansson *et al.*, 2007) is to suggest a method for identifying critical components or sets of components. A critical component, in this case, is referred to as a component that can cause large negative consequences if it fails or by other reasons is unavailable (e.g. are subjected to maintenance). As such, criticality can also be related to the operational definition of vulnerability in the sense that criticality is defined as the *vulnerability of the infrastructure system to failure in the component/set of components*. Thus, the failure of a component or a set of components is assumed to constitute a specific perturbation to the system. By identifying all relevant risk

scenarios and their corresponding probabilities and negative consequences the vulnerability of the system can be estimated in accordance with the operational definition. In many cases contextual factors can affect which consequences that arise due to failures. In an electric power system (which is the type of system that the suggested method is applied to in Paper 2) the consequences of failures can for example depend on the time of year, time of day, and the power demands at the time of the failures. Such conditions will therefore lead to the fact that many risk scenarios can occur given specific failures. In Paper 2, however, the power system modelling was assumed to be *deterministic* in the sense that specific failures only were related to a single risk scenario and therefore a single negative consequence. Such an approach is somewhat of a simplification since it requires assumptions to be made regarding the contextual factors in order to estimate *characteristic consequences* of failures; however, it reduces the computational time considerably making the analysis practically feasible.

In the area of risk and reliability, *importance measures* are often used to rank a system's components or sub-systems according to their contribution or impact on risk or reliability (for an overview see Cheok, Parry *et al.* (1998)). These often represent a *combination* of the probabilities and the consequences of failures. The criticality measure, proposed in Paper 2, should be seen as a complement to the traditional importance measures, in that it only considers the consequences *given* component failure or unavailability. A reason for not incorporating the probability of those failures in the measure is that the probabilities often can be difficult to estimate appropriately. In many cases generic probabilities or frequencies have to be used, which not always are representative to the system of interest. In addition, some threats and hazards make quantification of probabilities very difficult, such as the threats of terrorism or sabotage. Furthermore, when considering simultaneous failures assumptions regarding failure independence also often have to be made; however, when systems are exposed to external perturbations, such as adverse weather, independence of events and generic probabilities are no longer valid. This is because components are exposed to higher levels of stresses for a short period of time causing "failure bunching" (Billington, Singh *et al.*, 2006), i.e. a sharp increase in the failure rates of the exposed components. The probability of simultaneous failure, then, may increase drastically for some combinations of failures, which is not captured when using generic probabilities.

Not including probabilities of failures in the criticality measure is <u>not</u> to say that probabilities are irrelevant – they are highly relevant – it is rather to say that the uncertainties associated with estimating the probability of failures in many cases are much larger than the uncertainties associated with their consequences. It would be unfortunate not to be made aware of a component that with certainty give rise to

very large consequences if failing but where this is "expected" to be unlikely, e.g. based on statistics. In conducting the rankings based on consequences, components that need to be especially robust and are especially important to keep protected are identified. Measures can then be taken, if needed, such as measures that aim at guaranteeing component reliability, installing additional barriers or monitor existing ones. Alternatively, the components could be made less critical by modifying the system's structure, for example by adding redundancy. Thus, it is not argued that probability of failure should be disregarded, only that it can make sense to *first* find the critical components and *then* consider the probability of failures. Furthermore, in following Hansson's device, cited in chapter 5.3, it may sometimes make sense to allocate resources to reduce the consequences of failures although these, based on the knowledge and data existing at the time of the analysis, would be highly unexpected to occur in the near future.

In Paper 2 the interest is not only with single failures, but also with combinations of component failures. A problem, then, is the combinatorial explosion that occurs, i.e. the number of possible combinations of component failures is very large for large systems. In a system composed of 1000 components, for example, there exist almost 500 000 combinations of pairs of failures. Therefore, there is a need for developing screening strategies in order to find the combinations of failures that can be particularly interesting. In the paper, it is suggested that such a screening strategy can be based on finding the combinations of failures that lead to large *synergistic* consequences, i.e. failures that if they occur individually do not give rise to large consequences, but if they occur simultaneously cause great negative impact on the underlying value system. These failures interact with each other and cause large consequences that can be difficult to become aware of without employing a systematic procedure. In Paper 2, therefore, all possible single, pairs and triads of components are analysed in regards to which consequences, in total and the synergistic fraction, they give rise to if they fail. It is argued that this approach facilitates the identification of critical components and sets of components. As such, it can complement analyses of global vulnerability by pointing out where system weaknesses may exist.

6.1.2 Emergency response capabilities

The second research theme that the present thesis is concerned with is *emergency response capabilities*. In the methods described in the previous section the focus was mainly on technical systems, although it is emphasized in these methods that the negative consequences of a perturbation not should be estimated only with reference to the technical system per se, but to the harm to the underlying value system. However, emergency response actors' capabilities are not taken into account explicitly in these methods. But when considering a technical

infrastructure system there are many different actors that can affect how a risk scenario will evolve. The most obvious actors in this case are probably the repair teams; however, many other actors may also affect how the emergency evolves. Many of these actors may not even play a role in the normal operations of the system that is the "source" of the emergency. In regards to technical infrastructures such actors include the Fire and Rescue Services, civil defence groups and NGOs, whose influence for example was evident during and after the storm Gudrun that struck Sweden in 2005.

The same arguments are applicable when expanding the scope of the discussion to not only consider emergencies directly related to technical infrastructures. Of course, some types of consequences, e.g. instant fatalities (such as in an airplane disaster), cannot be affected by emergency response actors; however, whether they are able to meet the assistance needs that arise during and after an emergency can significantly affect the negative consequences. Therefore, in order to obtain a more complete picture of risks and vulnerabilities, emergency response capabilities in most cases also need to be addressed in risk and vulnerability analyses.

Often risk analyses are conducted in order to provide input to decisions regarding which *preventive measures* that should be implemented. It is more uncommon to use a risk analysis to suggest which *preparatory measures* to implement in order to reduce risks and enhance capabilities. In addressing emergency response capabilities in risk and vulnerability analyses, the possibility of being able to compare preventive and preparatory measures are increased. To be able to do that is important, since sometimes preparatory measures are more effective than preventive measures, whereas on other occasions the relation is the opposite.

The long term goal of the research conducted in this area is therefore to integrate the emergency response capabilities of different actors in risk and vulnerability analyses. The present thesis takes one step towards this, which is done by suggesting an operational definition of emergency response capabilities (Paper 3). This definition builds on the operational definition of risk, presented in chapter 5.1.2. The intention of the operational definition is to provide a platform for *analysing* capabilities, in a similar way as the quantitative definition of risk provides a platform for analysing risk and the operational definition of vulnerability provides a platform for analysing vulnerability.

Here, an *analysis* is distinguished from an *evaluation*. In conducting an analysis one is striving toward gaining knowledge about future possible scenarios in the system of interest by using available evidence. Conducting an evaluation, on the other hand, is an inherently subjective task since it concerns value judgements regarding

whether something is "good enough" or "needs to be better" and so on. One of the points of Paper 3 is that it is important that the analysis of emergency response capabilities must be separated from the evaluation, which is not always done in other approaches.

The essential point of departure in the definition is that emergency response capability is about what an actor is able to *do*. Therefore, it is argued that the capability of an actor should be related to specific *tasks*, *functions* or *activities*. In addition, concrete measures regarding what characterise a task being well performed must be defined. Finally, the context in a specific situation will affect how well a task can be performed and this must be addressed when analysing capabilities. However, although the task, performance measures and the context have been specified it can be difficult to determine how well the task can be performed, i.e. uncertainties exist. This uncertainty can be expressed using a set of triplets – similar to the operational definitions of risk and vulnerability:

1. What can happen when an actor is performing a specific task, given a specific context?
2. How likely is it?
3. What are the consequences, for the performance measures defined for that particular task?

One of the main points of the operational definition is to increase the concreteness related to analyses of capabilities. It is not sufficient to claim that "our ability to evacuate is sufficient". Instead, one must first state what good ability to evacuate actually means – how is it possible to measure such a thing? Then, one must think about which factors that may influence how well an evacuation can be performed. – i.e. which are the dependencies? As such, how well an emergency response actor can perform a task often does not only depend on its "own" capabilities, but also on the performance of other actors' and systems'. Therefore, when an actor is analysing its capabilities, any estimations of how well a task can be performed must be contingent on a specific context. An analysis can therefore lead to insight regarding which factors in the context are critical for the actor's performance, such as critical resources, other actors that are critical and critical technological systems.

It is concluded that the suggested operational definition can provide an analytic framework for analysing capabilities and also be used as a point of departure when suggesting concrete methods. In addition, expressing capabilities in a similar way as risk and vulnerability is a means towards bridging the concepts together, which subsequently can facilitate analyses that integrate all these factors.

6.1.3 Value input to risk analysis and decision-making

In the previous two sections the issues of analysing complex systems from a risk and vulnerability perspective have been discussed. It has been assumed that the variables of interest to study in these analyses, i.e. the variables related to the negative consequences, are known. However, as argued in chapter 5.1, *values* and *preferences* are what defines risks (see chapter 5.1), or as Campbell argues: "preferences determine what counts as a harm" (Campbell, 2006). It is often acknowledged that knowledge about values is necessary in order to *evaluate risks*, i.e. to decide whether a risk can be accepted or not or how much money should be spent on risk reductions etc. However, while this definitely is the case, knowledge about values and preferences is also a prerequisite for being able to initiate a risk and/or vulnerability analysis at all. Thus, without knowledge about values and preferences it is impossible to know what constitutes a risk and which variables are of interest to study in an analysis. Often, however, values are treated rather implicit in risk analyses. The argument in the present thesis is that there is a need for increasing our knowledge about values, and to become more explicit regarding which values are being used as a basis for risk and vulnerability analyses.

In Paper 4 (Jönsson, Johansson *et al.*) the value part of risk analysis and management is therefore addressed. In the paper an empirical study was conducted in order to elicit people's values and preferences regarding different potential scenarios involving large consequences. The basic premise of this research follows what Cox (2007) argues to be in line with traditional decision analysis, namely that beliefs about future consequences of different possible actions ("facts") should be separated from the values assigned to different possible consequences.

Four attributes were used in Paper 4 to characterise the disaster scenarios: *number of fatalities*, *number of serious injuries*, *economic loss* and *the cause of the disaster*. Two different methods of fundamentally different type were used to elicit the weights for the attributes, the reason being that no method for elicitation is free of bias and using several methods for elicitation is a means to study the convergent validity of the elicited values; thus, increasing the insight that is possible to gain regarding the values. Furthermore, since no method for eliciting values is free of bias, using several methods is a way to investigate the uncertainties of the "value estimations". Knowledge about uncertainties related to the values and preferences that are used as a basis for risk and vulnerability analyses can be very important. These can for example be propagated to the analysis in order to investigate the effect of the uncertainties on the analysis result.

It is important to note that it is impossible to speak about attribute importance without relating the weights to the ranges of the attributes. In Paper 4 the following attribute ranges were used:

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

With these ranges in mind, the number of fatalities was in general seen as being the most important attribute for determining the seriousness of a disaster, followed by number of serious injuries. Economic loss and the cause of the disaster were seen as being least important but did in many cases have a significant effect on people's perceived seriousness. The values elicited from the two methods differed somewhat but the ordinal relation between the attribute importance was in general the same for the two methods. What is especially interesting is that the cause of a disaster seems to affect the perceived seriousness of a scenario; however, from the study it can not be concluded if it is the cause per se that this effect can be attributed to, or whether people see the cause as a cursor for other types of consequences. For example, some persons argued that a disaster scenario caused by a terrorist attack is worse than a disaster scenario caused by a natural event, although it causes the same harm, since a terrorist attack that is successful may be a signal for an increased likelihood of future attacks.

Paper 4 concludes that the elicited values and preferences can provide input to risk analysis efforts and decision-making; however, more studies of similar kind are needed. They are needed in order to gain a deeper knowledge of how values differ between different social groups and also to investigate how different methods of eliciting values affect the results.

6.2 Evaluation and reflections on the research

An important step in the development of methods and knowledge meant for practical application, as was described in chapter 1, is the evaluation phase. In an evaluation, the advantages and limitations for example associated with suggested methods are highlighted. As such, an evaluation can be the first step towards modifying and improving a method, design or such. Below the three research themes will be addressed in turn and some general reflections will also be given.

6.2.1 Methods for vulnerability analysis of critical infrastructure networks

Evaluation of methods and models, as is the case in all evaluations of designed systems and artefacts, always has to be done in relation to the *purpose* and *intended use* of the method. Petersen (1994) argues that such an evaluation can be either *user-oriented* or *scientific*. Thus, there may be two types of reasons why an analysis based on a certain method or model does not lead to a successful outcome. First, the analysis may have been carried out in another way than what was intended or the purpose of the analysis may not be in accordance with the purpose of the method. These reasons are evaluated in what Petersen calls a user-oriented review. The model and method may be formally and scientifically correct but lead to a bad result due to wrong application of the method. This, in turn, can depend on the user, such as the user having a lack of understanding of the methods; however, it can also depend on the characteristics of the method, such as it being "user-unfriendly". Secondly, an analysis based on a method or model, although they are being used appropriately, may lead to an unsuccessful result due to fact that there are deficiencies and flaws in the method/model. These reasons can be evaluated in what Peterson calls a scientific review. Although both these perspectives definitely are important for method evaluation, the interest here will mainly be on the latter, since such a review is better suited to evaluate methods that still are in a developing stage. The methods presented in the present thesis are simply not yet adapted to suit the needs of potential users.

Conducting a thorough scientific review of a method can be a comprehensive task. Here, only a rather overall evaluation will be made and reflections will be given concerning what features need to be incorporated in the methods and which tasks need to be performed in order to guarantee that the analysis result is of high quality, given an appropriate use of the method.

As mentioned previously, the evaluation of methods must be related to the purpose of the method. Both methods use the operational definition of vulnerability as a point of departure and the purpose of the methods is to suggest a practical approach for meeting the requirements of the definition, given in chapter 5.2.1. An effect of this is that the methods should provide a quantitative approach to vulnerability analysis. In addition, the methods aim to be applicable to large-scale technical infrastructures that are possible to model as networks, i.e. the methods aim to be quite broad approaches to vulnerability analysis. Another purpose is that it should be possible to consider large-scale perturbations by use of the methods. Several of these purposes are clearly fulfilled; however, a number of areas need to be further addressed and reflected upon.

More concrete attack strategies (global vulnerability only)

Often very broad and generic attack strategies are used when analysing the global vulnerability of a system, such as random and directed removal of components. The intention is that these should represent real perturbations to the systems. Random removal is often said to represent natural phenomena, whereas removal directed at some specific components is said to represent a deliberate attack. These generic attack strategies can be very useful to get an overall picture of the vulnerability of a system, for example by comparing the vulnerability of the system to other systems or to some reference system; however, it may be difficult to draw concrete conclusions regarding the system's vulnerability to real perturbations. A possible remediation is to develop attack strategies that represent real perturbations more appropriately. For example, if the interest is to analyse the vulnerability of an electric distribution system to hurricanes, a purely random removal may not be adequate. In that case edges representing long overhead lines would probably be more likely to fail than shorter lines or underground cables. There is a clear need for developing more concrete attack strategies that can be more practically attractive. By using existing knowledge (statistics, expert judgments etc.) regarding which types of components are more likely to fail in the face of a specific perturbation, it should be possible to develop more representative attack strategies.

Validation of the functional models

It has been argued that the methods proposed above are model agnostic, i.e. basically any functional model can be used to model the consequences of perturbations. However, much is gained if the computation time can be kept low since the methods generally require a large number of calculations to be carried out. Therefore, it would be highly interesting to make detailed studies regarding the accuracy of different functional models. Of course, the required accuracy will depend on the purpose of the analysis, but if a coarser functional model correlates highly with more detailed models, in regards to the consequences that arise from perturbations, there are few reasons for using the more detailed models. What is very clear, however, is that the extremely rudimentary functional models, which is sometimes used in network analysis (for example when not distinguishing between different types of components), is not sufficient to capture the relevant features of most infrastructure systems.

Complementing the methods for analysis with methods for evaluation

The methods described above have so far been concerned with *analysis*, i.e. to find an approach that is able to characterise/estimate the vulnerability of a system that is consistent with the suggested operational definition. An essential step, subsequent to the analysis, is evaluation of the analysis result. However, no clear guidelines or

methods exist to assist this process; therefore, there is a need for developing guidelines in order to take the analysis to the next step. Of course any evaluation carried out in practice must be related to the underlying values – what is seen as an "acceptable vulnerability" by a specific person does not necessarily constitute an acceptable vulnerability from the view of another person.

Accounting for time-dependence

The methods described above are static since time is not explicitly modelled. The consequence of a perturbation is evaluated in terms of for example number of customers without power supply, or power loss. The duration of disruption and how fast the electric grid could be brought back to a normal state is however not considered, but certainly very important. This fact diminishes the practical value of the approach. By incorporating time-dependence in the analyses, the possibilities of incorporating human and organisational factors are also increased.

Applying the methods to other types of infrastructures

The methods have so far been applied to the electric power distribution system, although it is believed that the methods are possible to generalise to other levels of the electric power system and to other technical infrastructures as well. This must however be investigated in further detail. What primarily is needed in order to make generalisations possible is knowledge about the functioning of the particular system of interest in order to be able to suggest a functional model that captures the main aspects of the system.

Accounting for interdependencies between infrastructures

Previously, it was argued that the dependencies and interdependencies between infrastructure systems are increasing. There is a demand for methods that are able to take interdependencies into account. The network approach described above is believed to provide a platform for analysing interdependencies as well, since it can provide a common modelling basis for different types of infrastructure systems. Taking interdependencies into account is believed to be a great challenge for future research.

6.2.2 Emergency response capabilities

The overall purpose of the operational definition of emergency response capabilities was to make the concept more concrete and also to suggest a structure for how the concept can be analysed. The definition provides an ideal way for determining/characterising the capability of an actor; however, before the operational definition of emergency response capabilities can be applied in practice, i.e. before the definition is extended into a method, a couple of issues need to be

addressed. One such issue is how a task should be defined, e.g. which level of detail is appropriate in a specific situation. The same holds for how to describe the context, such as how detailed the descriptions can be made. In principle, these concerns are analogue to how detailed a risk scenario should be described in a risk analysis. Another issue concerns how it is possible to gain knowledge about how well specific tasks can be performed in a future potential scenario, i.e. what sources of evidence can be used. Here, of course, persons *in* the system are important sources of knowledge; however, other sources of knowledge may complement this source, such as various modelling techniques, computer simulation, and statistics and so on.

It is important to distinguish between the two purposes an analysis can have (described in chapter 3.3), i.e. the process-oriented and the decision-oriented approach, when evaluating the approach. It is believed that analysing capabilities based on the proposed operational definition can help people learn about how a future emergency may evolve and which factors that influence the final outcome. This can be accomplished by bringing people with different knowledge together and make them exchange ideas, create trust relations and hopefully also create synergies. Such analyses can also facilitate the creation of a common mental picture and mutual awareness of future possible emergencies. As such, it can be very useful for process-oriented purposes. However, an ambition here is also to be able to analyse capabilities from a decision-oriented perspective, i.e. to improve decisions regarding for example how capabilities can be enhanced. This ambition leads to higher requirements on the method for analysing capabilities, which must be addressed when such a method is suggested.

6.2.3 Value input to risk analysis and decision-making

The biggest limitation of the empirical study is that the sample used in the study consists of a quite homogenous group of students. It is important that the users of the results are aware of the composition of the sample so that the results are used with care when applied in other contexts. Of course, it is always preferable to elicit the values and preferences of the particular stakeholders that are relevant in the specific situation of interest; however, if this by any reason is not possible, one has to either somehow assume values or use values and preferences elicited in other contexts. The empirical study presented here can provide one input regarding which values that can be used as a basis for risk analyses and decision-making, but the study should be complemented with inputs from other studies.

Another reason for using the result from several studies as input to risk analyses and decision-making is that no methods are free of bias. Results from several methods can thus give insight into uncertainties regarding the values, which can be

propagated to the analysis. The presented empirical study made use of two fundamentally different methods, which increases the value of the study. However, by investigating the convergent validity further, the value of the research can increase even more, although the studies become more time-consuming and demanding for the participants.

The study showed that the cause of a disaster may be relevant for determining its seriousness. However, it is unclear whether this is an effect of people making inferences about indirect consequences. For example, in case of a disaster scenario caused by a terrorist act, people may have made inferences about increased airport security in the future, that other people are encouraged to perform acts of terrorism, consequences related to psychological distress etc. Thus, it may not be the cause per se that affects values, but the beliefs about the "consequences of the consequences" associated with terrorist acts. It is important that the users of these results are aware of the problems associated with the interpretation of the result.

6.3 Future work

The evaluative comments and reflections given above, point to a number of areas where future work is possible. Below a couple of these areas, although not exhaustive, are mentioned for each research theme.

Methods for vulnerability analysis of critical infrastructure networks

- The practical usefulness of the methods should be increased by for example providing methods for evaluating the results obtained from the vulnerability analyses. How to relate the analysis to possible risk and vulnerability reducing measures should also be addressed in future work.
- The framework for analysing single infrastructure networks, provided by network analysis and the operational definition of vulnerability, should be extended to enable analysis of interdependent infrastructure networks. Network analysis is believed to facilitate the process of connecting different types of infrastructures, into a system of systems.
- The approaches presented in the present thesis should be further evaluated in regards to how they need to be modified and developed in order to better capture the features that are relevant from a societal vulnerability perspective. Validations of the functional models used to estimate the consequences of perturbations should be performed.

Emergency response capabilities

- A first step to apply the proposed definition can be to use it to analyse the response of an event that has occurred. In doing that, the scope of the

analysis can be kept limited. The purpose of such an analysis can be to study how alternative contexts could have affected the response to the emergency, i.e. what could have happened if the service of technical infrastructure would have been unavailable?

- The next step is to suggest a method, based on the operational definition that can be used to analyse emergency response capabilities in a forward-looking manner. The goal of such an analysis could be to identify critical dependencies, resources or actors, i.e. factors that need to be in certain states in order for an actor to be able to perform its tasks. Such an analysis can then provide input to decisions regarding how to improve the capabilities.

Value input to risk analysis and decision-making

- Empirical studies of other groups should be conducted in order to investigate the generalisability of the values and preferences that have been elicited.
- Studies should be conducted using other attributes than those used in the study presented here, since many other attributes are also relevant from an emergency management perspective, such as attributes related to the environment, constitutional values, etc.
- The study conducted was concerned with judgements under certainty; however, when making decisions regarding future possible risk scenarios one cannot know for sure which scenario will occur, therefore it should be interesting to study how the values and preferences for the attributes would change if the trade-offs are framed in terms of judgements under uncertainty.
- Methods other than the two used in the present thesis to elicit values should be used to further investigate the convergent validity and uncertainties of attribute weights.

7 Concluding remarks

The research presented here has largely been driven by a need to improve the ability to analyse and make sense of complex systems. This is because many of the systems that are interesting for risk and vulnerability analyses in an emergency management context can be described as being complex. The main problem associated with complexity is that there are many dependencies and interactions between different parts of a system and between the system and its environment, which means that it is difficult to divide the system into sub-systems and analyse each sub-system separately.

Consider a hypothetical analysis of the fire risk in a building, which is a quite simple system to analyse if compared to a complex emergency involving an array of emergency response actors and technological systems of various kind. Often such analyses are conducted by dividing the system into sub-systems which are quite independent of each other and the sub-analyses are then aggregated into an overall picture of the risk. A possible way to conduct such an analysis would be to divide the system into three sub-systems: 1) the flame and smoke spread, 2) people's behaviour and the egress from the building, 3) technical fire protection systems. Of course, it is impossible to analyse each sub-system in complete isolation from the other systems, for example since the reason that people start to egress is that they become aware of a possible fire. However, in this case the number of interactions that need to be considered and the problem associated with dividing the system into sub-systems is quite small.

When considering more complex type of systems, the number of dependencies and interactions are more extensive and it is increasingly difficult to divide analyses into sub-analyses, and systems into more-or-less independent sub-systems. Consider an analysis of the assistance needs of the affected population due to the occurrence of an emergency. The assistance needs that arise will be heavily dependent upon the actions taken by the emergency response actors. An early initiated and well planned response would probably lead to the fact the needs that otherwise would have arisen are prevented. Similarly, there are difficulties of analysing how well an emergency response actor is carrying out certain tasks, since this often depends on how other emergency response actors are carrying out their tasks. In addition, two emergency response actors may need the same resource for meeting an assistance need within their area of responsibility. It is therefore often very difficult to conduct an analysis of a sub-system in isolation from analyses of other sub-systems with which it interacts. It is obvious that some type of holistic or systems perspective is needed, where interactions and dependencies among different sub-

systems are taken into account. This clearly poses great challenges for future research regarding complex systems, such as in the emergency management area.

Below a number of concluding remarks will be given in connection to the research aims of the present thesis.

Operational definitions

The present thesis has suggested two operational definitions; one for the concept of vulnerability and one for the concept of emergency response capabilities. The intention of the definitions is that they should provide ideal ways of characterising the concepts, which subsequently can provide a framework or a platform for developing methods for analysis. The aim has not been to suggest definitions that should be universally applied; instead the main aim has been to be concrete about how the concepts are being used in the present context.

Methods for vulnerability analysis of critical infrastructure networks

Two methods for conducting vulnerability analysis of critical infrastructure networks have been suggested; one focusing on global vulnerability and one focusing on identification of critical components. The methods should be seen as complements when it comes to analysing the vulnerability of a system. The first is about analysing the overall vulnerability of a system for specific perturbation and the second is about finding the components that are critical for the functioning of the system. As such, the second method is about gaining insight into the reasons for vulnerability of the system to perturbations.

It is clear that there is a need for methods for risk and vulnerability analysis of complex infrastructures. This especially applies for the electric power system in Sweden, where new legislation stipulates that all power companies owning power networks with a voltage lower than 220kV have to conduct risk and vulnerability analyses. However, what these risk and vulnerability analyses should include, which requirements that are applicable and so on, seem to be quite fuzzy but it is too early to say what effect the new legislation will have. Another issue is that it seems unclear which acceptance criteria should be applied when evaluating the results of a risk and/or vulnerability analysis. This has recently been pointed out by the Swedish National Audit Office in an extensive audit of the activities performed by the Swedish State to manage electric power disruptions (Riksrevisionen, 2007). Since the electric power distribution is a public utility for the society as a whole it is unsatisfactory that no clear directives have been stipulated.

Emergency response capabilities

The long-term aim of the research related to emergency response capabilities is to find ways, approaches and methods for understanding the behaviour of a complex emergency response system, especially what influences the capabilities of the system and how capabilities can be analysed. The purpose of such an analysis is to identify weaknesses and find ways of improving the capabilities. It would also be interesting to be able to draw conclusions about how the capabilities of the emergency response system affect the overall level of vulnerability or risk in the society.

The operational definition of emergency respone capabilities, suggested in the thesis, builds on the operational definitions of risk and vulnerability, which is believed to facilitate the bridging of the concepts. The definition especially emphasizes that the performance of tasks in an emergency situation depends on the context in which the tasks are being performed. Therefore, in order to understand the behavior of a complex emergency response system, composed of multiple actors, during an emergency, the interactions between actors, tasks, resources etc. need to be studied, i.e. requiring a systems perspective to be adopted. The research on this area is still in a very early stage and much effort is believed to be required before a fruitful approach can be stipulated. In the area of accident investigation, however, research that has an explicit systemic focus has been initiated (Hollnagel, 2004; Leveson, 2004a) and it is believed that these efforts can provide important sources of inspiration for further research.

People's value and preferences regarding potential disaster scenarios

In the present thesis an empirical study of people's values regarding disaster scenarios has been presented and discussed. The study, although only comprising a limited sample of individuals, is believed to provide input to risk analyses regarding which attributes that are relevant to study and also to decisions that are taken using the risk analyses as support regarding how to trade-off attributes. It is clear that risk analyses and risk management activities need to be more explicit regarding which values are being used as basis. Large-scale projects often have the resources to conduct specific elicitations with the relevant stakeholders; however, more small-scale projects most often do not have these resources. The empirical study presented in the present thesis, can provide valuable input to such small projects, but it needs to be complemented with results from studies of other groups in order to investigate how the results generalise to other groups.

7.1 Final comments

Analysing risks and vulnerabilities is an essential activity for proactive emergency management, since it is the stage where we try to gain knowledge about the future

behaviour of the systems of interest. Without such analyses any measures taken to improve systems, enhance capabilities, reduce vulnerability etc. are not grounded on a systematic approach to acquire knowledge and therefore suffer the risk of being ineffective or even counter-productive.

Since many of the systems that are relevant in a societal emergency management context are complex, the methods used to analyse them must be adapted to suit these systems. The research community has made much advancement, but still many challenges lie ahead.

8 References

Abrahamsson, M., Johansson, H., Fredholm, L. and Eriksson, K. (2007), "Analytical Input to Emergency Preparedness Planning at the Municipal Level - a Case Study", *14th TIEMS Annual Conference*, Trogir, Croatia.

Ackoff, R. L. (1971), "Towards a System of Systems Concept", *Management Science*, **17**(11): 661-671.

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. (2002), *Principles of Emergency Planning and Management*, Oxford, Oxford University Press.

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.

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

Anderson, P. (1999), "Complexity Theory and Organization Science", *Organization Science*, **10**(3): 216-232.

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.

Ashby, W. R. (1957), *An Introduction to Cybernetics*, London, Chapman & Hall Ltd.

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

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 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.

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

Bak, P. and Paczuski, M. (1995), "Complexity, contingency, and criticality", *Proc. Natl. Acad. Sci.*, **92**: 6689-6696.

Barabási, A.-L. (2002), *Linked: The New Science of Networks*, Cambridge, Perseus Books Group.

Barabási, A.-L. and Albert, R. (1999), "Emergence of Scaling in Random Networks", *Science*, **286**: 509-512.

Bellamy, L. J., Ale, B. J. M., Geyer, T. A. W., Goossens, L. H. J., Hale, A. R., Oh, J., Mud, M., Bloemhof, A., Papazoglou, I. A. and Whiston, J. Y. (2007), "Storybuilder - A tool for the analysis of accident reports", *Reliability Engineering & System Safety*, **92**: 735-744.

Billington, R., Singh, G. and Acharya, J. (2006), "Failure bunching phenomena in electric power transmission systems", *Proceedings of the Institution of Mechanical Engineers, Part O: Journal of Risk and Reliability*, **220**(1): 1-7.

Boin, A. (2004), "Lessons from Crisis Research", *International Studies Review*, **6**: 165-174.

Boin, A. and 't Hart, P. (2007), "The Crisis Approach", in *Handbook of Disaster Research*, Rodriguez, H., Quarantelli, Q. L. and Dynes, R. (Eds.), New York, Springer.

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.

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 Crises Management*, **15**(1): 51-59.

Boulding, K. E. (1956), "General Systems Theory - The Skeleton of Science", *Management Science*, **2**(3): 197-208.

Brooks, N. (2003), "Vulnerability, risk and adaptation: A conceptual framework", Working paper 38, Tyndall Centre for Climate Change Research, Norwich.

Brooks, N., Adger, W. N. and Kelly, P. M. (2005), "The determinants of vulnerability and adaptive capacity at the national level and the implications for adaptation", *Global Environmental Change*, **15**: 151-163.

Brown, T., Beyler, W. and Barton, D. (2004), "Assessing infrastructure interdependencies: the challange of risk analysis for complex adaptive systems", *International Journal of Critical Infrastructures*, **1**(1): 108-117.

Buchanan, M. (2001), *Ubiquity*, New York, Three Rivers Press.

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.

Carlson, J. M. and Doyle, J. (1999), "Highly optimized tolerance: A mechanism for power laws in designed systems", *Physical Review E*, **60**(2): 1412-1427.

CCMD (2004). Crisis and Emergency Management: A Guide for the Public Services of Canada, Canadian Centre for Management Development.

CCPS (2000), *Guidelines for Chemical Process Quantitative Risk Analysis*, Center for Chemical Process Safety, New York.

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

Cheok, M. C., Parry, G. W. and Sherry, R. R. (1998), "Use of importance measures in risk-informed regulatory applications", *Reliability Engineering & System Safety*, **60**: 213-226.

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.

Covello, V. T. and Mumpower, J. (1985), "Risk Analysis and Risk Management: An Historical Perspective", *Risk Analysis*, **5**(2): 103-120.

Cox, J. L. A. (2007), "Does Concern-Driven Risk Management Provide a Viable Alternative to QRA?" *Risk Analysis*, **27**(1): 27-43.

Cronstedt, M. (2002), "Prevention, Preparedness, Response, and Recovery - an outdated concept?" *Australian Journal of Emergency Management*, **17**(2): 10-13.

Cross, N. (1993), "Science and Design Methodology: A Review", *Research in Engineering Design*, **5**: 63-69.

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., Mitchell, J. T. and Scott, M. S. (2000), "Revealing the Vulnerability of People and Places: A Case Study of Georgetown County, South Carolina", *Annals of the Association of American Geographers*, **90**(4): 713-737.

Cutter, S. L. (2003), "The Vulnerability of Science and the Science of Vulnerability", *Annals of the Association of American Geographers*, **93**(1): 1-12.

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

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 Crises Management*, **15**(1): 18-29.

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

Dorogovtsev, S. N. and Mendes, J. F. F. (2002), "Evolution of Networks", *Advances in Physics*, **51**(4): 1079-1187.

Dudenhoeffer, D. D., Permann, M. R. and Sussman, E. M. (2002), "A Parallel Simulation Framework for Infrastructure Modeling and Analysis", *Proceedings of the 2002 Winter Simulation Conference*, San Diego.

Dynes, R. R. (1994), "Community Emergency Planning: False Assumptions and Inappropriate Analogies", *International Journal of Mass Emergencies and Disasters*, **12**(2): 141-158.

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

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

Epstein, J. M. (1999), "Agent-Based Computational Models and Generative Social Science", *Complexity*, **4**(5): 41-60.

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

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 Developement", *Risk Analysis*, **21**(5): 913-921.

Frey, R. E. (1991), "Another Look at Technology and Science", *Journal of Technology Education*, **3**(1): 16-29.

Fromm, J. (2005), "On Engineering and Emergence", *Preprint article, arXiv:nlin.AO/0601002, http://arxiv.org/ftp/nlin/papers/0601/0601002.pdf*.

Fujita, Y. and Hollnagel, E. (2004), "Failures without errors: quantification of context in HRA", *Reliability Engineering & System Safety*, **83**: 145-151.

Gardner, P. L. (1994), "The Relationship between Technology and Science: Some Historical and Philosophical Reflections. Part I", *International Journal of Technology and Design Education*, **4**: 123-153.

Gell-Mann, M. (1997), *The Quark and the Jaguar: Adventures in the simple and in the complex*, New York, W.H. Freeman and Co.

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., 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.

Hale, A. (2006), "Defining Resilience", in *Resilience engineering: concepts and precepts*, Hollnagel, E., Woods, D. D. and Leveson, N. (Eds.), Aldershot, Ashgate Publishing Limited.

Hansson, S. O. (2004), "Philosophical Perspectives on Risk", *Techné: Research in Philosophy and Technology*, **8**(1): 10-35.

Hansson, S. O. (2005), "The Epistemology of Technological Risk", *Techné: Research in Philosophy and Technology*, **9**(2): 68-80.

Haque, C. E. and Etkin, D. (2007), "People and community as constituent parts of hazards: the significance of societal dimensions in hazards analysis", *Natural Hazards*, **41**: 271-282.

Hatfield, A. J. and Hipel, K. W. (2002), "Risk and Systems Theory", *Risk Analysis*, **22**(6): 1043-1057.

Heylighen, F. (2003), "The Science of Self-organization and Adaptivity", *The Encyclopedia of Life Support Systems*, Oxford, Eolss Publishers.

Holland, J. H. (1995), *Hidden Order: How Adaptation Builds Complexity*, New York, Basic Books.

Hollnagel, E. (2004), *Barriers and accident prevention*, Aldershot, Ashgate Publishing.

Hollnagel, E. and Woods, D. D. (2006), "Epilogue: Resilience Engineering Precepts", in *Resilience Engineering: Concepts and Precepts*, Hollnagel, E., Woods, D. D. and Leveson, N. (Eds.), Aldershot, Ashgate Publishing Limited.

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

Holme, P. (2004), *Form and Function of Complex Networks*, PhD-thesis, Department of Physics, University of Umeå, Umeå.

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).

Holmgren, Å. (2006), "Using Graph Models to Analyze the Vulnerability of Electric Power Networks", *Risk Analysis*, **26**(4): 955-969.

Johansson, J. (2007), *Risk and Vulnerability Analysis of Large-Scale Technical Infrastructure*, Licenciate-thesis, Department of Industrial Electrical Engineering and Automation, Lund University, Lund.

Johansson, J., Jönsson, H. and Johansson, H. (2007), "Analysing the Vulnerability of Electric Distribution Systems: a Step Towards Incorporationg the Societal Consequences of Disruptions", *International Journal of Emergency Management*, **4**(1): 4-17.

Johansson, H. and Jönsson, H. (2007), *Metoder för risk- och sårbarhetsanalys ur ett systemperspektiv*, LUCRAM Report 1010, Lund University, Lund.

Jönsson, H., Johansson, H. and Abrahamsson, M. "Evaluating the Seriousness of Disaster Scenarios", *Manuscript*.

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

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.

Kasperson, R. E., Renn, O., Slovic, P., Brown, H. S., Emel, J., Goble, R., Kasperson, J. X. and Ratick, S. (1988), "The Social Amplification of Risk: A Conceptual Framework", *Risk Analysis*, **8**(2): 177-187.

Keeney, R. L. (1991), "A Prescriptive Framework for Individual Health and Safety Decisions", *Risk Analysis*, **11**(3): 523-533.

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

Keeney, R. L. (1995), "Understanding Life-Threatening Risks", *Risk Analysis*, **15**(6): 627-637.

Keeney, R. L. and Raiffa, H. (1976), *Decisions with Multiple Objectives: Preferences and Value Tradeoffs*, New York, John Wiley & Sons.

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. and Cook, B. K. (2006), "Bulk Power Grid Risk Analysis: Ranking Infrastructure Elements According to Their Risk Significance", Working Paper Series, Engineering Systems Division, Massachusetts Institute of Technology, Cambridge.

Kristensen, V., Aven, T. and Ford, D. (2006), "A new perspective on Renn and Klinke's approach to risk evaluation and management", *Reliability Engineering & System Safety*, **91**: 421-432.

Le Coze, J.-C. (2005), "Are organisations too complex to be integrated in technical risk assessment and current safety auditing?" *Safety Science*, **43**:613-638.

Lee, E. E., Mitchell, J. E. and Wallace, W. A. (2004), "Assessing Vulnerability of Proposed Designs for Interdependent Infrastructure Systems", *37th Hawaii International Conference on Systems Sciences*, IEEE.

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

Leveson, N. (2004b), "Model-Based Analysis of Socio-Technical Risk", Working Paper Series, Engineering Systems Division, Massachusetts Institute of Technology, Cambridge.

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

Lewin, R. (1999), *Complexity: Life at the edge of chaos*, London, Phoenix.

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

Manyena, S. B. (2006), "The concept of reilience revisited", *Disasters*, **30**(4): 433-450.

Marais, K., Dulac, N. and Leveson, N. (2004), "Beyond Normal Accidents and High Reliability Organizations: The Need for an Alternative Approach to Safety in Complex Systems", *Engineering Systems Division Symposium*, Massachusetts Institute of Technology, Cambridge.

Maslow, A. H. (1954), *Motivation and personality*, New York, Harper and Row.

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

McEntire, D. A. (2001), "Triggering agents, vulnerabilities and disaster reduction: towards a holistic paradigm", *Disaster Prevention and Management*, **10**(3): 189-196.

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

McEntire, D. A., Fuller, C., Johnston, C. W. and Weber, R. (2002), "A Comparison of Disaster Paradigms: The Search for a Holistic Policy Guide", *Public Administration Review*, **62**(3): 267-281.

McLoughlin, D. (1985), "A Framework for Integrated Emergency Management", *Public Administration Review*, **45**: 165-172.

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

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.

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*, **21**(5): 923-937.

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.

Newman, D. E., Nkei, B., Carreras, B. A., Dobson, I., Lynch, V. E. and Gradney, P. (2005), "Risk Assessment in Complex Interacting Infrastructure Systems", *38th Hawaii International Conference on Systems Sciences*.

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

Nilsen, T. and Aven, T. (2003), "Models and model uncertainty in the context of risk analysis", *Reliability Engineering & System Safety*, **79**(3): 309-317.

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

Ottens, M., Franssen, M., Kroes, P. and van de Poel, I. (2006), "Modelling infrastructures as socio-technical systems", *International Journal of Critical Infrastructures*, **2**(2-3): 133-145.

Ottino, J. M. (2003), "Complex Systems", *AIChE Journal*, **49**(2): 292-299.

Pariès, J. (2006), "Complexity, Emergence, Resilience..." *Resilience Engineering: concepts and precepts*, Leveson, N., Hollnagel, E. and Woods, D. D. (Eds.), Aldershot, Ashgate Publishing Limited.

Perrow, C. (1984), *Normal accidents*, New York, Basic Books.

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

Petersen, K. (1994), "European model evaluation activity", *Journal of Loss Prev. Process Ind.*, **7**(2): 130-132.

Phelan, S. E. (1999), "A Note on the Correspondance Between Complexity and Systems Theory", *Systems Practice and Action Research*, **12**(3): 237-246.

Phelan, S. E. (2001), "What is complexity science, really?" *Emergence*, **3**(1): 120-136.

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

Prigogine, I. (1997), *The end of certainty*, New York, Free Press.

Quarantelli, Q. L. (1997), "Ten Criteria for Evaluating the Management of Community Disasters", *Disasters*, **21**(1): 39-56.

Quarantelli, Q. L. (1998), "Major Criteria For Judging Disaster Planning And Managing Their Applicability In Developing Countries", Preliminary Paper #268, 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, N. (1975), *Reactory Safety Study - an Assessment of Accident Risks in U.S. Nuclear Power Plants*, U.S. Nuclear Regulatory Commission, Washington D.C.

Renn, O. (1992), "Concepts of Risk: A Classification", in *Social Theories of Risk*, Krimsky, S. and Golding, D. (Eds.), Westport, Praeger Publisher.

Renn, O. (1998), "Three decades of risk research: accomplishments and new challanges", *Journal of Risk Research*, **1**(1): 49-71.

Riksrevisionen (2007), *Statens insatser för att hantera omfattande elavbrott*, RiR 2007:17, Stockholm.

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 Infrastructures Interdependecies", *IEEE Control Systems Magazine*, **21**(6): 11-25.

Ropohl, G. (1999), "Philosophy of Socio-Technical Systems", *Techné: Research in Philosophy and Technology*, **4**(3): 59-71.

Rosing, H. (2003), *Riskfilosofi - begrepp, kunskap, handling*, Åbo Akademi, Åbo.

Rouvroye, J. L. and van den Bliek, E. G. (2002), "Comparing safety analysis techniques", *Reliability Engineering & System Safety*, **75**: 289-294.

Saleh, J. H. and Marais, K. (2006), "Highlights from the early (and pre-) history of reliability engineering", *Reliability Engineering & System Safety*, **91**: 249-256.

Salter, J. (1997), "Risk Management in a Disaster Management Context", *Journal of Contingencies and Crises Management*, **5**(1): 60-65.

Scott, J. (2000), *Social Network Analysis - A Handbook*, London, SAGE Publications.

SEMA (2006a), *Risk- och sårbarhetsananlyser - Vägledning för statliga myndigheter*, Swedish Emergency Management Agency, Stockholm.

SEMA (2006b), *Risk- och sårbarhetsananlyser - Vägledning för kommuner och landsting*, Swedish Emergency Management Agency, Stockholm.

SFS 2006:942, *Förordning om krisberedskap och höjd beredskap,* Svensk Författningssamling.

SFS 2006:544, *Lag om kommuners och landstings åtgärder inför och vid extraordinära händelser i fredstid och höjd beredskap*, Svensk Författningssamling.

SFS 1997:857, *Ellag*, Svensk Författningssamling.

SFS 1999:381, *Lag om åtgärder för att förebygga och begränsa följderna av allvarliga kemikalielyckor*, Svensk Författningssamling.

SFS 1987:10, *Plan- och bygglag*, Svensk Författningssamling.

Simon, H. (1996), *The Sciences of the Artificial*, Cambridge, The MIT Press.

Simpson, D. M., Rockaway, T. D., Weigel, T. A., Coomes, P. A. and Holloman, C. O. (2005), "Framing a new approach to critical infrastructure modeling and extreme events", *International Journal of Critical Infrastructures*, **1**(2/3): 125-143.

Skyttner, L. (1996), *General Systems Theory: An Introduction*, Houndmills, MacMillan Press Ltd.

Slovic, P. (1999), "Trust, Emotion, Sex, Politics, and Science: Surveying the Risk-Assessment Battlefield", *Risk Analysis*, **19**(4): 689-701.

Strogatz, S. H. (2001), "Exploring complex networks", *Nature*, **410**: 268-276.

't Hart, P. (1997), "Preparing Policy Makers for Crisis Management: The Role of Simulations", *Journal of Contingencies and Crises Management*, **5**(4): 207-215.

't Hart, P. (2001), "New Trends in Crisis Management Practice and Crisis Management Research: Setting the Agenda", *Journal of Contingencies and Crises Management*, **9**(4): 181-188.

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

Watts, D. J. and Strogatz, S. H. (1998), "Collective dynamics of 'small-worlds' networks", *Nature*, **393**: 440-442.

Webler, T., Rakel, H., Renn, O. and Johnson, B. (1995), "Eliciting and Classifying Concerns: A Methodological Critique", *Risk Analysis*, **15**(3): 421-436.

Weichselgartner, J. (2001), "Disaster mitigation: the concept of vulnerability revisited", *Disaster Prevention and Management*, **10**(2): 85-94.

Weinberg, G. M. (1975), *An Introduction to General Systems Thinking*, New York, John Wiley & Sons.

Wildavsky, A. (1988), *Searching for Safety*, New Brunswick, Transaction Publishers.

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

Wisner, B., Blaikie, P., Cannon, T. and Davis, I. (2004), *At Risk. Natural hazards, people's vulnerability and disasters*, London, Routlegde.

von Winterfeldt, D. and Edwards, W. (1986), *Decision Analysis and Behavioral Research*, Cambridge, Cambridge University Press.

Zimmerman, R. (2001), "Social Implications of Infrastructure Interactions", *Journal of Urban Technology*, **8**(3): 97-119.

Appendix: The 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., "Identifying Critical Components in Technical Infrastructure Networks", Submitted to Journal of Risk and Reliability after invitation from the editor of ESREL 2007. Slightly adapted from Jönsson, H., Johansson, J. and Johansson, H. (2007), "Identifying Critical Components of Electric Power Systems: A Network Analytic Approach", *Risk, Reliability and Societal Safety* **1**:889-896, Proceedings of the European Safety and Reliability Conference 2007, Stavanger, Norway.

Paper III 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.

Paper IV Jönsson, H., Johansson, H. and Abrahamsson, M. "Evaluating the Seriousness of Disasters: Implications for Societal Decision Making". (Manuscript.)

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., "Identifying Critical Components in Technical Infrastructure Networks", Submitted to Journal of Risk and Reliability after invitation from the editor of ESREL 2007. Slightly adapted from Jönsson, H., Johansson, J. and Johansson, H. (2007), "Identifying Critical Components of Electric Power Systems: A Network Analytic Approach", *Risk, Reliability and Societal Safety* **1**:889-896, Proceedings of the European Safety and Reliability Conference 2007, Stavanger, Norway.

Paper III

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.

Paper IV

Jönsson, H., Johansson, H. and Abrahamsson, M. “Evaluating the Seriousness of Disasters: Implications for Societal Decision Making”. (Manuscript.)

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

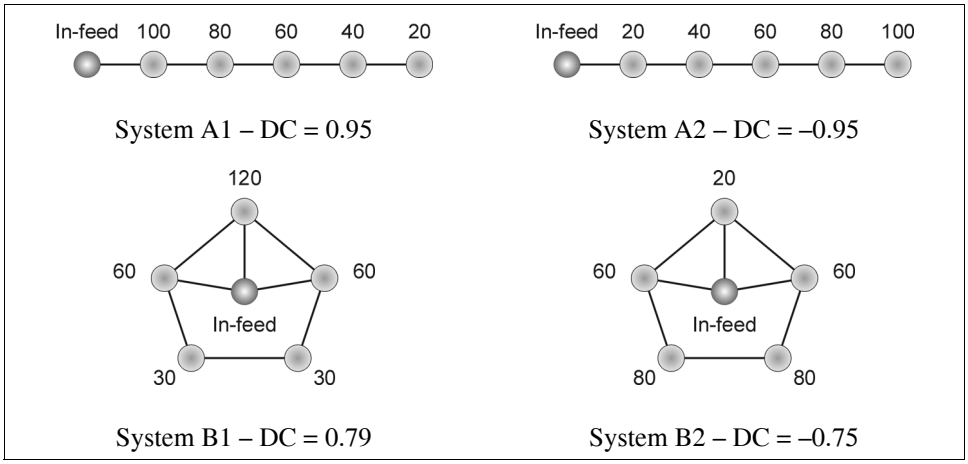
The result usually obtained from network-based vulnerability analyses is a plot of the performance measure as a function of the fraction of nodes or edges that have been removed. By studying this plot, conclusions regarding the vulnerability can be drawn, for example by comparing different systems. However, 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 $\mathrm{CE}_i > 0$ (Equation 2).

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

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

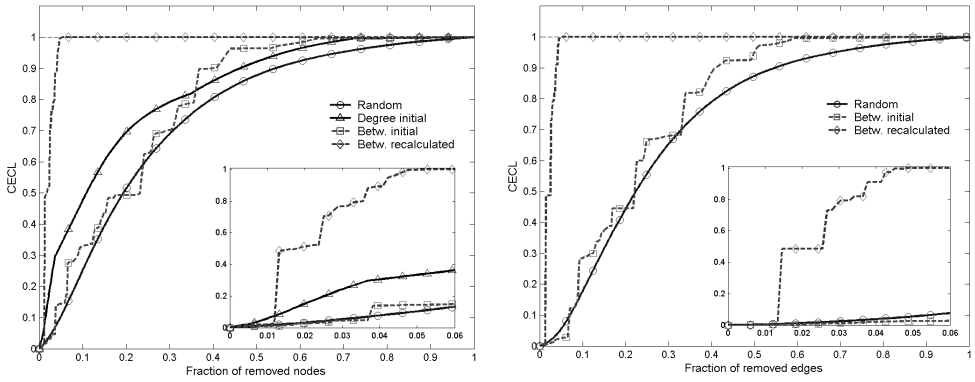
measure is based on the shortest paths between all in-feed points and distribution substations and is calculated as the sum of shortest paths traversing a specific node or edge, similar to the algorithm suggested by Newman (2001). However, instead of calculating the shortest paths between all pairs of 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

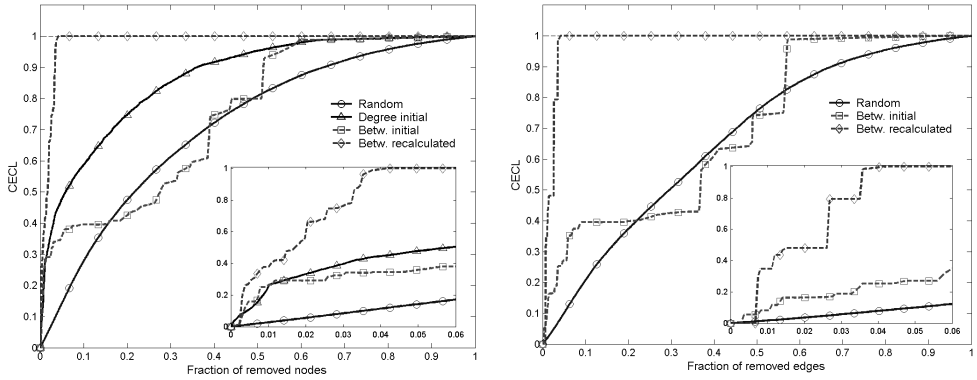
The most harmful removal strategy for System A is, as expected, the recalculated betweenness (Figure 2). For this strategy, all customers have lost power supply after the removal of 5.3% of the nodes or 5.2% of the edges. The strategy based on initial betweenness is only slightly more harmful than the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

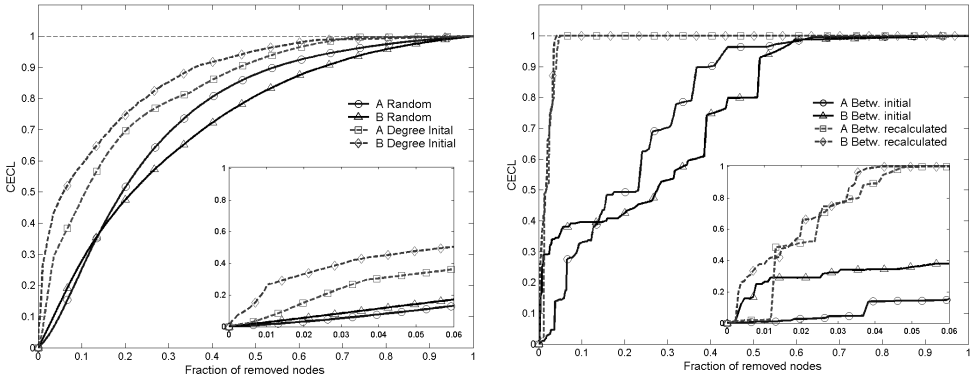


The node and edge-based removal strategies are very similar for both Systems A and B. This is due to the fact that the systems are mainly radially fed, *i.e.*, most nodes have a degree of two. In the remaining part of this paper, we focus on node-based removals, but much of the discussion is equally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

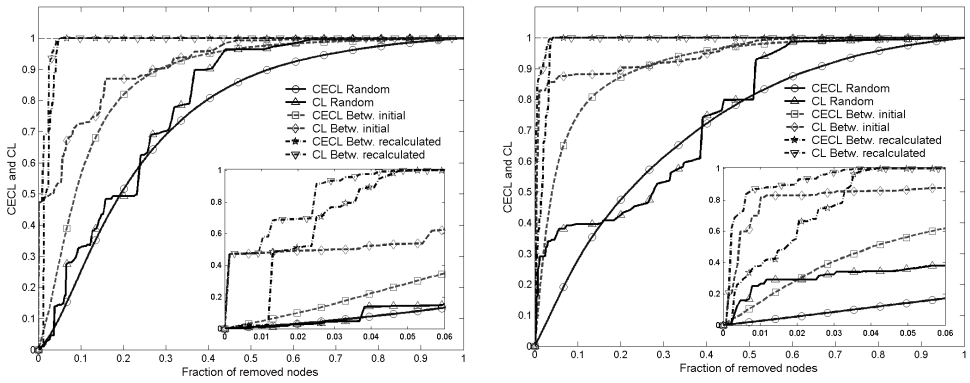
Note: * The letter in this column refers to the system that scores best on the particular measure

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.

Identifying Critical Components in Technical Infrastructure Networks

H. Jönsson
Department of Fire Safety Engineering and Systems Safety, Lund University, Lund, Sweden.

J. Johansson
Department of Industrial Electrical Engineering and Automation, Lund University, Lund, Sweden.

H. Johansson
Department of Fire Safety Engineering and Systems Safety, Lund University, Lund, Sweden.

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. In the present paper, we present 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 also include a component being unavailable by other reasons, such as maintenance. We use electric power distribution systems 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 elec-

tric power systems causing severe consequences that illustrate the importance of such systems. Examples of these power outages include the prolonged power outages in the central areas of Auckland, New Zealand, in 1998 [**1**], the large-scale outages in the eastern USA in 2003 [**2**] and the disruptions following the blackout in Sweden 2003 [**3**].

Network analysis has previously been utilised 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 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 implies that the negative consequences due 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, failures 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 not 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 fictive 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, e.g. [**16, 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 due to 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 characterised 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. 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.[1] 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 infeed transformer in an electric distribution system which constitutes the only point of infeed 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, i.e. these are the most critical components. 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 498501 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. 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 con-

[1] The number of possible failure sets is $\frac{t!}{(t-n)!\cdot n!}$, where t is the total number of system components and n is the size of the failure sets.

taining 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 $S^i_1,..,S^i_m$. 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 due to the failures, $C(F)$, is greater than the sum of the consequences for the proper subsets of F, for all possible divisions $V_1,...,V_p$:

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

A synergistic consequence of a failure set, $C_{syn}(F)$, 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).

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

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

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

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 due to the fact that all the failures in the set occur simultaneously, i.e. the consequences that arise *in addition* to the consequences due to the individual subsets. For example, synergistic consequences of size 3 failure sets cannot be calculated by adding up the consequences of its size 2 and 1 subsets. Thus, one cannot identify such critical failure sets 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 con-

sequences. 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 due 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 due 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.

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

where c_i is a specific component and n the size of the failure set. $\sum C_{syn}(F|c_i \in F, n)$ is the sum of the synergistic consequences of all failure sets of size n that contain the components of interest, c_i. $\sum C_{syn}(F|n)$ 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. Firstly, 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.

Secondly, in network analysis it is common that the electrical properties of the power system are neglected, i.e. no physical 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 HV/MV 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 due 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. Firstly, there has to be an unbroken path between the substation and at least one in-feed node. Secondly, 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 due to failures in the power system should be evaluated with regards to the deterioration of these services. In a previous paper we suggested a measure called *Customer Equivalents* (CE) 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, fictive electric distribution network. It consists of 1 in-feed node, 5 load nodes, and 7 edges, i.e. 13 components in total (see Figure 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.

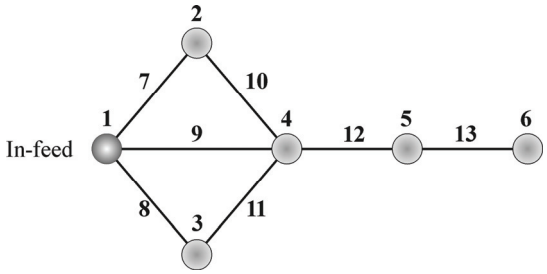


Figure 1. Example network. The numbers in the figure correspond to the component number of the specific node or edge.

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 Figure 2 scatter plots of all synergistic failure sets of size 2 and size 3 are presented. The figures show that some failure sets give rise to large consequences where the synergistic fraction is small. This indicates that a large part of the total consequences can be referred to a subset of the failure set. Consider, for example, the {4 8} set, which means that components 4 and 8 have failed, in Figure 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 Figure 2 it can also be seen that the failure set {7 8 9} is highly critical (maximum consequence) with a 100% synergistic consequence, i.e. none of the consequences of the failure set can be referred to any of its subsets. This set can be contrasted with {4 7 8}, which leads to the same consequences but only has 20% 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% 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.

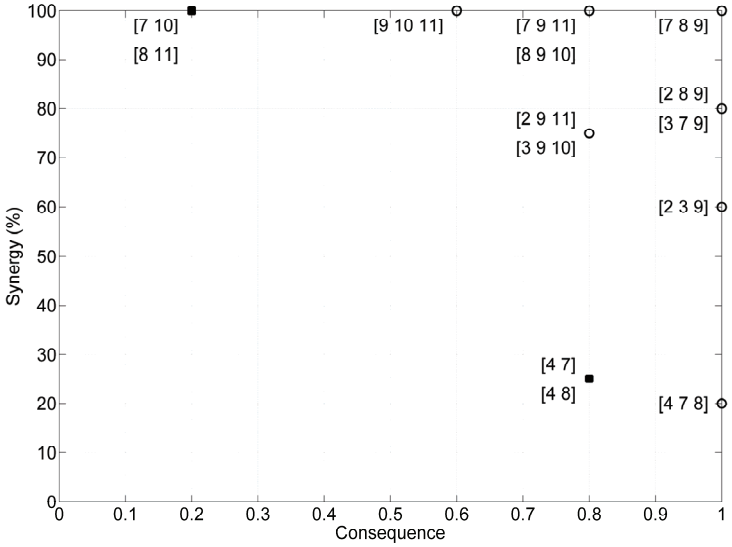


Figure 2. Consequence-synergistic scatter plot of synergistic failure sets of size 2 (filled squares) and size 3 (circles). The consequences of the failure sets, C(F) are presented on the horizontal axis and the fraction of synergistic consequences, f_{syn}, is presented on the vertical axis.

In Table 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 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.

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.

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.

c_i	1 failure		2 failures		3 failures	
	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.

c_i	2 failures		3 failures	
	Con. (%)	Rank	Con (%)	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	---

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 substations is modelled as a node and the bus bar breakers are modelled as edges. The MV/LV substations are modelled as single nodes. The aggregated nominal power rating for HV/MV transformers is 320 MVA and the aggregated peak power demand is 177 MVA, distributed 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 sectionalis-

ers and breakers are modelled as closed. This assumption leads, in some way, to an idealised 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:

$$CE_i = \frac{\left(\frac{N_i}{\overline{N}} + \frac{P_i}{\overline{P}}\right)}{2} \tag{6}$$

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

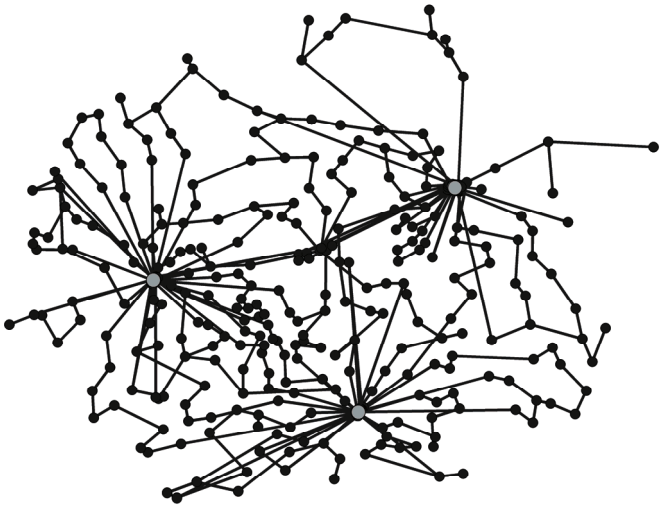


Figure 3. Overview of the electric distribution system. The larger circles indicate in-feed nodes and the smaller circles indicate load nodes and transfer nodes.

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 sets have synergistic consequences, respectively. In Figure 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 this analysis the failure sets of size 2 with consequences larger than 0.0488 and synergy fraction larger than 79% have been chosen for further study. For failure sets of size 3, sets

with consequences larger than 0.1020 and synergy fraction larger than 36% have been selected for further study. These failure sets are presented in Table 4.

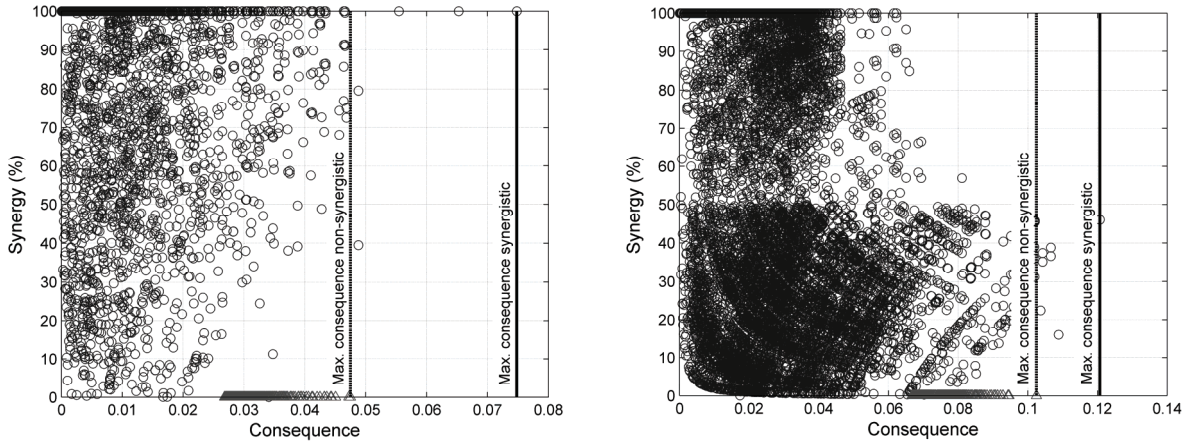


Figure 4. Consequence-synergistic scatter plot of synergistic failure sets of size 2 (a) and size 3 (b). The consequences of the failure sets, *C(F)*, are presented on the horizontal axis and the fraction of synergistic consequences, f_{syn}, is presented on the vertical axis. Synergistic failure sets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

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 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.

Table 5. Criticality of components in single and multiple failures.

Rank	1 failure		2 failures		3 failures	
	c_i	C	c_i	$\overline{C}$	c_i	$\overline{C}$
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	
	c_i	Con (%)	c_i	Con (%)
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

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 to realistically quantify the probability of simultaneous failures, especially for common cause failures and malicious attacks. Instead of trying to identify the phenomena that lead to common cause failures and 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.
3 **Larsson, S.** and **Ek, E.** The blackout in Southern Sweden and Eastern Denmark, September 23, 2003. *Proc. IEEE PES General Meeting*, 2004, Denver.
4 **Albert, R.**, **Albert, I.** and **Nakarado, G.L.** Structural vulnerability of the North American power grid. *Physical Review 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. *The European Physical Journal 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. *International Journal of Emergency Management*, 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 Letters*, 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. *Journal of Contingencies and Crisis Management*, 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. *Transportation Research Part A*, 2006, **40,** 537-560.
15 **Buckle, P.** and **Mars, G.** New approaches to assessing vulnerability and resilience. *Australian Journal of Emergency Management*, 2000, **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 and Management*, 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. *Physical Review 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. *Journal of Urban Technology*, 2002, **9**(1), 109-123.
24 **Michaud, D.** and **Apostolakis, G. E.** Methodology for Ranking the Elements of Water-Supply Networks. *Journal of Infrastructure Systems*, 2006, **12**(4), 230-242.

AN OPERATIONAL DEFINITION OF EMERGENCY RESPONSE CAPABILITIES

Henrik Jönsson[1,2,3]
Marcus Abrahamsson[1,2]
Henrik Johansson[1,2]

Lund University

Keywords

Emergency response capabilities, operational definition, analytic framework.

Abstract

Well developed emergency response capabilities are crucial in order to keep the risk in a community at low levels. Analysing these capabilities before an emergency occurs is important since it can identify weaknesses and possibilities for improvements. To start off from an operational definition is a possible point of departure in such an analysis. In this paper, therefore, we develop an operational definition of emergency response capabilities, which builds on systems theory and an operational definition of risk. The definition includes three essential elements; the task to which the capability is related, measures of how well that task can be performed and a description of the context affecting the performance of that particular task. The definition makes clear that the context might have large effects on how well a task can be performed and that there are uncertainties both regarding the context and how well a task can be performed given a context. Furthermore, we argue that it should be possible to make judgements about any statements that are made in the analysis regarding their validity and therefore the tasks and performance measures must be defined accordingly. The conclusion is that the operational definition provides an analytic structure which can help actors to gain knowledge about their emergency response capabilities and limits thereof.

Introduction

In the ideal world all hazards facing a community can be prevented and kept from materialising. Preventive risk reductions are indeed often effective in mitigating hazards; unfortunately perfect prevention is virtually impossible. Actually, it might be counter-effective to excessively focus on preventive measures since this often leads to an increased level of community vulnerability (McEntire, 2001), which is also known as the vulnerability paradox (Boin, 2004). In addition, many hazards are beyond the human ability to prevent (Gundel, 2005; McEntire, 2005) or beyond the authority of specific organisations to influence. Furthermore, prevention and mitigation measures might be known but impracticable because they are associated with too high costs, require technology that has not yet been developed or are otherwise not feasible. Another issue is that some hazards are extremely hard to predict and therefore impossible to prevent (Gundel, 2005). Because of these inherent insufficiencies of preventive strategies, it is sensible to complement preventive measures with mitigation and preparation efforts in order to increase response capabilities and reduce vulnerabilities in communities, so that the consequences are kept

[1] Department of Fire Safety Engineering, Lund University, P.O. Box 118, SE-221 00 Lund, Sweden.
[2] Lund University Centre of Risk Analysis and Management (LUCRAM).
[3] Corresponding author, henrik.jonsson@brand.lth.se.

at low levels once a hazard materialises. Achieving a balance between prevention and resilience (developing a capacity to absorb, respond to and recover from events) is thus a rational strategy in managing the risk in a community.

When a hazard materialises it exposes people, organisations and infrastructure in the community to strains and stresses of various magnitude, which put demands on their capabilities to resist, cope with and recover from the potentially harmful events. In such situations needs arise because fundamental values, such as human values, are threatened. These needs have to be met in a timely manner in order to minimise the negative consequences. However, in crises and emergencies, affected persons and groups may lack the capabilities (such as lacking the resources, knowledge or skills) that are required for meeting some of these needs, thus causing needs for external assistance to emerge. Meeting these needs then become the task for emergency management organisations (Fire and Emergency Services, NGOs etc.), which thus put demands on their emergency response capabilities. An important step in order to attain good emergency response capabilities is to work proactively with emergency planning and preparedness (Coles and Buckle, 2004). In the proactive work it is important to analyse and evaluate the existing emergency response capabilities in the organisation in order to highlight weaknesses and possibilities for improvements. Furthermore, conducting regular assessments are crucial since organisations and the environment in which they operate, constantly undergo change, which means that organisations have to adjust and adapt their current activities and strategies to even maintain their existing emergency response capability.

Suggestions of methods and frameworks for assessing capabilities have been made previously in the research literature and in various guidelines, e.g. Anderson and Woodrow (1991), UNDP (1998), IFRC (1999), Kuban and MacKenzie-Carey (2001). Some of these methods focus on organisational capabilities while other focus on the capabilities of the affected population to self-protect. An issue in applying these methods, however, is that there is no general consensus of how the relevant concepts are to be interpreted (Buckle and Mars, 2000; Weichelsgartner, 2001), which is exacerbated by the general lack of operational definitions. Furthermore, these frameworks generally provide a limited guidance of how to analyse capabilities in order to ensure the validity of the analysis. The aim of this paper is therefore to operationally define emergency response capability and the intention is that the operational definition should provide a framework for analysis as well. Here, an operational definition of emergency response capability is considered to be a definition that provides an operation or procedure, which can be used to determine what is required to comply with the definition. The definition builds on systems theory and an existing operational definition of risk. Therefore, we first review the definition of risk and also extend it to include the concept of vulnerability, which is tightly coupled to capability.

Risk framework

The concept of risk is used across many scientific disciplines and is also extensively used in practice. However, there is no general consensus regarding the definition of risk (Fischhoff, Watson et al, 1984). According to Renn all definitions of risk have in common that they make a distinction between reality and possibility and he proposes to define risk as “the possibility that human actions or events lead to consequences that affect aspects of what human values” (Renn, 1998). According to the standpoint on risk that is adopted in this paper, the risk in a system depends on two essential components; the likelihood of harmful events and the consequences of them. However, this view is by no means accepted universally. In some disciplinary areas related to emergency management, risk is given a different meaning, which is also pointed out by Dilley and Boudreau (2001) who argues that risk is sometimes used only referring to external events and hazards, not the consequences for the system in question. Cutter and colleagues, for example, relate risk only to the external hazard agent, where it is seen as “an objective measure of the likelihood of a hazard event” (Cutter, Boruff et al, 2003). References to the consequences of the hazards are thus not made in this definition. McEntire argues that “risk is a result of proximity or exposure to triggering agents, which increase the probability of disaster”(McEntire, 2001). This

definition clearly expands on the one proposed by Cutter and colleagues. In our view proximity to triggering agents contributes to the risk; however it is not the only factor that determines which consequences that arise. The approach to risk chosen in this paper leads to the conclusion that the purpose of all emergency management efforts, whether it is in the form of prevention, preparedness, response or recovery, is to reduce the risks, by reducing the likelihood of harmful event, the consequences of them or a combination of both.

A quantitative, operational definition of risk is proposed by Kaplan and colleagues (Kaplan and Garrick, 1981; Kaplan, 1997; Kaplan, Haimes et al, 2001) and is used extensively in risk research. The definition is based on systems theory and it is assumed that one has defined a system for which the risk is to be estimated. A system is perceived as a collection of state variables that can be used to describe the world. It is important to note that the system and the real world is not the same thing. Since "…every material object contains no less than an infinity of variables and therefore of possible systems" (Ashby, 1957) one has to define the system with the objective to achieve a good enough, for the purpose of the analysis, representation of the real world. The state variables can be lumped together into elements that consist of one or a collection of such variables and constitute some kind of meaningful unit in the context of interest. Here, for example, an element can be the Fire and Emergency Services which can be described by several state variables of which one could be the number of fire fighters that are engaged in an emergency response operation. One could employ a more detailed system definition, for example using individual fire fighters as elements in the system, but in the present context it is sufficient to use emergency response organisations as the elements of interest.

The assessment of emergency response organisations' capabilities has similarities with the problem of risk assessment. Both types of assessments are concerned with potential events that can happen in the future and therefore the development of an operational definition of emergency response capabilities can benefit from using the definition of risk as a point of departure. Of central importance in the definition of risk referred to above is the notion of scenarios, which is defined as "a trajectory in the state space of the system" (Kaplan, 1997). A scenario can thus be seen as the progression of the system over time. In determining the risk in a system one has to identify all (at least the most important ones) scenarios that deviate from the "success scenario", S_0. S_0 denotes a scenario where everything in the system behaves as intended and scenarios that deviate from S_0 are called risk scenarios. After estimating the probability and consequence of each scenario, one ends up with a set of risk scenarios (S_i) and their corresponding probabilities (L_i) and consequences (X_i). This set, called the "set of triplets", *is* the risk in the system. Therefore, when determining the risk in a system one really has to find the answer to the three questions: "What can go wrong?", "How likely is it?", "What are the consequences?" (Kaplan, 1997). Based on the set of triplets several risk metrics and measures can be expressed in order to facilitate risk presentations and decision making.

Obviously, an important issue resides in deciding which negative consequences to include in the definition of risk. Ashby uses the term essential variable to refer to a state variable that is related to a consequence dimension, i.e. the variables that are important to protect (Ashby, 1957). Consequences can be said to arise when these essential variables take on values outside some predefined range. However, there is no general answer to which state variables that should be seen as essential, since the consequences of interest depend on the values that the analysis is based on. The consequences to consider are thus contingent on the context of the particular analysis, such as its purpose. In addition, at which point in time the consequences should be estimated is also contingent on the particular context. Traditional application of the quantitative definition of risk, in what is frequently called "technical risk analyses", has been claimed to be too narrow in only focusing on a single consequence dimension (Renn, 1998), and only focusing on immediate impacts after a hazardous event (Einarsson and Rausand, 1998). However, we argue that there are no preconditions of which consequence dimensions to use when employing the quantitative definition of risk. The criticism thus addresses the traditional *application* of risk analysis, not the

definition of risk per se. Therefore, we believe that the quantitative definition of risk provides a suitable platform in an emergency management context as well.

Incorporating vulnerability into the risk framework

Research over the last couple of decades has recognised the limitations of the previously predominant view, in which the hazards where seen as the main concern for emergency and risk management. Since then there has been a shift in focus to a view that also account for the vulnerability of the exposed systems, e.g. persons, groups, organisations, communities (Weischelsgartner, 2001; Wisner, Blaikie et al, 2004). However, there is no general consensus as to how vulnerability is to be conceptualised, and some definitions are even contradictory (Cutter, Mitchell et al, 2000; Dilley and Boudreau, 2001; Haimes, 2006).

According to the view adopted in this paper the overall risk in a system is a result of the interactions between the characteristics of the various hazardous events that might affect the system and a range of "vulnerability inducing" factors (e.g. physical, economical, institutional and societal) that characterises the system (Salter, 1997; Dilley and Boudreau, 2001; Sarewitz, Pielke Jr. et al, 2003). These factors either aggravate or alleviate the effects of various hazardous events, but those "factors that make a system vulnerable to a hazard will depend on the nature of the system and the type of hazard in question" (Brooks, Adger et al, 2005). Therefore, vulnerability is context-dependent and has to be related to a specific hazardous event to be meaningful (Dilley and Boudreau, 2001). A corollary of this is that a system that is vulnerable to a certain hazardous events is not necessarily vulnerable to other, although there often exist generic factors that altersthe system's vulnerability to many hazards (Brooks, Adger et al, 2005). In this paper we use vulnerability to represent an emergent system property[4] that determines the effect a specific hazardous event has on the essential variables of the system.

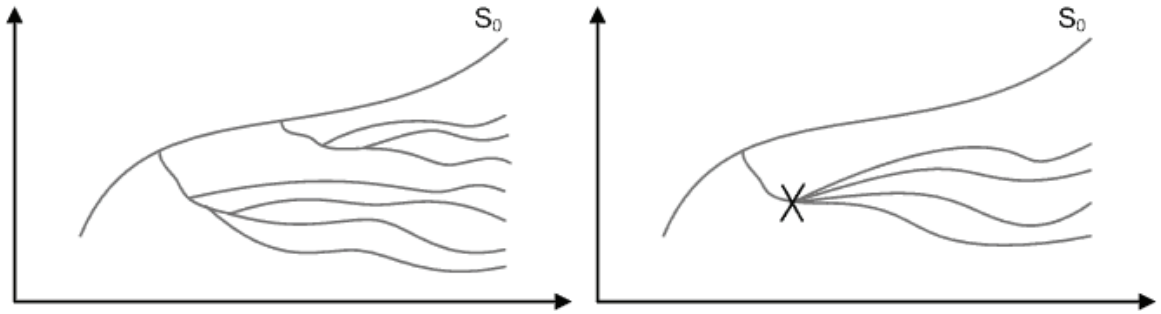
The framework provided by the quantitative definition of risk, referred to above, can also be utilized to define vulnerability in that the vulnerability of a system can be expressed as a "set of triplets". An imperative difference from the definition of risk, however, follows from the fact that vulnerability must be related to a specific hazardous event. The risk scenarios, i.e. the trajectories in the state space, described by the set of triplets are thus contingent on that the specific hazard has materialised and exposed the system. Thus, the vulnerability in a system is the answer to the three questions; "What can happen?", "How likely is it?" and "What are the consequences", where the answers are contingent upon that a specific hazardous event affects the system. In Figure 1 the difference between the definition of risk and vulnerability is illustrated using a state space representation.

To illustrate the use of the triplet assume that a community's vulnerability to a release of chlorine gas due to train derailment close to the city is to be analysed. The purpose of the analysis, such as whether the physical consequences (e.g. death and injuries), the consequences to the community's future prosperity, both these factors, or other factors are of interest, can have large effects on which the relevant scenarios are and which consequence dimensions to consider. Assume that we in this example are interested in the direct physical consequences. Next, one has to identify what can happen given that there is a chlorine gas release. One factor that affects the consequences of the gas release is the wind direction. If it blows away from the city negative consequences do not arise. If it blows towards the city the extent to which populated areas are exposed to the gas depends on for example wind speed, atmospheric stability class, and land exploitation proximate to the railway track. Furthermore, the extent to which the population in the affected areas are

[4] A closely related definition of vulnerability does not regard vulnerability as a system property, e.g. a "property of the whole". Instead vulnerability refers to the system's states or the conditions that "can be exploited to adversely affect (cause harm or damage to) that system" (Haimes 2006). Furtermore, Einarsson and Rausand suggest that vulnerability should be used to describe the *properties* of a system that "may weaken its ability to survive and perform its mission in the presence of threats" (Einarsson and Rausand 1998).

exposed to toxic gas concentrations for example depend on whether warning systems are in function and alert the community inhabitants, whether the ventilation can be shut down, either automatically or manually etc. From these varying conditions a number of scenarios can be defined and consequences and probabilities of each scenario can be estimated. The resulting set of triplets then represents the vulnerability of the community to the specified hazardous event.

Figure 1. The difference between risk and vulnerability using state space representations.*



* The definition of risk is illustrated to the left and the definition of vulnerability is illustrated to the right. The main difference can be seen in the right part of the figure where the scenarios in the definition of vulnerability are contingent on that a particular hazardous event has occurred and affected the system. This event is marked by a cross in the right figure. In a risk analysis, on the other hand, one is interested in all scenarios that deviate from the "success scenario", S_0.

It is important to note that the specification of the hazardous event and the purpose of the analysis can have large effects on the description and analysis of vulnerability. Assume for example that in addition to the specification of the hazardous event made above, the wind blows towards the city. The community is clearly more vulnerable to this event since the possibility of the wind blowing in a "harmless" direction is dismissed. However, no characteristics of the community has been altered, only the specification of the hazardous event. Therefore, we argue that it is important to clearly state the event that the vulnerability is related to. Regarding the purpose of the analysis, assume that instead of analysing the vulnerability of the community we are interested in the vulnerability of the responsible railway company to a chlorine gas release. The consequence dimensions of interest will be different than above, since the interest resides in how the company is affected. Damages to goodwill and costs due to damage liabilities are examples of consequence dimensions of interest. The physical consequences to the population certainly might have an effect on how the railway company is affected, but it is not necessarily in the central interest of the analysis. This example shows that changing the purpose of the analysis might also lead to a change in system definition. Thus, when analysing vulnerability it is important to clearly state the purpose of the analysis along with system definition and system boundaries.

Emergency response capabilities

The use of the term vulnerability has suffered some criticism since its main focus is on the negative characteristics of systems, i.e. their inabilities. The criticism has especially addressed those instances when vulnerability is applied to individuals or social groups since it might lead to a view that "treat them as passive victims" (Cannon, Twigg et al, 2003). Instead, the argument goes, one should focus on the capabilities of systems to resist, cope with and recover from hazardous events. In this paper we are interested in applying the concepts to emergency response organisations. However, this focus is not to be interpreted that we are depreciating the importance of the capabilities of the affected population. Both these types of capabilities are crucial for the overall vulnerability of a community. We agree with Coles and Buckle who state that "governments are rarely able to meet all needs of affected people" (Coles and Buckle, 2004), therefore it is important that the affected population are empowered and encouraged to take proper actions.

As described in the introduction, emergencies and crises are often characterised by the fact that the affected population is not self-sufficient. Thus, needs of external assistance emerge, which if unmet will lead to negative consequences. The extent and character of the assistance needs is determined by factors such as the nature of the hazardous events, its severity and the capabilities of the affected to resist, respond to, and recover from the events. Relieving these needs and preventing additional needs to arise becomes the overarching goal for the emergency response organisations in a community, e.g. Fire and Emergency Services, NGOs etc. Perry and Lindell argues that it is important that emergency planning aims at identifying "the demands that a disaster would impose upon emergency response organisations and the resources (personnel, facilities, equipment and materials) that are needed by those organisations to meet the emergency demands" (Perry and Lindell, 2003). However, it is not only the demands directly imposed by the hazard agent upon the emergency response organisations that they have to deal with. Other demands arise due to the fact that a response is initiated. As such, two fundamentally different types of demands can be distinguished; *agent generated demands* – those stemming directly from the hazardous event, such as demand for meeting assistance needs and demands for hazard containment, and *response generated demands* – those emerging from the response to the emergency, such as information distribution and coordination (Dynes, 1994). What ultimately determines the success of an overall emergency response is to which extent the agent generated demands are met, since these are related to the essential variables of the system. The extent to which the response generated demands are met have an indirect effect in that it facilitates or impedes the possibilities to meet the agent generated demands.

An operational definition of emergency response capabilities

Whether emergency response organisations are able to meet the demands that are put on them in a crisis depends on their *emergency response capabilities*. The operational definition of emergency response capabilities that is proposed in this paper acknowledges that analysing capabilities and evaluating them are distinct processes. Evaluating capabilities, i.e. deciding whether a capability is acceptable or not, is a process that is intrinsically value-laden and subjective. The proposed definition aims at facilitating an *analysis* of capabilities and does not address issues of evaluation. The definition includes three essential elements: the *task* to which the capability is related, *measures* of how well that task can be performed and a description of the *context* affecting the performance of that particular task. However, given a specific context there might still be uncertainties about how well the task can be performed, which can be expressed as a set of scenarios similar to the quantitative definition of risk. In the following sections these elements are explored further.

A capability should be related to the performance of a specific task or function when being analysed, i.e. capability to do what?, not just capability in general. For instance, in the case of train derailment mentioned above examples of tasks for the actor Fire and Emergency Service might be "to stop the release" and "to issue warnings". In being specific about the particular task, capabilities are related to the actual course of events, which enables the analyst to be concrete about whether that particular task can be performed or not and providing support for or against it. We argue that in an analysis of capabilities one should strive towards defining tasks such that it is possible to determine if they can be performed or not (or to which degree they can be performed).

It is important to be clear about how to measure how well a task can be performed. Performance measures might vary for different tasks but important dimensions often include effectiveness (the extent to which the response actually satisfy the need that correspond to the demand) and efficiency (whether the task can be performed in a timely manner and within reasonable resource limits). Some performance measures might be directly related to the essential variables of the system as a whole while others might have a more indirect relation, depending on the nature of the task. Since the performance measures determine how well a specific task can be performed they need to be possible to derive, given a specific scenario. This means that they cannot be, for example, of the type "how good the release was managed", unless a clear definition of "good" is

provided. Returning to the example above a suitable performance measure related to the task "to stop the release" might be "time from alarm until the release is stopped".

Variation in context, such as conditions in the environment and effects of the hazardous event, will have an affect on how well the tasks can be performed in an emergency situation. Emergency response capabilities are thus context dependent and this must be accounted for in an analysis. In the example above, a description of the context may include, for instance, whether the scene of the accident is accessible by road and whether the actor has access to certain resources. The capabilities that organisations possess during "optimal" conditions might thus be reduced if the context is different.

Given a specific context there might be uncertainties regarding how well a task can be performed. The emergency response capability can thus be seen as a set of triplets, similar to the quantitative definition of risk, corresponding to the three questions:

- "What can happen when an actor is performing a specific task, given a specific context?"
- "How likely is it?"
- "What are the consequences, for the performance measures defined for that particular task?"

An actor can in this case be seen as a part of an organisation, an organisation, or several organisations, thus the definition is flexible regarding the scope. From the scenarios it is possible to extract measures and metrics very much similar to what is done in a quantitative risk analysis, for example curves equivalent to risk curves or expected values. However, the details of how to do this in practice are outside the scope of this paper.

The relation between the definition of emergency response capabilities and the definition of vulnerability, proposed in a previous section is quite straightforward. In a system, for example a geographic region, there might be several actors that possess different emergency response capabilities. The actors and their capabilities will affect the unfolding of the scenarios, i.e. the trajectories in the state space of the system, given that the system is affected by a hazardous event. Thus, the emergency response capabilities will affect the vulnerability of the system as a whole. Some capabilities will certainly have a larger influence on the overall system vulnerability than others, which is important to consider in a comprehensive vulnerability analysis.

Discussion

The use of the definition of emergency response capabilities might be perceived as being demanding, in the sense that it can be time-consuming to carry out a comprehensive analysis. However, the definition should be seen as an ideal operationalisation and be used as a guidance for how a systematic analysis can be structured. The definition acknowledges that there are uncertainties about future events, both regarding the context in which the task are to be performed and regarding how well the task can be performed given a specific context. Furthermore, it should be possible to make judgements about the validity of any statements that are made about capabilities.

We argue that the main purpose of adopting the definition to analyse emergency response capabilities is to introduce a proactive mode of thinking into emergency response organisations. The definition provides an analytic structure that can encourage actors to be systematic when anticipating future events, the demands that are put on them in these events and whether these demands can be met. In the analysis it is possible to identify weaknesses in the emergency response capabilities of actors and alternatives regarding improvements can be suggested. In addition, such an analysis might have the potential of creating a mental awareness of the actors' capabilities and the limits thereof. The limits of the capabilities can then be communicated to other organisations and people and thereby increasing the awareness of the society as a whole. Furthermore, in analysing capabilities the organisations are forced to be concrete about how well the tasks can be performed and to express the capability in measurable quantities.

If the analysis is carried out as a coordinated exercise between many emergency response organisations, there might be additional benefits of analysing emergency response capabilities. First, there is a possibility that adoption of a common perspective on emergencies and a common language can be encouraged. This would for example facilitate communication and cooperation during an emergency and thereby improve the emergency response. By making an analysis of emergency response capabilities into a coordinated exercise between many organisations in a community it is also easier to gain knowledge about the emergency response capabilities of the community as a whole.

In the proposed definition, capabilities are analysed in a concrete manner where tasks are directly related to the actual course of events in the emergency. Another approach could be to analyse higher level abstractions, such as flexibility or capacity to improvise. However, since these are hard to relate to the actual course of events in an emergency it is hard to gain knowledge about the effect these abstractions have on the emergency response and evaluating the validity about statements addressing higher level abstractions might be difficult. In addition, these higher level abstractions are often effects of having a set of concrete capabilities. An example is flexibility, which is often an effect of the ability to perform tasks in different contexts and conditions, for example being able to perform a task even though the regular personnel are disabled. Higher level abstractions can thus often be extracted from the more concrete capabilities.

In analysing emergency response capabilities one will encounter the same problem as one does when applying the quantitative definition of risk, namely choosing an appropriate level of detail in the description of scenarios and context. In theory, there is an infinite set of scenarios and an infinite number of possible contexts, since a description always can be made more detailed. However, very detailed descriptions are often unpractical in real world applications since there is a trade-off between for example the level of detail and the time required to complete the analysis. An important task when analysing emergency response capabilities is therefore to choose an appropriate level of detail. Choosing a too fine level of detail will lead to that too much effort is committed to details that will not affect, or have very limited effect on, the overall analysis. Choosing a too coarse level of detail, on the other hand, could result in that important aspects are overlooked. An example is how to define a task. At the most general level regarding the example with the derailed train, the task might be “to manage the situation”. This could be divided into a number of more detailed tasks, e.g. “stopping the release”, “issue warning” etc., which in turn could be further divided into tasks of even higher level of detail. The level of detail will in turn affect the number and character of the performance measures that are used to capture what is to constitute a well performed task. The level of detail that is ultimately chosen need to depend on the aim of the specific analysis.

There are several areas for further research. Firstly, there is a need to apply the definition of emergency response capabilities in a comprehensive case study with the purpose of testing the applicability of the framework. Choosing an appropriate level of detail in the analysis is one issue that needs to be addressed. Secondly, the problem of synthesis should be addressed. Using the proposed definition capabilities are *analysed*, i.e. the overall emergency response is broken down into separate tasks, but it is sometimes not straightforward how to synthesise these capabilities into an overall assessment of the capabilities of for example a community.

Conclusions

In this paper we have proposed an operational definition of emergency response capabilities that includes three essential elements. The task to which the capability is related, measures of how well that task can be performed and a description of the context affecting the performance of that particular task. The definition makes clear that there are uncertainties about how well a particular task can be performed given a specific context and that this must be taken into account in an analysis. We conclude that the definition provides a framework for analysing emergency response

capabilities which can help actors to gain knowledge about their capabilities and limits thereof. Such an analysis can also serve as a basis for a subsequent evaluation and suggestions for capability improvements.

References

Anderson, M. B. & Woodrow, P. J. (1998). *Rising from the Ashes: Development Strategies in Times of Disaster*. Intermediate Technology Publications, London, United Kingdom.

Ashby, W. R. (1957). *An Introduction to Cybernetics*, Chapman & Hall, London, United Kingdom.

Boin, A. (2004). Lessons from Crisis Research. *Int. Studies Review*, Vol. 6, pp. 165-174. Blackwell Publishing, United States.

Brooks, N. & Adger, W. N., Kelly, P. M. (2005). The determinants of vulnerability and adaptive capacity at the national level and the implications for adaptation. *Global Environmental Change*, Vol. 15, pp. 151-163. Elsevier Ltd., United Kingdom.

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

Cannon, T., Twigg, J., & Rowell, J. (2003). Social Vulnerability, Sustainable Livelihoods and Disasters. *Report to DFID Conflict and Humanitarian Assistance Department (CHAD) and Sustainable Livelihoods Support Office*. Department for International Development. London, United Kingdom.

Coles, E. & Buckle, P. (2004). Developing community resilience as a foundation for effective disaster recovery. *The Australian J. of Emergency Management*, Vol. 19, No. 4, pp. 6-15. Emergency Management Australia, Australia.

Cutter, S., Boruff, B. J., Shirely, W. L. (2003). Social Vulnerability to Environmental Hazards, *Social Science Quarterly*, Vol. 84, No. 2, pp. 242-261. Blackwell Publishing, United States.

Cutter, S., Mitchell, J. T. & Scott, M. S. (2000). Revealing the Vulnerability of People and Places: A Case Study of Georgetown County, South Carolina. *Annals of the Association of American Geographers*, Vol. 90, No. 4, pp. 713-737. Blackwell Publishing, United States.

Dilley, M. & Boudreau, T. E. (2001). Coming to terms with vulnerability: a critique of the food security definition. *Food Policy*, Vol. 26, pp. 229-247. Pergamon, United Kingdom.

Dynes, R. R. (1994). Community Emergency Planning: False Assumptions and Inappropriate Analogies. *Int. J. of Mass Emergencies and Disasters*, Vol. 12, No. 2, pp. 141-158. International Research Committee on Disasters, United States.

Einarsson, S. & Rausand, M. (1998). An Approach to Vulnerability Analysis of Complex Industrial Systems. *Risk Analysis*, Vol. 18, No. 5, pp. 535-546. Plenum Press, United States..

Fischhoff, B., Watson, S. R. & Hope, C. (1984). Defining Risk. *Policy Sciences*, Vol. 17, pp. 123-139. Elsevier Science Publishers, the Netherlands.

Gundel, S. (2005). Towards a New Typology of Crises. *J. of Contingencies and Crises Management*, Vol. 13, No. 3, pp. 106-115. Blackwell Publishing, United Kingdom.

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

IFRC (1999). *Vulnerability and capacity assessment: An International Federation Guide*. International Federation of Red Cross and Red Crescent Societies. Geneva, Switzerland.

Kaplan, S. (1997). The Words of Risk Analysis. *Risk Analysis*, Vol. 17, No. 4, pp. 407-417. Plenum Press, United States.

Kaplan, S. & Garrick, B. J. (1981). On The Quantitative Definition of Risk. *Risk Analysis*, Vol. 1, No. 1, pp. 11-27. Plenum Press, United States.

Kaplan, S., Haimes, Y. Y., & Garrick, B. J. (2001). Fitting hierarchical holographic modeling into the theory of scenario structuring and a resulting refinement to the quantitative definition of risk. *Risk Analysis*, Vol. 21, No. 5, pp. 807-819. Blackwell Publishing, United States.

Kuban, R. & MacKenzie-Carey, H. (2001*). Community-Wide Vulnerability and Capacity Assessment*. Office of Critical Infrastructure Protection and Emergency Preparedness. Ottawa, Canada.
McEntire, D. A. (2001). Triggering agents, vulnerabilities and disaster reduction: towards a holistic paradigm. *Disaster Prevention and Management*, Vol. 10, No. 3, pp. 189-196. Emerald Group Publishing Ltd., United Kingdom.
McEntire, D. A. (2005). Why vulnerability matters - Exploring the merit of an inclusive disaster reduction concept. *Disaster Prevention and Management*, Vol. 14, No. 2, pp. 206-222. Emerald Group Publishing Ltd., United Kingdom.
Perry, R. W. & Lindell, M. K. (2003). Preparedness for Emergency Response: Guidelines for the Emergency Planning Process. *Disasters*, Vol. 27, No. 4, pp. 336-350. Blackwell Publishing, United Kingdom.
Renn, O. (1998). Three decades of risk research: accomplishments and new challanges. *J. of Risk Research*, Vol. 1, No. 1, pp. 49-71. Routledge, United Kingdom.
Salter, J. (1997). Risk Management in a Disaster Management Context. *J. of Contingencies and Crises Management*, Vol 5. No. 1, pp. 60-65. Blackwell Publishing, United Kingdom.
Sarewitz, D., Pielke Jr., R. & Keykhah, M. (2003). Vulnerability and Risk: Some Thoughts from a Political and Policy Perspective. *Risk Analysis*, Vol. 23, No. 4, pp. 805-810. Blackwell Publishing, United States.
UNDP (1998). Capacity Assessment and Development - In a Systems and Strategic Management Context, United Nations Development Programme. New York, United States.
Weichselgartner, J. (2001). Disaster mitigation: the concept of vulnerability revisited. *Disaster Prevention and Management*, Vol. 10, No. 2, pp. 85-94. Emerald Group Publishing Ltd., United Kingdom.
Wisner, B., Blaikie, P., Cannon, T, & Davies, I. (2004). *At Risk. Natural hazards, people's vulnerability and disasters*, Routledge, London, United Kingdom.

Acknowledgements

This work is part of the Framework Programme for Risk and Vulnerability Analysis (FRIVA) at Lund University Centre for Risk Analysis and Management (LUCRAM) financed by the Swedish Emergency Management Agency (SEMA).

Author Biographies

Henrik Jönsson is a PhD student at the Department of Fire Safety Engineering and has a M.Sc. in Risk Management and Safety Engineering and a B.Sc. in Fire Safety Engineering. His main research area is risk and vulnerability analysis of complex social and technical systems.

Marcus Abrahamsson is a PhD student at the Department of Fire Safety Engineering at Lund University and holds a Licentiate degree in Fire Safety Engineering. His main research areas are risk and vulnerability analysis of social and technical systems and treatment of uncertainties in quantitative risk analysis.

Henrik Johansson is an assistant professor at the Department of Fire Safety Engineering at Lund University and has a Ph.D. in Fire Safety Engineering and a M.Sc. in Civil Engineering. His main research areas are vulnerability analysis of social and technical systems and decision analysis concerning investments in risk reducing measures.

Evaluating the Seriousness of Disasters: Implications for Societal Decision Making

ABSTRACT

In making societal decisions concerning hazards with potentially disastrous consequences it is important to have soundly based knowledge, not only of the factual characteristics of the possible scenarios, but also of how people evaluate the seriousness of disasters. In the present study a group of students evaluated the seriousness of disasters described in terms of four basic attributes: *number of fatalities*, *number of serious injuries*, *economic loss*, and *cause of the disaster*. Attribute weights were elicited by two separate methods adapted from comparable methods, one direct and the other indirect, developed within decision and judgment analysis. Use of these two methods together provides insight into the stability and the uncertainty of the weights elicited, matters important in connection with societal decision making in this area. Most participants regarded attributes related to physical harm, especially the *number of fatalities*, to be most important. The cause of a disaster also affected many of the participants' judgments of its seriousness. This suggests that not only teleological but also deontological considerations may be relevant to normative decisions of this sort. Although the participants cannot be regarded as representative of the public in general, the findings are of value to societal decision making concerning hazards with possible disastrous consequences, particularly in the case of projects of small to medium size in which specific elicitations of the values involved for the populations potentially affected are rarely made.

KEYWORDS

Scenario evaluation, disaster seriousness, value elicitation, preferences

1. INTRODUCTION

In efforts to reduce the risks of disasters, 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, mitigate its effects or to prepare for it, as well as what risks and hazards efforts of this sort should be focused on. For such decisions, it is highly important to be able to evaluate effectively the seriousness of potential disaster scenarios differing in the consequences they involve.

The process of making such decisions consists of a factually oriented and a value-oriented part (von Winterfeldt, 1992; Keeney, 1994). The factual part involves identifying the possible outcomes of different action alternatives and estimating for each such outcome the probability of its occurrence. The accuracy of these estimates depends on the validity of the factual knowledge taken account of. For societal decision making of this sort to be fully rational the best knowledge available should be made use of (Webler *et al.*, 1995; Cooksey, 1996), therefore it is highly desirable to use science and experts as "the providers of facts" (DeKay & McClelland, 1996).

A thorough understanding of the value aspects of a decision is also essential since values determine what are regarded as positive or negative consequences, a matter emphasized by Keeney who points out that "values are what we care about" (Keeney, 1992) and that they are "essential for guiding decisionmaking" (Keeney, 1994).

Rational societal decision making require that one takes account of the values and preferences of the members of society potentially affected by a decision. The public should be treated in this respect as "value consultants" (Webler *et al.*, 1995). Having soundly based knowledge of people's values is of importance for decisions in risk and disaster management as well as having adequate knowledge of the facts. However, the values connected with these decisions often appear to not be dealt with comprehensively enough or to not be made explicit. This reduces the transparency and the quality of decisions. There is thus a need of more thorough knowledge of the values involved. The value and preference elicitation procedures developed within decision analysis (von Winterfeldt & Edwards, 1986) and judgment analysis (Cooksey, 1996) can be useful for obtaining such knowledge.

The theory of the nature of preferences has been modified considerably in recent decades. According to classical theory, preferences are well-defined (Tversky *et al.*, 1988), the goal of an elicitation process being to measure "true" preferences. Yet, research has shown that classical theory is often lacking in validity, particularly in contexts unfamiliar to the subject (Slovic, 1995). Rather, preferences are seen as being constructed when they are needed (Payne *et al.*, 1992; Fischer *et al.*, 1999). Instead of trying to measure a person's "true" preferences, the elicitation process should thus ensure that preferences are constructed in a proper way. As Slovic (1995) indicates, "Truth ultimately resides in the process, rather than in the outcome".

Many procedures for eliciting people's preferences have been proposed, see Borcherding *et al.* (1991) and Weber and Borcherding (1993) for example, 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 judgments and decisions (Tversky & Kahneman, 1981; Hershey *et al.*, 1982; Weber & Borcherding, 1993; von Nitzsch & Weber, 1993; Fischer, 1995; Baron, 1997a). No procedure is free of bias and it is also unclear which procedure is least biased (Weber & Borcherding, 1993). Procedures may differ primarily simply in the biases they trigger, and accordingly in the preferences they yield (Pitz & Sachs, 1984). Nevertheless, being aware of how the biases called forth by different procedures may distort the preferences that are elicited can be seen as a first step towards designing elicitation processes able to elicit valid preferences. A recommendation commonly made is to use more than one procedure for eliciting preferences (Payne *et al.*, 1999). This can cast light on the uncertainty as well as stability of the preferences obtained and clarify how the preferences are constructed.

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 trade-offs that people are willing to make between low-probability scenarios in which there are many fatalities and scenarios of higher probability in which there are fewer fatalities, and guidelines for such trade-offs have previously been carried out (e.g. Keeney, 1980; Slovic *et al.*, 1984; Hubert *et al.*, 1991; Abrahamsson & 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). Of the studies just referred to it is only that of Christen *et al.* (1994) in which any systematic elicitation of values was performed to determine trade-offs 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 Disaster Database[1], makes use of only a

few attributes, such as the number of fatalities, the number of injuries, the economic loss and what the main cause of the disaster was. Regarding cause, there is psychological research which "has shown that the causes of harms do affect values" (Kahneman and Ritov 1994). In line with this, negative environmental consequences have been shown to be perceived as being more serious when humans are to blame for them than when they are caused by natural events (Kahneman & Ritov, 1994; Walker *et al.*, 1999; Brown *et al.*, 2002; Brown *et al.*, 2005; Bulte *et al.*, 2005). Explanations for this that have been suggested include outrage effects, i.e. the emotional upset induced by knowing that humans are to blame (Kahneman & 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 to not 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 judgments of the seriousness of a disaster that give rise to fatalities and injuries are affected by the apparent cause of the disaster.

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 characterized 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 the value aspects of risks are often investigated in an integrated way, in the sense of people's perception of risks being 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 more clear distinction between facts and values. Florig *et al.* (2001), for example, have proposed a method for eliciting people's risk preferences in which the levels of the attributes considered are derived from risk assessments that are based on scientific literature and from judgments of experts. Risk summaries are presented to persons who perform rankings of the risks involved, 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. Whereas in that approach, however, judgments under conditions of uncertainty are involved, since risk rankings are made without knowledge of which one of the various risk scenarios that are possible will occur, in the present study judgments under conditions of certainty are involved. This since our concern is in assessing, for a particular risk scenario or any of a variety of possible risk scenarios of interest, how negative its occurrence would be, i.e. the seriousness of the risk scenario in question, given that it occurs. Note in this connection that risk assessment in its entirety involves consideration of the complete set of risk scenarios that are possible, for each the probability that it will occur and the negative consequences its occurrence would have, and aggregating these assessments over the risk scenarios as a whole (Kaplan & 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 attributes employed are *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 one indirect and holistic method and the other a direct method involving judgements of the relative importance of attributes. This makes it possible to study the convergent validity of the two methods and to gain insight into the respective advantages and disadvantages of the two.

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 participated in the study. All of them were taking courses at the Department of Fire Safety Engineering at 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. Emphasizing this was seen as increasing the students' readiness to take the tasks seriously. Altogether, participation was voluntary. 81 persons (22 females and 59 males) between the ages of 18 and 45 (mean of about 23) took part. Three separate testing sessions took place during a period of a year. Two of them involved first-year students and the third involved third-year students.

2.2. Materials

The questions and tasks presented could be completed by use of a computer interface involving software the authors developed specifically for this purpose. Participants were given extensive instructions and support with the aim of ensuring the quality and validity of their responses. The instructions given 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

Since it may not be possible to determine a priori what method provides the most valid weights in a given context, using more than one method can be a very sensible approach to gaining insight into people's preferences here, and into the validity and stability of the attribute weights obtained. To this end, two fundamentally different methods, one indirect and one direct, were used 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 judgments regarding the scenarios of interest, 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 judgments of the relative importance of the different attributes.

These two methods differ in their advantages and their drawbacks. First, the indirect method is more time-consuming and is often perceived as being more difficult. Secondly, deriving preferences statistically as is done in the indirect method enables one to gain insight into the consistency of the judgments made (indicating how adequate a picture the model provides of the participants' judgment), the cross-validity of the results obtained (how well the model generalizes) 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 & Weber, 1993; Fischer, 1995), for example, whereas the indirect method is more prone to prominence effects (Fischer *et al.*, 1999).

Since a major aim of the study was to elicit preferences that could be used as input to societal decision making in this area, it was important that the effects of known biases and heuristics were limited as much as possible. One example of such an effort was to restrict the number of attributes employed 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 judgments, taking all of the attributes into account simultaneously, it was deemed likely that using too many attributes would trigger participants into using heuristics so as to simplify their judgments, for example through ignoring less salient though relevant attributes (Green & Srinivasan, 1978; Fischer, 1979; Weber & Borcherding, 1993).

2.4. Design of the Study

The study was so designed that the individual subject was treated as the unit of analysis. The attributes used to characterise each disaster scenario and its consequences were *number of fatalities*, *number of serious injuries*, *economic loss* and *the cause of the disaster*. The definitions of these attributes are given in Table I and the ranges of each is contained in Table II. 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 to serve as reference points were presented to the participants, such as the economic losses incurred by a hurricane that occurred in Sweden recently.

Each participant was tested in a single session, which consisted of five major steps. Testing was mainly in groups. In step 1, participants were asked to provide personal details, such as name[2], age and gender. Steps 2 and 3 involved use of the indirect method and step 4 use of the direct method. Employing the indirect method first had the advantage that, since there participants have to consider the attribute ranges rather explicitly, the awareness of range that this creates tends to reduce the range insensitivity bias characteristic of the direct method. In step 5 the participants were to fill out a short questionnaire concerned with how they perceived the study, how they arrived at their judgments, and the like. The parts of the session prior to completing the questionnaire, typically took about 30 minutes to complete.

Table I. 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 for the Swedish population generally.
Number of serious injuries	The number of persons requiring acute medical treatment because of the disaster, in many cases followed by long periods of recuperation and possibly lifelong impairment. The types of persons involved can also be seen as representative for the Swedish population generally.
Economic loss	The economic loss here is expressed in billions of Swedish Kronor. It includes loss of value in terms of property, equipment, infrastructure, crops and the like, together with indirect losses 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 II. The levels and categories of the four different attributes employed.

	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	0	4	20	40
Cause of the disaster	Accidental	Terrorism	Natural	-

2.4.1. Indirect Method

In the indirect method, participants made holistic judgments of the seriousness of 24 hypothetical disaster scenarios, described only in terms of the four attributes shown in Table I. The scenarios were designed using a fractional factorial design in which the attributes could take on levels and categories in accordance with Table II. The levels and categories were combined orthogonally in order to minimise the correlations between the attributes, since this provides the most straightforward and statistically stable estimates of the regression coefficients (Cooksey, 1996; Karren & Woodard Barringer, 2002). The scenarios were also so constructed as to avoid dominant scenarios, i.e. scenarios having lower (more undesirable) level on all the attributes as compared with the other scenarios involved.

Research has shown that comparative rather than absolute judgments are perceived to be easier to make and that they result in greater consistency (Brown *et al.*, 2002). This applies especially to judgments of seriousness of a disaster, since it is difficult there to construct an absolute scale that the judgments can be related to. So that comparative judgments could be made, the indirect method was divided into two separate steps. In the first step, scenarios were

presented in pairs and 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). Then, participants had the opportunity of adjusting 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, 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, in order to maintain agreement with their previously expressed choices. Although it was possible for participants to assign scores that deviated from the rank-ordering they had created earlier, they were informed when such deviation occurred.

In order to reduce the occurrence of any systematic biases in the order in which the attributes were presented, a *between*-participant randomization of this was carried out. The reason for not changing the order of presentation of the attributes throughout elicitation for each of the participant individually 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 direct method that was employed was similar to the "Max100"-procedure discussed by Bottomley and Doyle (2001). The four attributes and the ranges of possible outcomes that each attribute could take were presented to participants in a randomly ordered list. Participants were asked to assign an "importance score" of 100 to the attribute that was the most important one for them in making judgments 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. Participants were instructed that in making judgments of the importance of an attribute, they should take account of the range of each of the attributes, an example also being presented to illustrate the importance of this.

2.5. Analysis of the Data

2.5.1. Judged Seriousness and Value Functions

For each participant, any judgment 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 is a specific disaster scenario, w_i is the relative weight of attribute i (the relative weights of the different attributes being normalized to sum to 1), v_i is the single-attribute value function for attribute i (normalized to range from 0 to 1), and x_{ij} is 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.

Value functions for single attributes, v_i, were not elicited separately, as often is done in a multi-attribute context. Instead they were simply assumed or were derived from the participant's holistic judgments 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 being a larger number of fatalities and of serious

injuries and larger economic losses (everything else being equal) implies the scenario being more serious. Accordingly, the single-attribute value functions were assumed to be consistent with equation 2.

$$v_i(x_i) = \left(\frac{\left(x_i - x_{i,\min}\right)}{\left(x_{i,\max} - x_{i,\min}\right)} \right)^{z_i}, \quad (2)$$

where x_i is the level or category of attribute i, $v_i(x_i)$ is the value of the i:th attribute at level x_i, $x_{i,\min}$ and $x_{i,\max}$, respectively, are the minimum and the maximum level of attribute i, and z_i is a parameter larger than 0 describing the shape of the single attribute value function, and where z_i = 1 implies constant marginal values, $z_i > 1$ increasing marginal values, and $0<z_i< 1$ diminishing marginal values.

Converting the categorical attribute *cause of the disaster* into a value function involved applying multiple regression analysis to the participants' holistic judgments 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 the natural cause as the baseline category, using one dummy then to code for terrorism (1 if terrorism was the cause and otherwise 0) and another dummy to code for an accident (1 if accident was the cause and otherwise 0). Regression coefficients 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 use of equation 3,

$$v_c = \frac{b_c - b_{c,\min}}{b_{c,\max} - b_{c,\min}}, \quad (3)$$

where v_c is the "value" of category c, b_c is the estimated regression coefficient of the dummy that coded category c (if a natural event was the cause, b_c was set to 0), and $b_{c,\min}$ and $b_{c,\max}$ are the minimum and maximum, respectively, 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,

$$Score_j = \beta_0 + \sum_{i=1}^{4} \beta_i \cdot v_{ij} + \varepsilon_j, \quad (4)$$

where $Score_j$ is a participant's "seriousness score" for scenario j, β_0 is the y-intercept[3], β_i is the regression coefficient for attribute i, v_{ij} is the value of attribute i in scenario j, and ε_j is the error term for scenario j. In the regression analysis, two assumptions regarding the 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 in order to find the transformation that provided the best fit to the judgments 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 125 transformations being tested for each participant and the goodness-of-fit of these transformations being evaluated using the adjusted R^2 (Kutner *et al.*, 2004) as the criterion. Only the transformation with the highest adjusted R^2 was considered further. In order to obtain the relative weights (w_i in eguation 1) of the four attributes, the estimated regression coefficients, b_i, obtained from the regression analyses were normalized 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 in using the direct method was straightforward. The weights were simply obtained by normalizing 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 in this way, based on assessments made for each of the participants separately, are shown in Table III. As can be seen, for more than half of the participants Terrorism was the cause considered to have 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: 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 the average, higher seriousness scores than Natural Cause; though the difference is not statistically significant, $t(160) = 1.29$, $p = 0.20$.

Table III. Values for the three categories of the attribute *cause of the disaster*.

$Cause_c$	Percentage of participants involved			
	$v_c=1$	$0<v_c<1$	$v_c=0$	$\overline{v_c}$
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 use of the Indirect Method

In the indirect method, the attributes were regressed on the seriousness scores for each participant separately, 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' judgments 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, cross-validation by use of the "leave-one-out" (or jack-knifing) procedure (Cooksey, 1996)[4] were conducted to determine how well the models describe the participants' preferences for scenarios not included in the sample, but still within the range of the attributes.

3.2.1. Constant Marginal Values for the Quantitative Attributes

In Fig. 1, distributions of the coefficient of multiple determination, R^2, and the cross-validated coefficient of multiple determination, R^2_{CV}, are presented for the participants as a whole, assuming constant marginal values for the quantitative attributes. The figure shows that for most of the participants the R^2 values are fairly high, ¾ of the participants having an R^2 larger than 0.8. Results for a few of them with R^2 values of between 0.5 and 0.6 can be considered as outliers. The R^2_{CV} values are somewhat lower, of course, but still fairly high, ¾ 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 IV, 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 normalized to a range of 0 to 1. The average of the estimated regression coefficients can be interpreted, therefore, as the average impact that a specific attribute has on the seriousness score when the attribute is changed 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 a an effect on the seriousness scores of the 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 the disaster*, $t(160)=1.11$, $p=0.27$.

Table IV. Estimated regression coefficients averaged over the participants as a whole and the percentage of participants whose coefficients are statistically significant at the levels indicated, assuming constant marginal values.

Attribute, i	$\overline{b_i}$	Percentage of the participants for which the estimated regression coefficients, b_i, are significant at the level indicated			
		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 the disaster	9.8	34.6	29.6	18.5	14.8

In Fig. 2, 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 the disaster* has the smallest.

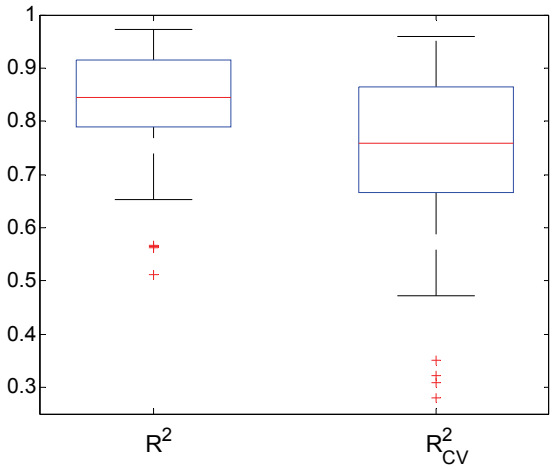


Fig. 1. Distributions of R^2 and R^2_{CV} for the participants as a whole, assuming constant marginal values

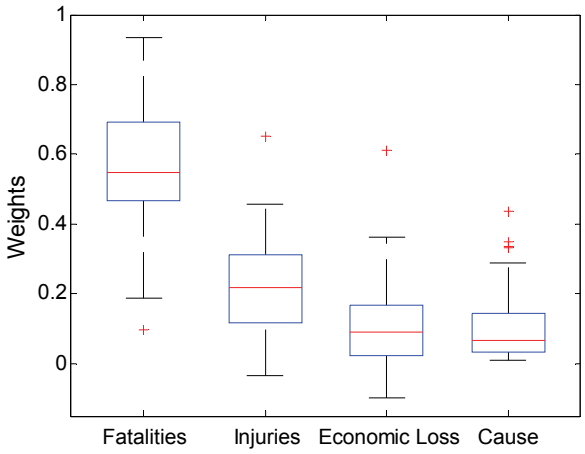


Fig. 2. Distributions of the relative weights obtained using the indirect method for the participants as a whole, assuming constant marginal values

Presenting relative weights as an indicator of attribute importance has the drawback of its being dependent on the range of the respective attributes. Attribute importance need to be interpreted in light of the ranges involved. In order to facilitate the interpretation of attribute importance, the "rates of substitution" between attributes were calculated, such as the number of serious injuries "needed" to match the adjudged seriousness of a single fatality. The median[5] of the substitution rates when assuming constant marginal values is that of one fatality being equivalent in seriousness to 9.9 serious injuries having occurred (as the attribute is defined in Table I) as well as to 144 million Swedish Kronor (about $20 million).

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. Distributions of the R^2 and R^2_{CV} values of the participants are shown in Fig. 3. Both coefficients increased considerably when the assumption of constant marginal values was relaxed, suggesting that use of these transformed value functions improved the regression models. There were still several 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. 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 use of the transformed value functions.

The transformations involving the z-values contained in equation 2 that provided the best possible fits are shown in Table V. Only z-values pertaining to 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 judgments of seriousness, which a non-significant 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 both of *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 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 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.

Table V. Best fitted transformations of the quantitative attributes for participants as a whole.

	Percentages of the participants, for whom the marginal values of the best transformations possible were as follows:				
Attributes	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

[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 VI. The distribution of the relative weights for all participants is presented in Fig. 4. 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 *number of serious injuries*, where the estimated regression coefficient now is statistically significant at the 0.05-level for over 95% of the participants (in comparison to only about 65% when assuming constant marginal values).

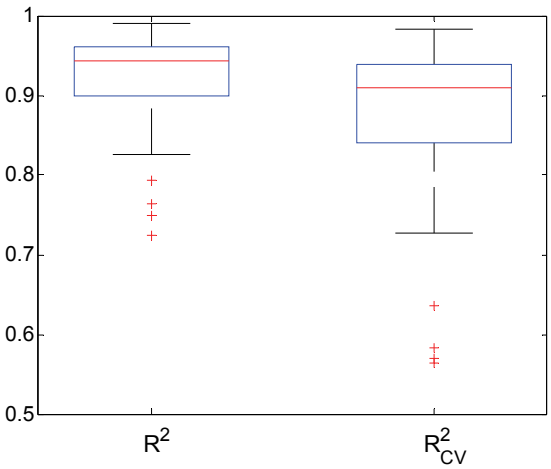


Fig. 3. Distribution of R^2 and R^2_{CV} obtained for the participants with use of transformed value functions.

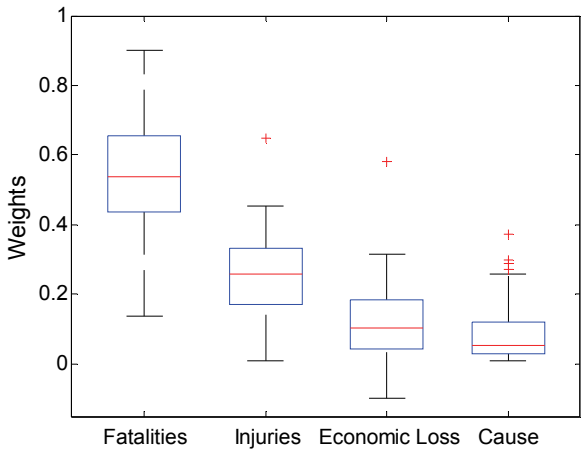


Fig. 4. Relative weights based on transformed value functions using the indirect method.

Table VI. Estimated regression coefficients averaged over the participants as a whole and the percentages of the participants whose coefficients were statistically significant at the levels referred to, using transformed value functions.

Attribute, i	$\overline{b_i}$	Percentage of the participants for whom the estimated regression coefficients, b_i, were significant the p-level			
		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 the disaster	9.7	48.1	38.3	29.6	22.2

3.3. Participants' Preferences Obtained by use of the Direct Method

The distributions of relative weights obtained by use of the direct method for the participants as a whole are presented in Fig. 5. As can be seen there, *number of fatalities* was regarded in general as the most important attribute, followed by *number of serious injuries*, there being more than 90% of the participants who judged *number of fatalities* to be the most important attribute. The least important attribute, for most participants appears to be either *economic loss* or *cause of the disaster*. The relative weight for *cause of the disaster* appears to vary across participants more than the other attributes do, which is the opposite of what was found using the indirect method.

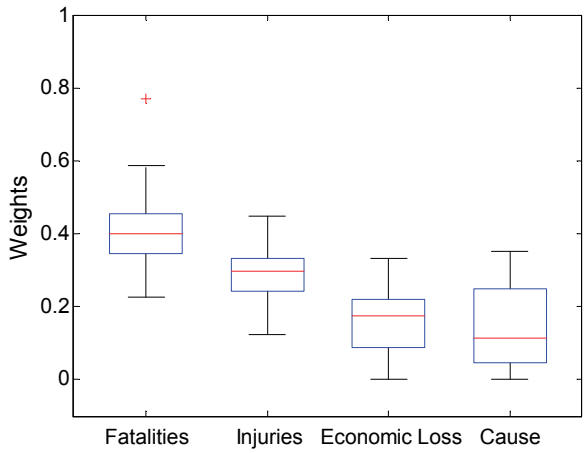


Fig. 5. Distributions of relative weights obtained using the direct method.

The rate of substitution can also be calculated from the relative weights obtained by use of the direct method. When constant marginal values are assumed, the rate of substitution is such that one fatality is equivalent to 5 serious injuries (as the attribute is defined in Table I) and to 100 million Swedish Kronor (about $14 million).

3.4. Comparison of the two Different Methods

The relative weights the two different methods provide are summarized in Table VII. As can be seen, on the average both methods provide the same rank-ordering of the relative importance

of the four attributes. The main difference between the two methods is that the distribution of weights the direct method provides is flatter, the difference between the largest and the smallest weight there being less. This difference can be clearly seen in Table VII or by comparing either Fig. 2 or Fig. 4 with Fig. 5. The difference obtained in comparing the average difference between the largest and smallest weight that the indirect method provides (with use of transformed value functions) and that provided by use of the direct method is also statistically significant, $t(160)=6.81$, $p<0.001$. Similar findings have been obtained in other studies in comparing methods requiring holistic judgment and those requiring direct judgments of attribute importance (Weber & Borcherding, 1993). The overall conclusion that can be drawn is that methods that require holistic judgments lead to greater attention being directed at the most prominent attributes (*number of fatalities* in the present case), whereas methods involving direct elicitation of weights lead to the weights being distributed more evenly.

Table VII. Summary of the average relative weights obtained with use of the two different methods.

	Indirect method		Direct method
	Constant Values	Transformed Values	
Number of fatalities	0.549	0.537	0.400
Number of serious injuries	0.217	0.257	0.296
Economic loss	0.089	0.105	0.174
Cause of the disaster	0.068	0.055	0.114

The two methods can also be compared by calculating the judged seriousness (equation 1) of different disaster scenarios using the relative weights the two methods provide and then correlating the respective scores obtained, checking the convergent validity of the two methods in this way. 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 the 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 results of these calculations are presented in Table VIII. As can be seen, the correlations between the two methods are quite high generally, suggesting the two methods to be quite consistent with each other. This in turn supports the validity of the weights obtained in the study and of the judged seriousness that these weights imply.

Table VIII. Distribution of the correlations calculated for each participant separately, between the judged seriousness measures the two methods provided.

Percentiles				
5	25	50	75	95
0.828	0.870	0.892	0.918	0.942

4. DISCUSSION

Although it was found, as expected, that attributes related to physical harm (especially *number of fatalities*) were regarded as being the most important, it was also shown that the cause of a disaster can affect judgments of its seriousness. This raises questions in connection with the

use of utility theory as a normative basis for decisions, often being applied in the sense of teleological decision rules, i.e. that decisions should depend only on the consequences of decision alternatives available. 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 an important factor in assessing the seriousness of the disaster, implying them to use deontological decision rules as well. In addition, in the questionnaire given at the end of the session, many of the subjects stated that they incorporated considerations other than the undesirability of the consequences alone into their judgments of the seriousness of a disaster. These additional considerations included the following:

- the low degree of preventability that natural events were seen as having led to their being perceived as less serious,
- the high degree of acceptance that unpreventable events were seen as having led to their being perceived as less serious,
- the malicious intent characterizing terrorist attacks led to their being perceived as more serious,
- questions about who to blame, more prominent in connection with intentional and accidental events, led to such events being perceived as more serious, and
- the fear that successful terrorist attacks would encourage future attacks made such events appear more serious.

The basic findings obtained here are supported by previous research, in which it has likewise been found that people often use deontological rules in making judgments. 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 & 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).

Although, from a descriptive point of view it is thus clear that people often have deontological concerns when making judgments of the seriousness of a disaster, whether such considerations should be used in a normative or prescriptive way in decision making is less obvious. The matter is complicated by the facts that some of these considerations concern not only people's *values* but also their preconceived notions concerning *facts*. For example, many participants here appeared to assume that natural disastrous events and their consequences were impossible or at least very difficult to prevent, which led to their being perceived as less serious. Although these preconceived notions may have some validity, it is clearly not the case that all natural events and their consequences are impossible to prevent or mitigate. Thus, scenario evaluations based on these preconceived notions can be misleading. Such problems have to do with the difficulties of disentangling facts from values in making value judgments. Factual inferences may "contaminate" values that are being assessed. In using elicited values as prescriptive inputs to decision making it is thus highly important to consider whether these values may inadvertently have been contaminated by erroneous judgments of what is factually correct. Further research concerning the extent to which the cause of a disaster affects its perceived seriousness due to erroneous inferences rather than to "valid" deontological concerns is needed.

For most participants, the single-attribute value functions for the best transformations both for *number of fatalities* and *number of injuries* that were obtained 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 attribute *number of fatalities*, Abrahamsson and Johansson (2006) obtained *utility* functions that were marginally diminishing, indicating the subjects to have shown risk-prone attitudes. Keeney (1980) argues 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 argues for is more an effect of people's strength of preference for different levels of the attribute *number of fatalities* than their attitudes towards risk taking per se. People's relative risk attitude, as defined by Dyer and Sarin (1982)[6], towards *number of fatalities* might then actually be neutral or even averse.

A question that arises in relation to the previous paragraph whether marginally diminishing value functions are appropriate to use in evaluating the attributes *number of fatalities* and *number of injuries* in societal decision making. What complicates matters and makes straightforward application of the value functions that are elicited difficult is the phenomenon of "diminishing sensitivity" (also termed to as 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 often seeming 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 49000 and 50000 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 less and less impact on the seriousness of a disaster as the number of fatalities increases, since this means an additional fatality constituting a smaller and smaller proportional difference. The problems connected with using the value functions elicited as prescriptive inputs to decision making have to do with these possibly being effects of human cognitive biases rather than their being a representation of the underlying values. Further research is needed to obtain a better understanding of the effects of diminishing sensitivity on people's judgments of the seriousness of a disaster.

It is of interest to compare the economic valuation of lives implicit in our study with the values of statistical lives (VSL) that have been derived in studies of people's willingness to pay (WTP) for risk reductions, and the value of a life used by various regulatory agencies. Viscusi and Aldy (2003) conducted an extensive review of studies aimed at estimating VSL, finding American studies to typically indicate the median VSL to lie in the range of $4 million to $9 million, although large individual variations were evident. Values obtained in similar studies in other developed countries, and values used by US regulatory agencies, appeared to be in the same order of magnitude.

In the present study, we found trade-offs between economic losses and human lives that corresponded in most cases to larger values than those reported above (a median of $20 million for the indirect method and $14 million for the direct method). However, the methods used to derive these values are fundamentally different than those used for deriving WTP values. The trade-offs with which our study dealt were between monetary values and *number of fatalities*.

Participants were given no information regarding who would have been affected by the disaster. In WTP, on the other hand, the trade-offs of concern are between monetary values and *risk reduction*, under the assumed condition that it is the subject's own finances and exposure to risk that are affected by his/her actions. The differences found between the two methods in terms of the monetary value of a life arrived at are not surprising since a direct trade-off between monetary values and physical harm is more likely to give a larger weight to life and health. To explain this phenomenon, a parallel can be drawn to what can be referred to as the "Identifiable Victim Effect" (Keeney, 1995; Jenni & Loewenstein, 1997), where the willingness to pay for saving an identified victim, for example a person that has fallen down a well shaft, is greater than the willingness to pay for saving a statistical victim, such as allocating money to a prevention program concerned with reducing the risk of cancer. Although the victims in our study are not identified in the same sense as a person trapped inside a well shaft is, the trade-offs concern number of "fatalities for certain" as compared with fatalities that can be statistically expected, which is the case in the WTP studies referred to above.

Using more than one method to elicit attribute weights is a way of checking the validity and stability of the weights obtained. The difference in the distribution of the attribute weights obtained by use of the two methods is similar to previous findings. Baron (1997a) has argued that "typically, weights derived from holistic judgments are more variable across attributes than those derived from direct comparisons [of attributes]". This was the case in our study as well. Weber and Borcherding (1993) argue that the reason for this is that, since holistic judgments focus on alternatives and scenarios as a whole which are characterised by multiple attributes, the subjects tend to reduce complexity of the judgments by concentrating overly on the most salient attributes, which leads to unduly steep distribution of weights. They also argue that when direct weights are elicited, 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. The two sets of weights, obtained from the two methods, can also be seen as indicating the degree of uncertainty present in the value judgments arrived at. Explicitly modelling this uncertainty in making decisions enables adequate conclusions to be drawn regarding the effect of these uncertainties on the decision made.

In further comparing the two methods, the indirect method was found to be more time-consuming and was also perceived as being more difficult. However, use of 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 participant's responses, enabling participants who give highly inconsistent responses to be identified and the reasons for such inconsistency to be sought. Participants can then be screened out for further analysis if their inconsistencies are believed to stem from their being unfocused in performing the tasks or their not taking the tasks seriously. Secondly, the indirect method provides information concerning the statistical significance of the attributes obtained, 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. We would recommend that in eliciting values one should, if possible, utilize several different methods, since this can enable one to gain deeper insight into people's preferences.

The types of preferences that were elicited here, which aim at being 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 to check the generalisability of the results obtained however, 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 the different types of biases that are to a varying degree inherent in all available techniques. We agree with Payne *et al.* (1992) however, who argue that the alternative of using some kind of intuitive approach or of 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 the best one can to limit biases and to elicit values as accurately as possible. Further studies of the basic type carried out here are clearly needed for gaining a better understanding of people's preferences regarding potential disaster scenarios.

ACKNOWLEDGEMENTS

This research is part of the Framework Programme for Risk and Vulnerability Analysis (FRIVA) at Lund University Centre for Risk Analysis and Management (LUCRAM) financed by the Swedish Emergency Management Agency (SEMA). The authors would like in particular to thank Professor Kurt Petersen for his valuable input to the research.

REFERENCES

Abrahamsson, M. & Johansson, H. (2006). Risk Preferences Regarding Multiple Fatalities and Some Implications for Societal Decision Making - An Empirical Study. *Journal of Risk Research*, *9*(7), 703-715.

Aiman-Smith, L., Scullen, S. E., & 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*, *5*(4), 388-414.

Baron, J. (1997a). Biases in the Quantitative Measurement of Values for Public Decisions. *Psychological Bulletin*, *122*(1), 72-88.

Baron, J. (1997b). Confusion of Relative and Absolute Risk in Valuation. *Journal of Risk and Uncertainty*, *14*, 301-309.

Borcherding, K., Eppel, T. & von Winterfeldt, D. (1991). Comparison of Weighting Judgments in Multiattribute Utility Measurement. *Management Science*, *37*(12), 1603-1619.

Bottomley, P. A. & Doyle, J. R. (2001). A comparison of three weight elicitation methods: good better, and the best. *Omega*, *29*, 553-560.

Brown , T. C., Nannini, D., Gorter, R. B., Bell, P. A. & Peterson, G. L. (2002). Judged Seriousness of environmental losses: reliability and cause of loss. *Ecological Economics*, *42*, 479-491.

Brown , T. C., Peterson, G. L., Brodersen, R. M., Ford, V. & Bell, P. A. (2005). The judged seriousness of an environmental loss is a matter of what caused it. *Journal of Environmental Psychology*, *25*, 13-21.

Bulte, E., Gerking, S., List, J. A. & 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*, *49*, 330-342.

Christen, P., Bohnenblust, H., & 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*, *13*(4), 234-238.

Clement, C. F. (1989). The characteristics of risks of major disasters. *Proceedings of the Royal Society of London*, *424*, 439-459.

Cooksey, R. W. (1996). *Judgment analysis: theory, methods, and applications*. San Diego: Academia Press.

DeKay, M. L. & McClelland, G. H. (1996). Probability and Utility Components of Endangered Species Preservation Programs. *Journal of Experimental Psychology: Applied*, *2*(1), 60-83.

Dyer, J. S. & Sarin, R. K. (1982). Relative Risk Aversion. *Management Science*, *28*(8), 875-886.

Fetherstonhaugh, D., Slovic, P., Johnson, S. M. & Friedrich, J. (1997). Insensitivity to the Value of Human Life: A Study of Psychophysical Numbing. *Journal of Risk and Uncertainty*, *14,* 283-300.

Fischer, G. W. (1979). Utility Models for Multiple Objective Decisions: Do They Accurately Represent Human Preferences? *Decision Sciences*, *10*(3), 451-479.

Fischer, G. W. (1995). Range Sensitivity of Attribute Weights in Multiattribute Value Models. *Organizational Behaviour and Human Decision Processes*, *62*(3), 252-266.

Fischer, G. W., Carmon, Z., Ariely, D. & Zimmerman, G. (1999). Goal-Based Construction of Preferences: Task Goals and the Prominence Effect. *Management Science*, *45*(8), 1057-1075.

Fischhoff, B., Slovic, P., Lichtenstein, S., Read, S. & Combs, B. (1978). How Safe is Safe Enough? A Psychometric Study of Attitudes Toward Technological Risk and Benefits. *Policy Sciences*, *9,* 127-152.

Florig, H. K., Morgan, M. G., Morgan, K. M., Jenni, K.E., Fischhoff, B., Fischbeck, P. S., & DeKay, M. L. (2001). A Deliberative Method for Ranking Risks (I): Overview and Test Bed Development. *Risk Analysis*, *21*(5), 913-921.

Green, P. E. & Srinivasan, V. (1978). Conjoint Analysis in Consumer Research: Issues and Outlook. *The Journal of Consumer Research*, *5*(2), 103-123.

Guidi, G., Ludovisi, G. & 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 - Towards a safer world, Torino, Italy, September 16-20, 2001, European Safety & Reliability Association.

Hershey, J. C., Kunreuther, H. C. & Schoemaker, P. J. H. (1982). Sources of Bias in Assessment Procedures for Utility Functions. *Management Science*, *28*(8), 936-954.

Hubert, P., Barny, M. H. & Moatti, J. P. (1991). Elicitation of Decision-Makers' Preferences for Management of Major Hazards. *Risk Analysis*, *11*(2), 199-206.

Jenni, K. E. & Loewenstein, G. (1997). Explaining the ”Identifiable Victim Effect”. *Journal of Risk and Uncertainty*, *14*, 235-257.

Kahneman, D. & Ritov, I. (1994). Determinants of Stated Willingness to Pay for Public Goods: A Study of the Headline Method. *Journal of Risk and Uncertainty*, *9*, 5-38.

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

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

Karren, R. J. & Woodard Barringer, M. (2002). A Review and Analysis of the Policy-Capturing Methodology in Organizational Research: Guidelines for Research and Practice. *Organizational Research Methods*, *5*(4), 337-361.
Keeney, R. L. (1980). Evaluating Alternatives Involving Potential Fatalities. *Operations Research*, *28*(1), 188-205.
Keeney, R. L. (1992). *Value-Focused Thinking, a Path to Creative Decisionmaking*. Cambrigde: Harvard University Press.
Keeney, R. L. (1994). Using Values in Operations Research. *Operations Research*, *42*(5), 793-813.
Keeney, R. L. (1995). Understanding Life-Threatening Risks. *Risk Analysis*, *15*(6), 627-637.
Keller, A. Z., Meniconi, M., Al-Shammari, I. & Cassidy, K. (1997). Analysis of fatality, injury, evacuation and cost data using the Bradford Disaster Scale. *Disaster Prevention and Management*, *6*(1), 33-42.
Kutner, M. H., Nachtsheim, C. J., & 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*, *101*(2), 343-352.
Morgan, K. M., DeKay, M. L., Fischbeck, P. S., Morgan, M. G., Fischhoff, B. & Florig, H. K. (2001). A Deliberative Method for Ranking Risks (II): Evaluation of Validity and Agreement among Risk Managers. *Risk Analysis*, *21*(5), 923-937.
Payne, J. W., Bettman, J. R. & Johnson, E. J. (1992). Behavioral Decision Research: A Constructive Processing Approach. *Annual Reviews Psychology*, *43*, 87-131.
Payne, J. W., Bettman, J. R. & Schkade, D. A. (1999). Measuring Constructed Preferences: Towards a Building Code. *Journal of Risk and Uncertainty*, *19*(1-3), 243-270.
Pitz, G. F. & Sachs, N. J. (1984). Judgment and Decision - Theory and Application. *Annual Review of Psychology*, *35*, 139-163.
Renn, O. (2004). Perceptions of risks. *Toxicology Letters*, *149*, 405-413.
Ritov, I. & Baron, J. (1999). Protected Values and Omission Bias. *Organizational Behaviour and Human Decision Processes*, *79*(2), 79-94.
Slovic, P. (1995). The Construction of Preference. *American Psychologist*, *50*(5), 364-371.
Slovic, P., Fischhoff, B., Lichtenstein, S. (1980). Facts and Fears: Understanding Perceived Risk. In Albers Jr., W. A. (Ed.), *Societal Risk Assessment: How Safe is Safe Enough?* New York: Plenum.
Slovic, P., Lichtenstein, S. & Fischhoff, B. (1984). Modeling the Societal Impact of Fatal Accidents. *Management Science*, *30*(4), 464-474.
Tversky, A. & Kahneman, D. (1981). The Framing of Decisions and the Psychology of Choice. *Science*, *211*(4481), 453-458.
Tversky, A., Slovic, P. & Sattah, S. (1988). Contingent Weighting in Judgment and Choice. *Psychological Review*, *95*(3), 371-384.
Walker, M. E., Morera, O. F., Vining, J. & Orland, B. (1999). Disparate WTA-WTP Disparities: The Influences of Human versus Natural Causes. *Journal of Behavioral Decision Making*, *12,* 219-232.
Weber, M. & Borcherding, K. (1993). Behavioral influences on weight judgments in multiattribute decision making. *European Journal of Operational Research*, *67*, 1-12.
Webler, T., Rakel, H., Renn, O., & Johnson, B. (1995). Eliciting and Classifying Concerns: A Methodological Critique. *Risk Analysis*, *15*(3), 421-436.

Willis, H. H., DeKay, M. L., Morgan, M. G., Florig, H. K. & Fischbeck, P. (2004). Ecological Risk Ranking: Development and Evaluation of a Method for Improving Public Participation in Environmental Decision Making. *Risk Analysis*, *24*(2), 363-378.

Viscusi, W. K. & Aldy, J. E. (2003). The Value of a Statistical Life: A Critical Review of Market Estimates Throughout the World. *Journal of Risk and Uncertainty*, *27*(1), 5-76.

von Nitzsch, R. & Weber, M. (1993). The Effect of Attribute Range on Weights in Multiattribute Utility Measurements. *Management Science*, *39*(8), 937-943.

von Winterfeldt, D. (1992). Expert Knowledge and Public Values in Risk Management: The Role of Decision Analysis. In Krimsky, S. & Golding, D. (Ed.), *Social Theories of Risk*. Westport: Praeger Publishers.

von Winterfeldt, D. & Edwards, W. (1986). *Decision Analysis and Behavioral Research*. Cambridge: Cambridge University Press.

FOOTNOTES

1. EM-DAT is a database of disaster event maintained by the Centre for Research on the Epidemiology of Disasters (CRED), located at The Catholic University of Leuven.

2. Participants also had a possibility of remaining anonymous.

3. Since we were only concerned with the relative importance of the four attributes, the y-intercept was of no interest in this study.

4. 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 then, one case being withheld and the residual obtained from the prediction being recorded in each case. A cross-validated coefficient of determination is computed finally as 1-PRESS/TSS, PRESS being the Prediction Error Sum of Squares and TSS the Total Sum of Squares.

5. 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.

6. 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.