DRAFT

Report #05-016

ELECTRICITY CASE: RISK ANALYSIS OF INFRASTRUCTURE SYSTEMS-DIFFERENT APPROACHES FOR RISK ANALYSIS OF ELECTRIC POWER SYSTEMS

Holmgren, A.

CREATE REPORT
Under FEMA Grant EMW-2004-GR-0112

May 31, 2005

Center for Risk and Economic Analysis of Terrorism Events
University of Southern California
Los Angeles, California

Abstract

This paper discusses various approaches to risk analysis of infrastructure systems. The discussion is applied to electric power delivery systems, i.e. transmission and distribution of electric power, with an emphasis on the electric power grid in Sweden. In reviewing a number of the methods of risk analysis, it is concluded that methods from the systems safety and reliability discipline can to some extent be used to analyze the technical systems that form the infrastructure. However, recent advances in modeling and simulation of complex networks and also game theoretical approaches should be taken into account.

Acknowledgements

This research was supported by the United States Department of Homeland Security through the Center for Risk and Economic Analysis of Terrorism Events (CREATE), grant number EMW-2004-GR-0112. However, any opinions, findings, and conclusions or ecommendations in this document are those of the author (s) and do not necessarily reflect views of the U.S. Department of Homeland Security.

This text summarizes ideas presented in Holmgren (2004), Holmgren (2005), Holmgren & Molin (2005), and Holmgren & Thedéen (2003), which are based on work primarily sponsored by The Swedish Emergency Management Agency (SEMA). The material has been modified and also expanded (new material appears primarily in the section about expert based risk analysis) in order to be included in the current report by The Institute for Civil Infrastructure Systems (ICIS) and The Center for Risk and Economic Analysis of Terrorism Events (CREATE). The author would like to thank Professor Rae Zimmerman for being given the opportunity to spend one semester (Spring 2005) as a Visiting Scholar at The Institute for Civil Infrastructure Systems (ICIS) at New York University (NYU).

Risk Analysis of Infrastructure Systems

– Different Approaches for Risk Analysis of Electric Power Systems

Åke J. Holmgren[†]

Introduction

The modern society is depending on electricity, telecommunications, and other services delivered through a number of large sociotechnical systems. Well functioning infrastructure systems are of major importance for everyday life, economic prosperity and national security. Disturbances in the services supplied by the infrastructure systems can originate from natural disasters, adverse weather, technical failures, human factors, sabotage, terrorism, and acts of war.

Risk analysis is an essential part of the proactive risk management process, and can serve as a basis for decision-making about actions or measures to avoid disturbances, or minimize the negative consequences of disturbances. In this text, the following definition of the risk concept will be used: Risk is a combination of the probability/likelihood for an accident to occur and the resulting negative consequences if the accident occurs. Thus, the risk concept consists of two components: the probability or likelihood of a negative event and the resulting negative consequences. Risk is often reserved for random/uncertain events with negative consequences for human life and health and the environment. However, dealing with infrastructure systems, the focus is principally on the survivability of the systems, and also on the major disturbances that can cause severe strain on the whole society.

[†] Visiting Scholar (February - June, 2005), The Institute for Civil Infrastructure Systems (ICIS), New York University (NYU), 295 Lafayette Street, New York, NY 10012. E-mail: ake.holmgren@infra.kth.se

Swedish affiliations:

The Safety Research Group, The Division of Systems Analysis and Economics, The Department of Infrastructure, Royal Institute of Technology (KTH).

The Department of Technology Foresight Assessment, The Division of Defence Analysis, The Swedish Defence Research Agency (FOI).

A well-established approach when studying large technical systems are the perspectives proposed by Linstone (1984): a technical perspective, an organizational perspective and a personal perspective. Kaijser (1994) offers another set of perspectives, adapted to studies of infrastructure systems: a technical perspective, a geographical perspective, an economical perspective and an institutional perspective.

This text discusses various approaches to risk analysis of infrastructure systems. The discussion is applied to electric power delivery systems, i.e. transmission and distribution of electric power. A power system can schematically be divided into power generation, transmission and distribution, and consumption. Below, a short description of the electric power delivery system can be found. Although, there have only been a few known antagonistic attacks directed at electric power in the western world (all resulting in minor outages), electric power delivery systems must presently be considered as a potential terrorist target. Hence, antagonistic attacks play an important role in risk analysis of electric power deliver systems.

The *Swedish electric power delivery system consists* of the following types of electric grids (Holmgren, 2005):

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

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

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

The following questions summarize the major steps in the traditional risk analysis (IEC, 1995):

- What can go wrong (by hazard or threat identification)?
- How likely is it to happen (by frequency analysis)?
- What are the consequences (by consequence analysis)?

A typical situation when analyzing risk in technical systems is that there are few data of accidents or disturbances with severe consequences. Hence, it is seldom possible to use ordinary statistical methods to estimate the risk. Sometimes, useful information can be obtained from incidents (precursors) or minor disturbances. However, in many situations, especially when we are dealing with new technologies or new systems, no severe accidents have yet occurred. Theoretical (logical) models and/or experts' opinions might therefore have to be employed.

Accordingly, three principal ways to estimate the *probability* (likelihood) that a certain event (disturbance) will occur can be discerned (Holmgren & Thedéen, 2003):

- Ordinary *statistical analysis of empirical* accident or incident *data*, e.g. analysis of traffic or workplace accidents
- *Theoretical* (mathematical) *modeling* of technical systems in combination with *empirical data for components*, e.g. probabilistic safety analysis (PSA) in the nuclear and process industries
- *Expert judgments*, e.g. qualitative engineering risk analysis methods, collected through more or less formalized methods, i.e. interviews, surveys, group discussions etc.

Concerning the *negative consequences* of a disturbance or accident, a similar division can be made. There are a large number of analytical and numerical engineering models to conduct consequence analyses of fire and explosions (e.g. gas dispersion models). In many situations

it is not difficult to describe possible events with negative consequences. However, there are also areas where one faces a genuine uncertainty, e.g. environmental effects of some pollutants or the effects of low doses of radioactive radiation (i.e. dose-response problem).

Risk Analysis Using Statistical Analyses of Empirical Data

The first approach of estimating the risk is foremost applicable to areas and activities where data sets of good quality exist (stabile data sets). Two areas where this is the case are traffic accidents and occupational accidents on nation-wide levels. For example, it is possible to predict, with relatively good accuracy, the number of fatalities that will be caused by traffic accidents in Sweden during the next year. Hence, in this case the negative consequence is easy to describe (fatality) and the corresponding probability can be estimated. Further, it is achievable to calculate an accurate number of the size of the activity (a figure that captures the total amount of road transportation). Thus, a risk measure can be established (e.g. the number of fatalities in relation to the size of the activity). Finally, since there are time series spanning several years, it is also possible to study how the risk has changed over time.

In Holmgren & Molin (2005), statistical analyses of disturbance data from Swedish power transmission and distribution grids are presented and discussed (two case studies). The basic idea is to study if available data can be used to select a probability distribution function, thus enabling an estimate of the risk of major power disturbances.

Let the random variable Q be the negative consequences of a power outage. In the two Swedish data sets, consequences of outages are given as electric power indicators – i.e. unserved energy (MWh), power loss (MW), and restoration time (h). That is, the initial consequences are possible to determine, but there is no further information about the societal consequences of the outage (i.e. the effects on other services). The risk measure (in the studies also related to a measure of the activity's size, i.e. transmitted or distributed energy) can be expressed as $P(Q > q) = 1 - F(q) = R(q)$, where $F(q)$ is denoted as the probability distribution function and $R(q)$ is the survivor function. For a continuous random variable, $F(q)$ is obtained by integrating the probability density function $f(q)$.

The probability density functions of the size of disturbances in both time series (the Swedish national transmission grid, data from 11 years, and the Stockholm distribution grid, data from six years) have skewed shapes, and the largest recorded disturbance is 100,000 times larger than the smallest. This is possibly a characteristic feature of time series of accident and disturbance data from many areas, i.e. there are several minor accidents or incidents, but few major ones (compare with the discussion in the previous section). The Log-Logistic and the Log-Normal distributions have somewhat reasonable fits (Figure 1). Evaluations of the probability plots shows a tendency for the data to be heavier in the tails than both these distributions, but the Log-Logistic distribution cannot be rejected in hypothesis tests.

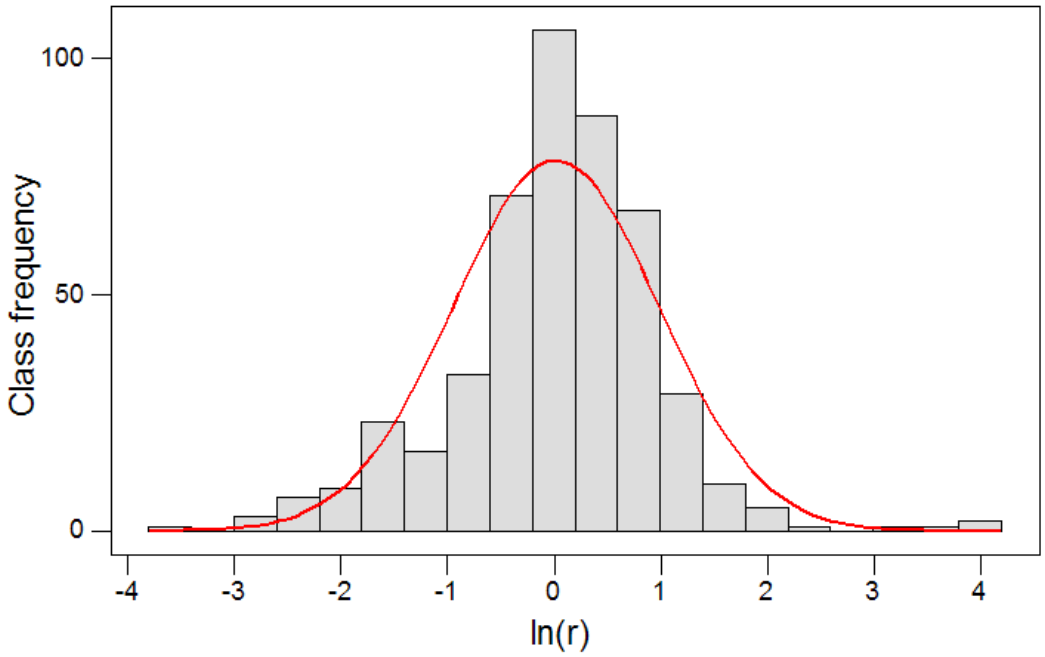

Figure 1: Histogram of the natural logarithm of the size of electric power disturbances (restoration time, hours), i.e. $\ln(r_n)$. The data set is from the Stockholm distribution grid (1998–2003) and consists of 476 observations, i.e. $n = 1,\ldots,476$. In the figure the estimated corresponding normal curve is also depicted. The Log-Normal distribution has a somewhat reasonable fit, but is rejected in the hypothesis test (Holmgren & Molin, 2005).

Recent studies of disturbance data from the bulk electric systems in North America (data from the North American Electric Reliability Council) show that the size of larger disturbances follows a power law (Chen et al., 2001; Carreras et al., 2000), i.e. there is a good

linear fit in the plot of the empirical cumulative survivor function $\ln(P(Q > q))$ versus the size of disturbances $\ln(q)$. There are observations of power laws in a wide variety of complex systems, and this has also been a pertinent topic in Physics (e.g. when studying phase transitions).

The studies show that the disturbance size Q – measured as the unserved energy (MWh), the power loss (MW) and the restoration time (h) – for the large disturbances from both the Swedish data sets, also follows a power law $P(Q > q) \sim k/\beta \cdot q^{-\beta}$ $(q \to \infty)$; see Figure 2. Further, the values of the fitted exponent β for the Swedish time series are in the same range as in the American studies.

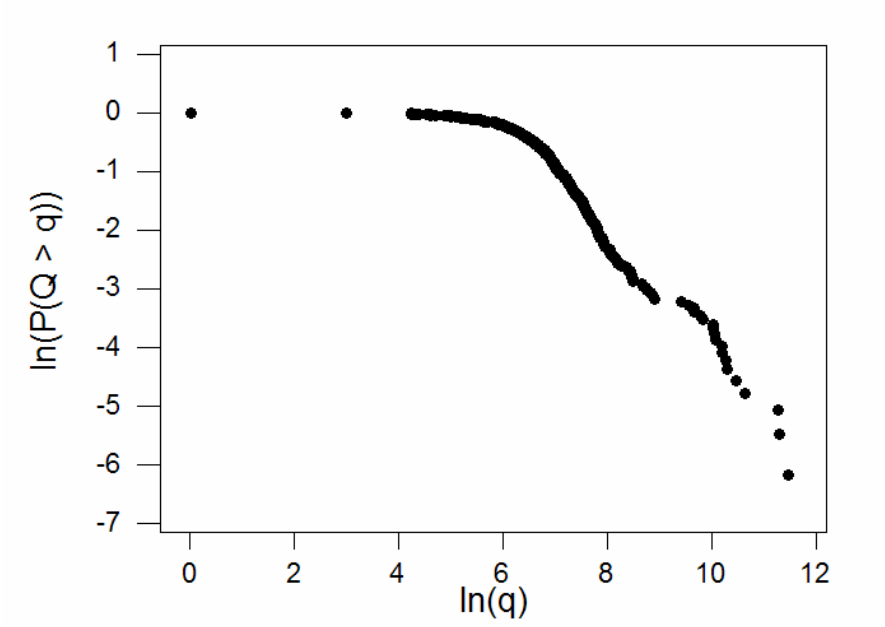

Figure 2: Log-log plot of the size of electric power disturbance data (power loss, MW) from the Stockholm distribution grid, 1998–2003, i.e. $\ln(P(Q > q))$ versus $\ln(q_n)$ for $n = 1,\ldots,476$ (Holmgren & Molin, 2005).

To study if the size of the disturbances has changed over time, a regression analysis is conducted. However, the size of the disturbances varies substantially, and even if various methods to smooth out the short-term variations (transforming data, using moving averages and removing outliers) are employed, there are large deviations from the regression line (the

standard regression analysis assumes independently normally distributed variables). Thus, a straight line is fitted to the observations with the method of least squares, and a qualitative evaluation of the plot is conducted. The result of this analysis is that the size of the disturbances does not seem to be dependent on time, i.e. the disturbance size has not increased over the studied period of time.

The data from the transmission grid has a strong seasonal component (lightning in the summer). However, if these data are removed, the Poisson process appears to be a suitable model to describe how the disturbances are distributed in time for both the time series. The analyses demonstrate that the times between disturbances are independent and exponentially distributed with mean $1/\lambda$. That is, the times of disturbances are distributed as Poisson processes with intensity $\lambda_{transmission} = 0.016$ and $\lambda_{distribution} = 0.22$ number of disturbances per day, respectively. Calculating the sample autocorrelation function of the modified series of disturbance size, no trend or periodic component is detected in either of the case studies.

Table 1: Disturbance data from the Stockholm distribution grid (1998–2003). The cause of the disturbances is classified in the following categories: Nature/weather (natural hazards or adverse weather), human factors (failure by the utility's personnel), technical failures (failure in technical equipment controlled by the utility), lightning strike, damage (deliberate attacks or sabotage), other (e.g. technical and human failures outside the utility's responsibility) and unknown (Holmgren, 2005).

Cause of disturbance	*Number of recorded disturbances*	*Largest disturbance (MWh)*	*Median disturbance size (MWh)*	*Standard deviation (MWh)*
Equipment failure	325	3900	1.0	271.8
Unknown	55	106	0.6	14.6
Other	45	9	1.6	2.4
Human factors	41	11	0.3	2.1
Damage	5	20	0.9	8.6
Nature/weather	3	71	3.8	39.8
Lightning	2	65	33.1	45.2
All disturbances	476	3900	0.97	224.8

In Table 1, data from the distribution grid is separated by the cause of the disturbance. As expected, there are very few disturbances caused by attacks (here denoted "Damage"), and it is difficult to make more profound statements about this disturbance category. The data material can also be sorted by the affected component in the grid. A possible way of using the

data material to study e.g. the consequences of an attack could be to study disturbances caused by other events, affecting components that are thought to be preferred targets by terrorists (e.g. overhead lines and transformer stations). Since the cause of the disturbance most likely will affect the consequences, this would be a very rough estimate. That is, the duration of, for example, a disturbance caused by a technical failure in an overhead line might not be a good estimate of the duration of a disturbance caused by an attack against an overhead line.

Risk Analysis Using Theoretical Modeling

Existing methods for risk analysis was originally developed to conduct analyses of nuclear power plants, airplanes and facilities within the process industry. Logical models, i.e. Fault- and event tree analysis (FTA and ETA), are well known and widely used in the systems safety and reliability discipline (usually referred to as quantitative or probabilistic risk analysis or safety analysis, abbreviated QRA or PSA), see e.g. Bedford & Cooke (2001) and Hoyland & Rausand (1994).

Presently, more and more advanced computer based supervisory, control and data acquisition systems are employed to optimize industrial processes. As a result there are increasing interdependencies between, for example, digital communication systems and electric power delivery systems. Programmable electronic systems and computer control of safety-related functions continue to replace the more traditional electromechanical implementations in commercial products. When software is combined with hardware to create programmable systems, the ability to assure conformity assessment through analysis, testing and certification becomes more difficult.

The traditional risk analysis of technical systems has mainly been concerned with technical failures and weather related events, and sometimes also human factors (i.e. a safety perspective has usually been employed). However, as mentioned above, there is an increasing international concern about antagonistic attacks against infrastructure systems (and other large-scale technical systems in society). Existing quantitative risk analysis methods can to

some extent be adjusted and used when analyzing the infrastructure systems, but a major challenge is to further develop methods to also capture the aforementioned aspects, i.e. interdependencies between different systems and antagonistic attacks. Here traditional methods of conducting quantitative risk analyses of technical systems, e.g. electric power system reliability analysis, will not be considered. Instead, two more forward-looking approaches, not specifically developed for electric power system analysis, will be discussed very briefly.

Typically, planned attacks have been analyzed in the risk analysis using conditional probabilities, i.e. given that a specific event (attack) takes place, what is the likelihood/probability of certain negative consequences? However, using the probability concept when dealing with the event itself (i.e. the likelihood of an attack) is problematic. The measures applied to protect the infrastructure affect the antagonists' course of action. Changes in the opponents' way of acting, will, again, affect the measures that are applied to protect the infrastructure. Thus, when analyzing planned attacks against the infrastructure, interactions between the defenders and the opponents must be considered. The interactions between different parties can be modeled as a game. Game theory is widely used, e.g. in economics, and attempts has been made to model antagonistic attacks with game theory in quantitative risk analyses, see e.g. Bier & Abhichandani (2003).

There has been a revival of network modeling in the past years due to increased computing power, the computerization of data acquisition, and the awakened interest in complex systems. Albert & Barabási (2002) review the recent advances that have been made in the field of graph theory and analysis of complex networks. The most studied networks are the Internet and the World-Wide Web; other studied networks are social networks such as criminal and terrorist organizations and various technical and biological networks. The following electric power grids have been studied (the same aspects have not been studied in all the networks): the Western States transmission grid in the U.S. (Watts & Strogatz, 1998; Amaral et al., 2000; Crucitti et al., 2003), the North American grid (Albert et al., 2004) and the Nordic transmission grid (Holmgren, 2004). Other studied infrastructure systems are: the Indian railway network (Sen et al., 2003), the Boston subway (Latora & Marchiori, 2002), the

network of world airports (Amaral et al., 2000), and the road network in northern Sweden (Petersen & Jenelius, 2005).

Albert et al. (2004), studies the North American power grid from a structural perspective, i.e. the grid is represented as a graph (sets of vertices and edges). The actual flow of electrical energy is not considered; only the grid's topology is modeled. In short, Albert et al. calculate statistical measures to characterize the topology of the U.S. power network and investigate the connectivity loss in the grid due to the removal of vertices corresponding to transmission substations. The study by Albert et al. has some similarities with the author's study of electric power delivery networks presented in Holmgren (2004), where the Nordic and the Western States (U.S.) transmission grid are compared with two frequently used theoretical mathematical reference networks.

This study uses a threat model that takes into consideration two kinds of threats, namely random failures (errors) and antagonistic attacks. The so-called error tolerance, e.g. failure in technical components, is modeled by removing randomly chosen vertices in the network. Attacks are realized through the removal of the vertices in decreasing degree order (the degree of a vertex is the number of connected edges). Two different attack strategies are studied: First vertices are removed by their initial degree (ID-attack) second, the degree is recalculated after every removed vertex (RD-attack). Compare with studies of other networks in Albert et al. (2000) and Holme et al. (2002).

All the studied networks disintegrate considerably faster when the vertices are removed deliberately rather than randomly, i.e. they have a lower attack tolerance than failure tolerance. For example, it is shown that the scale-free network and the electric power grids are more sensitive to attacks than the random graph. In Figure 3, an example from the analyses presented in Holmgren (2004) is shown.

Physicists have dominated the network modeling research within the field of graph theory. Lately, criticism has been put forward from the engineering community, and it has been argued that the models lack important engineering aspects, see e.g. Willinger et al. (2002). In Holmgren (2004) it is shown that a generic topological analysis is too imprecise to study the

benefits of a realistic, but not topologically far-reaching, upgrading of the Nordic transmission grid (i.e. an upgrading that electric power experts believe would increase the reliability of the overall power grid noticeably). Thus, the author agrees that the models still are very crude. However, there are no models that fully describe all the characteristics of an electric power grid (existing electric power engineering models usually have a strong technical focus). As put forward earlier in this text, the systems need to be studied from multiple perspectives. Consequently, graph models, or other abstract models, can give a conceptual picture of the network and serve as simple reference models to compare with. There have also been attempts to include more realistic features such as cascading failures in the graph models.

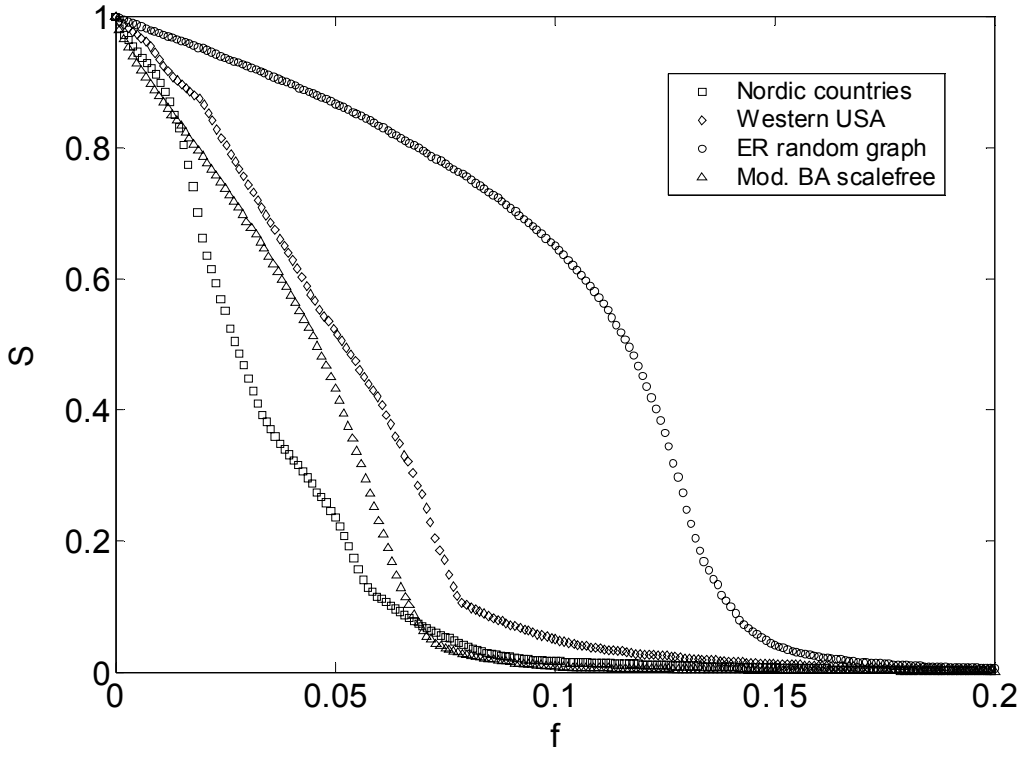

Figure 3: Attack tolerance of four different networks, i.e. two electric power transmission grids and two well-known mathematical network models. The vertices (fraction *f*) are removed in decreasing degree order. After every removed vertex, the degree is recalculated (RD-attack). The relative size of the largest component *S* is used as a measure of the network's performance (Holmgren, 2004).

However, when it comes to analyses of electric power transmission grids, the flow in the network plays a very important role. There are indications that the structure of the grid is less important than the way the grid is operated, at least when trying to avoid major power outages. That is, the large blackouts often have their origin in cascading failures, and thus the marginal in the system (the amount of load) is more essential than the topology (given that the transmission grid is constructed as a meshed network).[1] Presently, models that combine engineering aspects (e.g. the flow in the system) with ideas from the mathematical network modeling (e.g. graph theory and agent-based modeling) are being developed; see e.g. Glass (2005).

Risk Analysis Using Expert Judgments

The majority of the practical risk analyses that are carried out is qualitative or semi-quantitative, and relies extensively on expert judgments. A well-known (and standardized) practical engineering risk analysis method is the Failure Mode and Effects Analysis (FMEA), but there are a large number of scenario-based methods and work sheets to help conduct the analyses.

Typically, the qualitative analysis consists of risk scenarios generated by the experts, and includes experience-based estimates of the likelihood for an accident to occur and the resulting negative consequences if the accident occurs. The analysis is often presented as a risk matrix, where the frequency (e.g. low, medium, and high) is given on one axis, and the consequence (e.g. insignificant, moderate, and serious) is given on the other axis.

Ideally, expert opinions are based on rational reasoning, enhanced by, or derived from, practical knowledge, but they are naturally also influenced by the experts' own values and beliefs. A forward-looking perspective is most often required since the analyses can deal with systems that do not exist yet or just recently have become operational or may be operated under different circumstances or face a different set of threats in the future. Thus, fantasy and creativity are always important elements in a risk analysis.

[1] Personal communication with Professor Ian Dobson at University of Wisconsin (April 22, 2005).

There are more or less formalized ways of collecting experts' judgment, e.g. interviews, surveys, and group discussion (ranging from "brain storming" to Delphi techniques). Empirical data can also be combined with expert judgments with Bayesian statistical tools. Here, a short example of an expert based analysis will be given. The important questions of how to select experts, extract knowledge from experts, collect experts' opinions, and weigh together different experts' opinions, is considered to be outside the scope of this text. In summary, it is usually put forward that a risk analysis requires a broad range of experts (including people with practical knowledge of the studied system) and an experienced risk analyst (facilitator) to lead the work. Also, the upper management's commitment to the task, and the support from the organization, is crucial. From experience, this makes it easier to elicit knowledge from the participating experts, and maybe also less complicated to treat sensitive matters in the analysis.

There is no doubt that an integral part of the analysis is finding, organizing, and categorizing the set of risk scenarios, i.e. the hazard and threat identification. This will most likely be an even more prominent part of the analysis when dealing with planned attacks, as the estimation of the probability becomes less important, or definitely more questionable (i.e. since it in fact is a game situation – not a decision situation).

Eriksson & Ritchey (2002) emphasize the significance of a structured scenario development process:

> Development of scenarios is a common task within military analysis, but one that is sometimes approached more as an art than as a science. It is not uncommon that scenarios are developed using the proverbial 'BOGSAT' method (Bunch Of Guys Sitting Around a Table) – involving subject matter specialists but employing a rather unstructured approach for developing the scenarios. In many cases, older scenarios, also generated by 'BOGSAT', are used as a starting point.

A structured method for scenario development that has been used extensively at The Swedish Defence Research Agency (FOI) is Morphological Analysis (MA). Eriksson & Ritchey (2002) describe the method in the following way:

> Morphological analysis is a non-quantified modelling method for structuring and analysing technological, organisational and social problem complexes. It relies on the representation of a problem using a number of parameters (or variables), which are allowed to assume a number of conditions (or states). This is the analysis phase of MA. From these parameters, consistent configurations (alternatives) are derived by considering the consistency between conditions for different parameters in a pair-wise fashion. This is the synthesis phase. /…/ Problem complexes where MA is useful typically contain non-resolvable uncertainties, cannot be causally modelled or simulated, and require a judgmental approach. For this reason, morphological analysis is used in workshop sessions with experts and problem-owners. These workshop sessions are facilitated by a person knowledgeable in the method.

Morphological Analysis was used in a FOI study – see Frost et al. (2004) – about security and preparedness strategies for Swedish electric power supply systems. In Figure 4, a general morphological field from that study is shown. Highlighted in gray (the headline of each column), are the different parameters, and the possible conditions they can assume are represented as boxes in the column. In the workshop setting, the process of agreeing on the parameters is iterative. Thus, the initial set of parameters and conditions are typically reworked several times. A scenario is highlighted as a set of the black boxes (i.e. conditions that the different parameters can assume). Consequently, at this stage, a very large number of possible scenarios exist (i.e. it requires only a simple combinatory calculation to determine the number of possible scenarios).

The next step in the analysis is the pair-wise comparison between the conditions of the different parameters. For example, can Parameter 1 take on its first condition at the same time as Parameter 2 takes on its first condition? The scale used to determine consistency can in the simplest form be yes/no, but more elaborate scales are usually employed (in the FOI study a scale with four degrees was used). The result of this process is a cross-consistency matrix that makes it is possible to eliminate a large number of the scenarios (technically it is a quadratic assignment problem that is solved).

The latter phase of the Morphological analysis benefits significantly from support by computer implementation. FOI has developed such a computer application (with a graphical user interface, and running under the Windows operating system), and different versions of CASPER (Computer Aided Scenario and Problem Evaluation Routine) have been used extensively since the mid-90s (Ritchey, 1997). As a final point in the analysis, one or a number of configurations are used by the expert group for further discussion or for the solution of the problem. It is possible to go back to the preceding step and modify the morphological field or the cross-consistency matrix, and more than one morphological field can also be used to study a complicated problem.

Cause of disturbance	Operational situation in the grid (demand/ transmission)	Type of affected facility (part of the system)	Voltage level	Duration of disturbance	Geographical extension of disturbance	Affected sectors in society
Insider (low capacity)	High/High	Generation – hydro	National transmission grid	< 1 h	Rural area	Distant heating and electricity (in households)
Insider (High capacity)	High/Low	Generation – nuclear	Regional grid (sub transmission)	1 – 6 h	Urban area	Emergency care
External attacker (low capacity)	Low/High	Generation – wind	Local grid (primary distribution)	6 – 24 h	Region	General health care
External attacker (high capacity)	Low/Low	Generation – gas turbines (reserves)	Low voltage grid (secondary distribution)	24 h – 1 week	National	Rescue services
Human factors		Generation/trans-mission abroad		1 – 4 weeks		Law and order
Technical failure		Overhead line		> 1 month		Emergency call number (operators)
Natural disasters (extreme weather)		Underground cable		Irregularly recurrent power failures		Information and communication (including command and control)
		Transformer station				Technical systems in municipalities
		Switching station				Distribution of provisions
		Operation central				Keeping of livestock
		Communication system				Industrial services/ production
		Staff				Financial services
						Transportation and fuel

Figure 4: Morphological Analysis is an example of a structured method for scenario development that can be useful in a qualitative risk analysis. The figure shows a morphological field from a study about security and preparedness strategies for Swedish electric power supply systems, conducted by The Swedish Defence Research Agency (FOI), see Frost et al. (2004). The author has adapted the material and translated it from Swedish. Highlighted in gray are the different parameters, and the boxes below in each column are the conditions they can assume. Thus, the black boxes represent one scenario. About 20 persons (representatives from agencies, municipalities, industry, utilities and project members from FOI) participated in the workshops of the project.

Finally, it can be concluded that there also is a long tradition of using games (e.g. in work shop settings with experts) to analyze threats from planned attacks within military analysis. In summary, games have been used for planning, education, and for generating knowledge.

Concluding Remarks

Risk analysis is an important part of the proactive risk management process. However, societal crisis management consists of a number of phases, for example: prevent, mitigate, response, recover, and learn. When identifying actions and measures to protect the infrastructure systems, all these phases ought to be considered. That is, the whole disturbance process needs to be considered. Minimizing the duration of a power outage might in some situations be a more effective allocation of resources than using the resources to trying to prevent the event from occurring.

The preferred risk analysis approach depends on the objective of the analysis, but also on the available information about the system (e.g. are there stabile data sets of accident data?). Methods from the systems safety and reliability discipline can to some extent be used to analyze the technical systems that form the infrastructure. However, recent advances in modeling and simulation of complex networks and also game theoretical approaches should be taken into account.

Bibliography

Albert, R., Albert, I. & Nakarado, G.L. (2004). "Structural vulnerability of the North American power grid". *Physical Review E*, **69**, 025103(R) (Rapid Communications).

Albert, R. and A.-L. Barabasi (2002) *Review of Modern Physics*, 74, 47.

Albert, R., Jeong, H. & Barabási, A.-L. (2000). "Error and attack tolerance of complex networks". *Nature*, **406**, pp. 378–381. Macmillan Magazines Ltd.

Amaral, L.A.N., Scala, A., Barthélemy, M. & Stanley, H.E. (2000). "Classes of small-world networks". *Proceedings of the National Academy of Sciences*, **97**, pp. 11149–11152.

Bedford, T. & Cooke, R. (2001). *Probabilistic risk analysis: foundations and methods*. Cambridge University Press, Cambridge.

Bier, W. & Abhichandani, V. (2003). *Optimal allocation of resources for defense of simple series and parallel systems from determined adversaries*. Working paper WP030003, Decision Analysis Society.

Carreras, B., Newman, D., Dobson, I. & Poole, A. (2000). "Initial evidence for self-organized criticality in electric power system blackouts". *Proceedings of the 33rd Hawaii International Conference on System Sciences, January 2000*, Maui, Hawaii. ©2001 IEEE.

Chen, J., Thorp, J., & Parashar, M. (2001). "Analysis of electric power system disturbance data". Proceedings of the 34th *Hawaii International Conference on System Sciences, January 2001*, Maui, Hawaii. ©2001 IEEE.

Crucitti, P., Latora, V. & Marchiori, M. (2003). *A model for cascading failures in complex networks*. Preprint, arXiv:cond-mat/0309141.

Eriksson, T. & Ritchey T. (2002). "Scenario Development using Computerised Morphological Analysis". Adapted from a paper presented at *the Winchester International OR Conference*, England 2002.

Frost, C., Lövkvist Andersen, A-L., Barck-Holst, S. & Ånäs, P. (2004). *Acceptabla elavbrott? Fyra strategier för säker elförsörjning*. (Acceptable outages? Four strategies for dependable electric power supply), FOI-R--1163--SE, The Swedish Defence Research Agency (FOI), Stockholm.

Glass, R. (2005). "Simulation and analysis of cascading failure in critical infrastructure". Paper presented at *Working Together: R & D Partnerships in Homeland Security*, April 2005, Boston.

Holme, P., Kim, B. J., Yoon, C.N. & Han, S.K. (2002). "Attack vulnerability of complex networks". *Physical Review E*, **65**, 056109.

Holmgren, Å. (2004). "Using graph models to analyze the vulnerability of electric power networks". Paper submitted to *Risk Analysis*. Blackwell Publishing, London.

Holmgren, Å. (2005). "A framework for vulnerability assessment of electric power delivery systems". In review, to appear in: Murray, A. & Grubesic, T. (eds). *Reliability and Vulnerability in Critical Infrastructure: A Quantitative Geographic Perspective.* Advances in Spatial Science Series, Springer-Verlag.

Holmgren, Å. & Molin, S. (2005). "Using disturbance data to assess vulnerability of electric power delivery systems". Paper accepted for publication in *The Journal of Infrastructure Systems*, American Society of Civil Engineers (ASCE).

Holmgren, Å. & Thedéen, T. (2003). "Riskanalys" (Risk analysis). In Grimvall, G., Jacobsson, P. & Thedéen, T. (eds.) 2003. *Risker i tekniska system* (Risk in technical systems). Studentlitteratur, Stockholm.

Hoyland, A. & Rausand, M. (1994). *System reliability theory: models and statistical methods*. Wiley, New York.

IEC (1995). *Dependability management – Part 3: Application guide – Section 9: Risk analysis of technological systems*. International Electrotechnical Commission (IEC), Geneva.

Kaijser, A. (1994). *I fädrens spår. Den svenska infrastrukturens historiska utveckling och framtida utmaningar* (The Swedish infrastructure – historical development and future challenges). Carlsson Bokförlag, Stockholm.

Latora, V. & Marchiori, M. (2002). "Is the Boston subway a small-world network?". *Physica A*, **314**, pp. 109–113.

Linstone, H. (1984). *Multiple perspectives for decision-making; bridging the gap between analysis and action*. North-Holland, Amsterdam.

Petersen, T. & Jenelius, E. (2005). "Applying the concepts of importance and exposure in road network vulnerability analysis: A case study for Northern Sweden". Paper to be presented at the *NECTAR Conference 2005* (Network on European Communication and Transportation Activities Research), June 2005, Las Palmas.

Ritchey, T. (1997). "Scenario development and risk management using morphological field analysis: research in progress", *Proceedings of the 5th European Conference on Information Systems*, Vol. III, pp. 1053-1059.

Sen, P., Dasgupta, S., Chatterjee, A., Sreeram, P., Mukherjee, G. & Manna, S. (2003). "Small-world properties of the Indian railway network". *Physical Review E*, **67**, 036106.

Watts, D.J. & Strogatz, S.H. (1998). "Collective dynamics of 'small-world' networks". *Nature*, **393**, pp. 440–442.

Willinger, W., Govindan, R., Jamin, S., Paxson., & Shenker, S. (2002) “Scaling phenomena in the Internet: critically examining criticality”. *Proceedings of the National Academy of Sciences*, **99**, pp. 2573–2580.