3 A Framework for Vulnerability Assessment of Electric Power Systems

Åke J. Holmgren

Division of Safety Research, Royal Institute of Technology (KTH), Sweden, and the Swedish Defence Research Agency (FOI); Email: ake.holmgren@foi.se

3.1 Critical Infrastructure Protection

The infrastructure of a society consists of facilities such as communications, power supplies, transportation, water supplies, and the stock of buildings. In a broad definition of infrastructure, it is also possible to include basic societal functions like education, national defense, and financial and judicial systems. Here, the notion critical infrastructure will refer to the collection of large technical systems, for example electric power grids, which form the basis for most activities in a modern society, and are of great importance for the economic prosperity. Today, critical infrastructure protection is also considered to be a matter of national security.[1]

This chapter introduces a *framework for quantitative vulnerability assessment* (vulnerability analysis and evaluation) of critical infrastructure systems. The framework is applied to *electric power delivery* (i.e. electric power transmission and distribution). Vulnerability is described as a susceptibility (sensitivity) to threats and hazards that substantially will reduce the ability of the system to maintain its intended function.

Disturbances in the electric power supply can originate from natural disasters, adverse weather, technical failures, human errors, labor conflicts, sabotage, terrorism, and acts of war. A disturbance has its starting point in

[1] American security policy makes a distinction between "homeland security" and "national security". Critical infrastructure protection is identified as a "critical mission area" in the *National Strategy for Homeland Security* from 2002. However, protection of the infrastructures has traditionally been an integral part of the defense in countries such as Sweden and Norway (embraced by concepts such as "total defense" and "societal security").

an initiating event, i.e. a threat or hazard that is materialized. This event is, in turn, leading to one or more technical conditions in the power system that may lead to a smaller or larger power system failure and possibly a loss of electric power for all, or some, users, i.e. a power outage (black-out). In this chapter, a national security perspective is adopted, and the focus is, thus, on events that can cause severe stress on the whole society. For electric power delivery, this means power outages with a prolonged duration, a large power loss, and many affected people.

It is possible to find a broad range of checklists and practical frameworks for risk and vulnerability analysis. That is, step-by-step descriptions of how to conduct a specific method or how to use a particular analysis technique, as well as worksheets for conducting surveys (e.g. DoE 2002a; 2002b; IEC 1995). There are, however, few general frameworks that approach the subject of quantitative vulnerability assessment in a more scholarly manner. Relevant knowledge (modeling and analysis techniques) can be found in many scientific disciplines including mathematics, statistics, electric power systems engineering etc. (see also the other chapters). In order to be able to properly use quantitative techniques, there is a need for a fundamental discussion about the context of the quantitative modeling, as well as concepts such as “vulnerability” and “reliability”.

3.2 Electric Power Delivery and Major Power Outages

An electric power system can schematically be divided into generation units (generators, transformers etc.), delivery systems, and users. Where the *electric power delivery system* usually consists of:

- *Transmission grids* (high-voltage) are meshed networks, connecting large generating stations (e.g. hydro power and nuclear power), sub transmission grids, and very large users. Transmission grids enable power trading with other countries and facilitate the optimization of generation within a country.
- *Sub transmission grids*, or regional grids, are radial or locally meshed networks connected to the transmission grid via infeed points. Smaller generating plants (e.g. wind power stations and gas turbines), and large users are connected to these grids.
- *Distribution grids* (low-voltage) are radial networks that carry the electric power from the higher voltage levels to the final users. The number of levels in a distribution grid depends upon the density and magnitude of demand and the terrain.

In an electric power system there always has to be a *balance* between the load and the generation (the real time power balance stage is called dispatch). The *load* on the system varies over day and season, and so does the available *generation*. These conditions put special requirements on the operation and control of the electricity generation and delivery process. In general, there are three levels of control: i) The control center or Energy Management System (EMS); ii) The data collection system called SCADA (supervisory control and data acquisition system); iii) AGC (automatic generation control) for maintaining the instantaneous power balance.

The impact of a *major power outage* will be determined by the nature of the affected area, the duration of the disturbance, the time of day, the weather conditions etc. A major blackout will affect all functions in a society, and economical life stops in a region without electricity (UCTE 2003; U.S.-Canada Task Force 2004). People in large cities will usually be more affected than those living in rural areas. Indirect effects of a blackout can have a major spread in time and space, for example an increase in crimes in larger cities, interruptions in communications and transportations, and low indoor temperatures during wintertime. Especially critical is the state of dependence between telecommunications and power systems. After a few days there can be a shortage of food and fuel, which affects the reserve supply of electricity from backup generators.

3.3 Vulnerability Assessment

3.3.1 The Vulnerability Concept

The concept of vulnerability is employed in e.g. psychology, sociology, political science, economics, epidemiology, biology, environmental and geosciences, and engineering (McEntire 2005). For technical applications there is no generally accepted definition of the concept. In Holmgren and Molin (2005) the following working definition is used: “Vulnerability is the collection of properties of an infrastructure system that might weaken or limit its ability to maintain its intended function, or provide its intended services, when exposed to threats and hazards that originate both within and outside of the boundaries of the system”.

In this chapter, the concept of vulnerability is used to describe a lack of robustness and resilience in relation to various threats and hazards. Threats and hazards are the sources of potential harm or situations with a potential for harm. *Hazards* relate to accidental events, whereas *threats* relate to deliberate events. *Robustness* signifies that the system will retain its system structure (function) intact (remains unchanged or nearly unchanged) when

exposed to perturbations, and *resilience* implicates that the system can adapt to regain a new stable position (recover or return to, or close to, its original state) after perturbations. Here, robustness and resilience taken together is treated as the *complement of vulnerability* in the same way as safety can be an antonym to risk. (However, more refined distinctions can be made, e.g. Hansson and Helgesson (2003) show in a formal concept analysis that robustness can be treated as a special case of resilience.)

The *monadic* concept "vulnerability", divides systems into two categories: vulnerable, and not vulnerable. The *comparative* notion "at least as vulnerable as" compares systems according to their degrees of vulnerability. A monadic concept can, in theory, be obtained from the comparative one through the addition of precise limit somewhere on the scale of degrees of vulnerability. A monadic notion of vulnerability is not useful in real life – all systems are sensitive to some threats and hazards, and hence vulnerable in some respect. However, using the comparative notion is not always straightforward. A system may be vulnerable with respect to some threats (perturbations) but not to others. If two systems are vulnerable in relation to different kinds of threats, there may be no evident answer to the question which of them is more vulnerable. They may very well be incomparable in terms of vulnerability.

In this chapter, the following *formal definition of vulnerability* is proposed: the vulnerability of an infrastructure system is the probability of at least one disturbance with negative societal consequence Q larger than some large (critical) value q, during a given period of time T. Let $Q(t)$ be the societal consequence of a disturbance that occurs at time t, $t \in T$. Then, the vulnerability of the infrastructure system is measured by the function

$$P(\max_{t \in T} Q(t) > q). \tag{1}$$

Consequently, the vulnerability of an infrastructure system is the probability of a system collapse causing large negative societal consequences.

The consequence Q of a power outage can be described by technical indicators such as power loss (MW) or unserved energy (MWh). Also, more general indicators can be employed, for example the cost of the power outage or the number of affected users. No attempt will be made here to exactly specify what constitute large negative consequences (large q). However, the term severe strain on society (frequently used in Swedish official policy documents) can be used to loosely characterize what represents a major disturbance.

In some situations it is possible to estimate the probability that a hazard or threat is realized, however, in other situations (e.g. antagonistic threats),

a conditional approach can be used. Let A_i be an initiating event, then the *conditional vulnerability* can be defined as

$$P(\max_{t \in T} Q(t) > q \mid A_i). \tag{2}$$

In a study of road network vulnerability, Jenelius et al. (2006) discuss the vulnerability concept, and referrers to the conditional probability as "exposure" (See further Sect. 3.4).

There are obvious similarities to the risk and reliability concepts in the vulnerability measure above. However, the *risk* concept is both a bit more restricted and a bit broader. As with the risk concept, there are two dimensions: the probability or likelihood of a negative event and the resulting negative consequences. Risk is often reserved for random/uncertain events with negative consequences for human life and health, and the environment. Regarding the vulnerability of the critical infrastructures, planned attacks play an important role. Further, it is principally a focus on the survivability of the system, and the concept of vulnerability is not used in relation to minor disturbances. The *reliability* concept can be captured by several different measures. The reliability function (survivor function) $R(t)$ for an unreparied unit can be defined as $R(t) = P(T > t)$, for $t > 0$, where T is the time to failure. Accordingly, $R(t)$ is the probability that the unit survives the time interval $(0, t]$ (Høyland and Rausand 1994).

3.3.2 The Vulnerability Assessment Framework

A framework for quantitative vulnerability assessment of infrastructure systems is presented in Fig. 3.1. The framework draws on experiences from system studies conducted by the Swedish Defence Research Agency (FOI), and the traditional framework for risk assessment as presented in IEC (1995). Examples of vulnerability assessment frameworks inspired by the conventional risk analysis can also be found in Einarsson and Rausand (1998) and Doorman et al. (2006).

The aim of a *vulnerability assessment* can be to identify events that can lead to critical situations (large negative consequences), and study how the function of the system can be restored after the disturbance. Further, the assessment can involve an evaluation of the level of vulnerability, and (if needed) an analysis of options for enhancing the robustness and/or resilience of the system. The assessment of an existing system involves checking its status or following up changes. A vulnerability assessment can, thus, facilitate the development of responses to possible crisis situations, and found the basis for prioritization between different alternatives to im-

prove system performance. The task of conducting an assessment can create an awareness of risk and vulnerability management in the organization and increases the motivation to work with these issues.

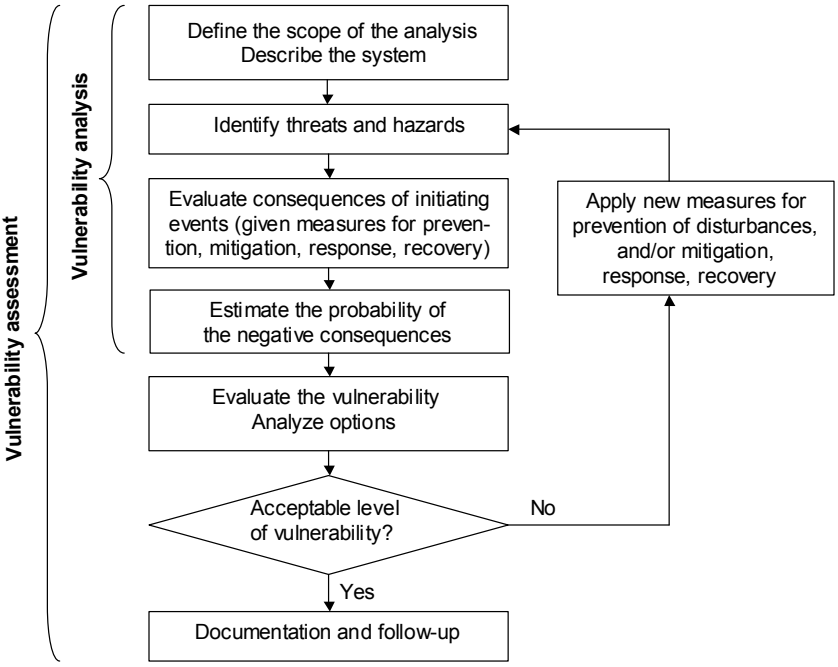

Fig 3.1 A framework for quantitative vulnerability assessment of infrastructures

3.4 Foundations of Vulnerability Analysis

A fundamental part of the vulnerability assessment is the vulnerability analysis, which can be captured by the following four questions (compare with Fig. 3.1):

1) What can go wrong?
2) What are the consequences?
3) How likely is it to happen?
4) How is a normal state restored?

The major difference between the risk and the vulnerability analysis is that the latter focuses on the whole *disturbance process* (the survivability of the system), and the major disturbances. For some initiating events (e.g. failure of technical components), it might be possible to estimate their fre-

quency. For other events, the conditional probability can be used (Eq. 2). Thus, the total probability is a sum where the terms consists of two parts: i) the probability that the initiating events A_i occur, and ii) the probability that this leads to consequences $Q > q$, i.e.

$$P(\max_{t\in T} Q(t) > q) = \sum_i P(A_i) \cdot P(\max_{t\in T} Q(t) > q \mid A_i). \tag{3}$$

A typical situation when analyzing the vulnerability of technical systems, especially when dealing with new technologies, is that there are few data of disturbances with severe consequences (a low probability high consequence, LPHC, problem). Useful information can be obtained from incidents (precursors), but it is seldom possible to use standard statistical techniques to estimate the vulnerability. Instead, mathematical models and/or experts' opinions have to be used. In summary, there are three principal ways to estimate the probability of occurrence of a negative event:

a) Statistical analysis of empirical disturbance (accident) data
b) Mathematical modeling combined with empirical component data
c) Expert judgments

Regarding the resulting negative *consequences* of an event, a similar division can be made. Within the engineering disciplines, analytical and numerical models play an important role in consequence analysis, among others for evaluating the consequences of fire, explosions, dispersion of chemical agents etc. There are advanced numerical models for static and dynamic analysis of power systems (e.g. optimal power flow). For example, Milano (2005) provides a description of an open source toolbox for design and analysis of small to medium size electric power systems.

Ordinary *statistical analysis* of *empirical* accident *data* is used extensively in studies of traffic and workplace accidents. The use of *mathematical modeling in combination with empirical component data* is well established in the nuclear and process industries (quantitative risk analysis or probabilistic safety analysis). *Expert judgments* are normally the primary sources of information in typical engineering risk analysis methods, and can be collected through more or less formalized methods (interviews, surveys, workshops etc.). Empirical data can also be combined with expert judgments with Bayesian statistical tools. Overall, the traditional *risk analysis offers a toolbox* of established quantitative, and semi-quantitative, methods for safety analysis of well-defined technical systems.

The rapid proliferation of *information and control systems* has increased the possibilities of optimizing, and controlling, industrial processes. Today, large technical systems are inherently so complicated that a layer of control, monitoring, and coordination is required for their normal opera-

tion. When software is combined with hardware to create programmable systems, the ability to assure conformity assessment through analysis, testing and certification becomes more difficult.

A fundamental problem in system studies lies in the fact that the response to all possible stimuli is not fully understood. Describing, and delimiting, a system as a first step in a vulnerability assessment is, thus, a daunting task. Uncertainties are experienced not only when it comes to the system itself, i.e. the *interactions* between the parts of the system, but also regarding the properties of the environment, i.e. the context. The interactions between different infrastructures, often referred to as *interdependencies*, are particularly important when dealing with critical infrastructure protection since infrastructures often act together to provide a service.

In the literature, critical infrastructures are typically portrayed as *complex systems*, but the meaning of the concept "complex" is often unclear. Commonly, the concept is used for *characterizing* the system, but it can also be a *metaphor* or analogy. The term complex can also be used to make an arbitrary distinction between something *perceived* as simple, and something perceived as complicated – the simple/complex dichotomy. Complexity, used as a metaphor, generally implies a critique against the traditional reductionist approaches and the predominant systems theory. Thus, it is a conception that synergies emerge when large sets of entities are brought together. Labeling a system complex, can also be a way of swiftly capturing properties considered to be the hallmarks of complexity, i.e. nonlinearity, adaptability, self-organization, emergence etc.

A variety of different measures would, hence, be required to capture all intuitive ideas about what is meant by complexity, and complexity, however defined, is not entirely an intrinsic property of the entity described; it also depends on who or what is doing the describing (Gell-Mann 1997). No attempts to make a formal definition of a complex system shall be undertaken, instead the author agree with Simon (1962):

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

Accordingly, the author argues that studies of critical infrastructures must rely on both detailed engineering modeling, and coarse modeling that focus on generic mechanisms. Existing methods for risk analysis can, to some extent, be adjusted and used in vulnerability analysis of infrastructure systems, but a major challenge is to further develop methods for analysis of complex systems (see examples in Sects. 3.5–3.7).

3.5 Example 1 – Statistical Vulnerability Analysis

Generation and trading of electricity in Sweden is carried out in a competitive environment, but Swedish grids are still regulated monopolies. The Swedish Energy Agency is responsible for ensuring that the grids are operated efficiently. As a part of the evaluation of tariffs, all utilities are obligated to report power outages to the Agency. Utilities typically publish compiled power outage data in annual reports, but seldom use statistical tools in the analysis. The aim of the author's study, presented in Holmgren and Molin (2005), is to explore the possibilities of using *statistical analyses of power outage data in vulnerability analysis* of electric power delivery (compare with approach a) in Sect. 3.4).

The vulnerability measure in Eq. (1) can be formulated as

$$P(Q > q) = 1 - F(q) = R(q)\,, \tag{4}$$

where $F(q)$ is the probability distribution function, and $R(q)$ is denoted the survivor function. For a continuous random variable, $F(q)$ is obtained by integrating the probability density function $f(q)$. The study includes data from the Swedish national transmission grid (153 observations from 11 years,), and the Stockholm distribution grid (Table 3.1). The power outage size Q is measured as the unserved energy (MWh), the power loss (MW), and the restoration time (h), i.e. there are six time series of power outage data.

Table 3.1 Power outage data from a Swedish distribution grid (1998–2003)

Cause	n	n_{max} [MWh]	n_{median} [MWh]	n_{Q3} [MWh]
Equipment failure[a]	325	3900	1.0	2.4
Unknown	55	106	0.6	1.4
Other[b]	45	9	1.6	2.9
Human factors[c]	41	11	0.3	1.3
Damage[d]	5	20	0.9	1.5
Nature/weather[e]	3	71	3.8	-
Lightning	2	65	33.1	-
All disturbances	476	3900	1.0	2.3

n number of recorded power outages, n_{max} largest power outage, n_{median} median power outage, n_{Q3} third quartile (75th percentile).

[a] Failure in technical equipment controlled by the utility.

[b] Technical, and human failures, outside the utility's responsibility.

[c] Failure by the utility's personnel.

[d] Deliberate attacks or sabotage.

[e] Natural hazards or adverse weather (except for lightning).

The *probability density functions f*(*q*) in all the data sets have *skewed shapes*, and the largest recorded power outage is 100 000 times larger than the smallest. This is a characteristic feature of time series of accident data from many areas, i.e. there are several minor accidents, but few major ones (the LPHC problem). Statistical distributions such as the log-logistic, and the lognormal, fit the data somewhat reasonable. Evaluations of probability plots show a tendency for the data to be heavier in the tails than in both these distributions (log-logistic cannot be rejected in hypothesis tests).

Recent studies of power outage data from the bulk electric systems in North America (data from the North American Reliability Council) show that the larger outages follow a *power law* (Chen et al. 2001; Carreras et al. 2000, 2004b). That is, there is good linear fit in a plot of the empirical cumulative survivor function $\ln(P(Q > q))$ versus the size of the power outages $\ln(q)$. The studies of the Swedish data also demonstrate that the power outage size follows a power law (see example in Fig. 3.2), where

$$P(Q > q) \sim A \cdot q^{-\beta} \quad (q \to \infty). \tag{5}$$

Since power law distributions have "heavy tails", the distribution allows for extremely rare events with extraordinarily large size (as compared to the standard normal distribution).

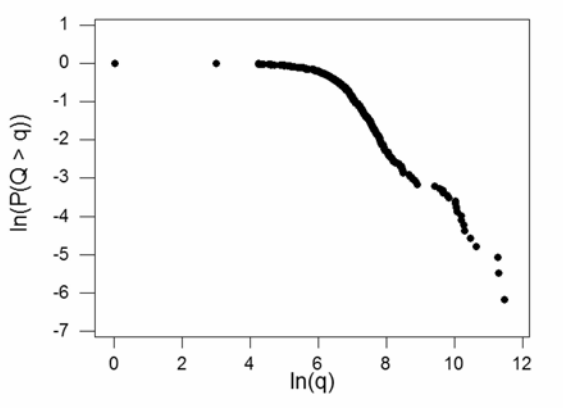

Fig. 3.2 Log-log plot of power outage data [power loss, MW] from the Stockholm distribution grid (1998–2003), i.e. $\ln(P(Q > q))$ versus for $\ln(q_n)$, $n = 1,\ldots,476$. The plot (and a regression analysis not displayed here) demonstrates that the distribution follows a power law for large q (Holmgren and Molin 2005).

Utilities can use information from *outage analysis* when deciding on equipment purchase or how to organize maintenance. Systems for reporting incidents and disturbances can give increased knowledge about how disturbances arise and how disturbances can be avoided. Further, statistical

analysis of outages data makes it possible to objectively follow-up the system performance, and to discover deficiencies that call for more detailed investigations. For both the studied Swedish power grids, there are no statistically significant shifts of the trend in the data – the outage size does not depend on the time. This can be an indication that the vulnerability of the systems not has changed considerably during the studied period.

3.6 Example 2 – Graph Theoretic Vulnerability Analysis

Complex systems can often in a useful way be described as networks, and networks can be represented as graphs. A *graph* $G = (V, E)$ can be defined as "a triple consisting of a vertex set $V(G)$, an edge set $E(G)$, and a relation that associates with each edge two vertices (not necessarily distinct) called its endpoints" (West 2001). Depending on what type of systems that is being observed, vertices and edges can be accentuated differently. In the following, the graphs will be undirected, and connected, which relates to the general structure (topology) of the network, whereas directed graphs relates to the actual flow of power in the network (given a specific operational scenario). Thus, the vertices can be generation units, stations, or users, and the edges can represent power lines.

Albert and Barabási (2002), and Dorogovtsev and Mendes (2002), review recent advances made in the field of graph theory and network analysis. A number of *statistical measures* have been proposed to characterize the structure of complex networks, and the following concepts are central:

- *Average path length:* the distance between two vertices is defined as the number of edges along the shortest path connecting them. In most complex networks there is, despite their often-large size, a relatively short average path length between any two vertices.
- *Clustering coefficient*: this measure captures the density of triangles in the graph. The clustering coefficient of a vertex is the ratio between the actual number of edges that exist between the vertex and its neighbors and the maximum number of possible edges between these neighbors.
- *Degree distribution* the number of edges connected to a vertex is called the degree. The degree distribution $P(k)$ of many empirical networks has a power law tail, $P(k) \sim k^{-\beta}$, where β is between 1 and 3 (Albert and Barabási 2002).

The studies of networks has given birth to several classes of abstract network models. Erdös and Rényi introduced the idea of *random graphs* in

the late 1950s. The simple random graph model combines low clustering with an exponential degree distribution. Watts and Strogatz introduced the so-called *Small World model* in 1998. This model combines high clustering and a short average path length (Watts and Strogatz, 1998). In 1999 Barabási and Albert presented the *Scale-free network model* that has a power-law degree distribution (Albert and Barabási 2002).

As far as the author knows, graph theoretic models have been used to study the following electric power grids (the same aspects have not been studied for all networks): the Western States transmission grid in the U.S. (Watts and Strogatz 1998; Amaral et al. 2000; Crucitti et al. 2004a), the North American grid (Albert et al. 2004), the Italian grid (Crucitti et al. 2004b; Rosato et al 2006), the French grid, the Spanish grid (Rosato et al 2006), and the Nordic transmission grid (Holmgren 2006).

Table 3.2 The structure of electric power transmission networks[a]

Network	C_{Actual}	C_{Random}	l_{Actual}	l_{Random}
The Western States power grid[b]	0.0801	0.00054	18.99	8.7
The Nordic power grid[c]	0.0166	0.00049	21.75	10.0

C_{Actual} Clustering coefficient (empirical network), C_{Random} Clustering coefficient (random graph of equivalent size), l_{Actual} Average path length (empirical network), l_{Random} Average path length (random graph of equivalent size).

[a] For formal definitions and algorithms, see Holmgren (2006).

[b] 4941 vertices and 6594 edges.

[c] 4789 vertices and 5571 edges.

In Holmgren (2006), an analysis of the *structural vulnerability* of the Nordic Interconnected grid and the Western States (U.S.) transmission grid is presented. Table 3.2 compares the structure of the power grids with random graphs of the equivalent size (calculations for the U.S. grid are also presented in Watts and Strogatz (1998)).

The Nordic grid is more scattered than the Western States (U.S.) grid, i.e. the average path length is larger and the clustering coefficient is lower. However, both transmission grids have a clustering coefficient significantly larger than the random graphs, and the average path length is more than twice as large as in the random graph. That is, the transmission grids show the "small world" phenomenon (the clustering coefficient is much larger than in the equivalent random graph, but the average path length is only somewhat larger in the power grids). Further, it is shown that both power grids have approximately exponential degree distributions, which also is a characteristic feature of the random graph. (A study of the degree distribution of the Western States grid was initially presented by Amaral et al. (2000).)

In the structural vulnerability analysis, failures are modeled by removing randomly chosen vertices of the graph (error tolerance). Attacks are realized through the removal of the vertices in decreasing degree order (attack tolerance). Two different attack strategies are studied: vertices are removed by their initial degree (number of connected edges), or the degree is recalculated after every removed vertex. The power grids are compared with two network models, i.e. a random graph and a scale-free network (see also Albert et al. (2000) and Holme et al. (2002)).

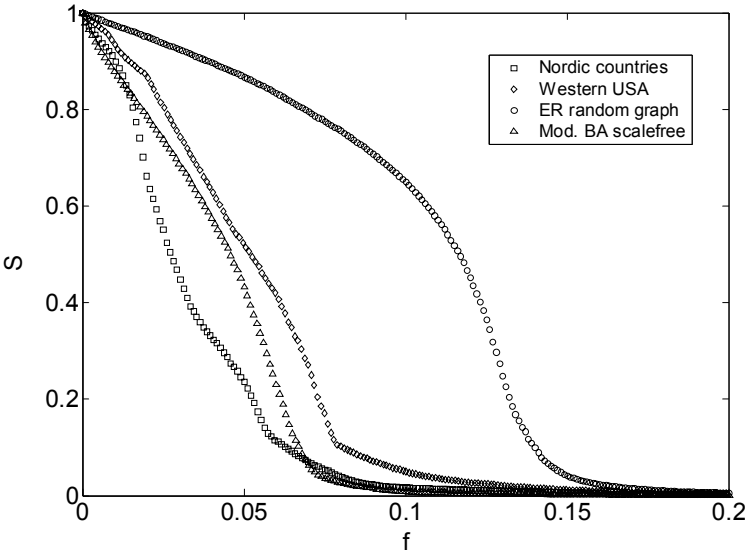

Fig. 3.3 Defragmentation of four different networks of approximately the same size. The vertices (fraction *f*) are removed in decreasing degree order (i.e. the vertex with most connected edges is removed first). After every removed vertex, the degree is recalculated. The relative size of the largest connected subgraph (component) *S* is used as a measure of the consequences of removing vertices, i.e. measure the attack tolerance of the network. The figure shows that the two electric power grids, and the scale-free network, are more sensitive to attacks than the random graph (Holmgren 2006).

Detailed data on the structure of the two transmission grids are restricted. Hence, it is not possible to separate vertices representing users from vertices representing other installations. Thus, different indirect measures are used to estimate the consequences of removing vertices in the network. The simulations confirm the results from previous studies above, and demonstrate that all studied networks disintegrate considerably faster when vertices are removed deliberately than randomly, i.e. the networks have a lower attack tolerance than failure tolerance. Further, the two electric power networks exhibit similar disintegration patterns, both for ran-

dom failures and attacks (Fig. 3.3). Also, it is shown that the scale-free network and the electric power grids are more sensitive to attacks than the random graph.

An important field of application for the vulnerability analysis is to evaluate alterations of an existing system. As an experiment, the graph of the Nordic power transmission grid is modified by incorporating two new edges (power lines) between Sweden and each country in the region, i.e. six new edges. The new power lines are positioned as in an internal study proposal from Svenska Kraftnät (SvK) – the utility that operates the Swedish national transmission grid. Comparing the augmented Nordic grid with the present Nordic grid, however, yields small, if no, visible changes in the error and attack tolerance (as analyzed here). Thus, a generic graph analysis, based on open-source data of the structure of the networks, is too simplistic for practical purposes.

Table 3.3 Examples of hazard and threat scenarios (Holmgren 2006)

Scenario	Description	Graph realization
Major technical failure	A major technical failure disables a station in the sub-transmission grid or the distribution grids.	Anyone of the vertices in the graph is removed with probability $p = 0.005$ (per year). Repair time: 12 h.
Snow-Storm	A snowstorm causes technical failures at the distribution level (overhead power lines).	Any two adjacent edges in the distributions grid are removed with $p = 0.01$. Repair time: 8 h.
Saboteur	This class of adversaries has a broad spectrum of motives, and can act irrational. The saboteur has little knowledge of the power system, does not have access to explosives, and is only capable of a single-entity attack.	Anyone of the vertices and edges in the distribution grids is a possible target. Attack by a rational (determined) saboteur: repair time 10 h. Attack by an irrational (opportunistic) saboteur: repair time 5 h.

In order to illustrate how the methodology can be applied in a more detailed evaluation of a system, a fictitious power delivery system is studied. A broad set of threat and hazard scenarios is represented as the removal of vertices and edges by introducing different repair times (a brief example is given in Table 3.3). The consequence of removing an entity in the graph might be a number of disconnected sink vertices (collectives of users). By assuming a load (MW) on each sink vertex, the consequence Q is measured as the *unserved energy* (MWh), here approximated as the power loss (MW) multiplied with the recovery time (h). The recovery time depends

on the repair times of the removed components. For all the scenarios, the measure $P(Q > q)$ is calculated (conditional vulnerability is used for attacks), and a relative comparison is made between three different tactics for upgrading the system: "Robustness" (strengthening the network by adding new edges), "Resilience" (shortening repair times), and "Combination" (a mix of the two other tactics).

As pointed out above, the study of abstract models can be a way of finding generic mechanisms, and increase the understanding of complex systems. Also, there are several practical reasons why studies of abstract network models of electric power systems can be a useful complement to the analysis of actual systems. Firstly, electric power grids, as other complex systems, are extremely large if modeled in detail, and the simulations will, therefore, be extremely demanding. Secondly, detailed data on electric power grids can seldom be obtained since they often are restricted. Thirdly, vulnerability assessment involves studies of antagonistic attacks. For security reasons, studies of attacks against authentic networks will most likely be classified.

However, the graph-based models described above are rather primitive, and a major drawback is that they do not capture how networks are operated. Electric power system analysis traditionally have a strong technical focus, including analysis of power flow, stability etc. for optimization of normal operations and emergency control (whereas the focus in this chapter is on "in extremis" states). For example, Salmeron et al. (2004) describe an analytical technique (an algorithm) to search for the worst-case disruptions in an electric power grid due to physical attacks. The terrorists' resources are specified as the number of people, and to interdict a power line, transformer station or sub station requires a given number of people.

Currently, there are no practically usable generic graph models of electric power grids. Holmgren and Thedéen (2006) use a simple analytical graph model to represent a distribution grid. The network is modeled as a random tree (branching process), and it is shown that failure in the network (removal of edges) results in a power outage size distribution that follows a power law (compare with Sect. 3.5). The branching process model captures the hierarchical nature of electric power grids, but at this stage it does not include clustering (the clustering coefficient $C = 0$ in a tree since there are no cycles).

Major power outages typically include *cascading failures* in electric power transmission grids, i.e. multiple failures that are the direct result of a common or shared root cause (UCTE 2003; U.S.-Canada Task Force 2004). Given a lightly loaded power system, there is a very low likelihood that a trip in a power line will cause a power outage. As the load increases, more dependent failures occur, and at some critical load, a trip in a power

line might cause an instability that cascades in the network, and eventually resulting in a major blackout.

There are several different approaches to studying cascading failures in power systems, see Dobson et al. (2005) for an overview of this subject. For example, Carreras et al. (2004a), use a DC load flow approximation, and standard linear programming optimization, to represent cascading transmission line overloads. Motter and Lai (2002) as well as Crucitti et al. (2004b) use graph models (simulation) that do not consider the flow in networks. There are also analytical models to study cascading failures, and Dobson et al. (2004) presents a branching process model for approximating the propagation of failures in a transmission grid.

In summary, the author believes that it is vital to improve the understanding of the relationship between *dynamics* and vulnerability of complex networks. Thus, vulnerability analysis of electric power networks would benefit greatly from more cross-fertilization between electric power engineering, and the network modeling and simulation of complex systems as introduced here.

3.8 Example 3 – Game Theoretic Vulnerability Analysis

Antagonistic attacks are typically analyzed using conditional probabilities (Eq. 2). To use the probability concept when dealing with planned attacks is, however, problematic. The measures applied to protect the infrastructure will affect the antagonist's course of action (assuming an informed adversary). Changes in how the defender perceives that the opponent will act, will again affect how the defense is allocated, which once more can affect the antagonist's behavior etc. There is an *interaction* between the attacker and the defender. Therefore, studies of attacks embrace a game situation rather than a decision situation. In defense analysis, *game theory* is widely used to analyze the effects of selecting alternative strategies to achieve a military objective (Shubik and Weber 1981). Games are used for planning, education, and for generating knowledge. Penetration testing ("red teaming") is conducted to seek out technical and structural weaknesses in computer systems, and for studying attack approaches and consequences of attacks.

Paté-Cornell and Guikema (2002) presents a model based on probabilistic risk analysis, and elements of game theory, for setting priorities among threats and among countermeasures. Bell (2003) studies the vulnerability of networks, and a game is set up between a router, who seeks to minimize the travel cost for data packets (or vehicles) by choosing routes in the net-

work, and an antagonist, who seeks to maximize the travel cost by destroying edges. Bier et al. (2005) apply elements of game theory and network reliability analysis to identify optimal strategies for allocating resources to defend idealized systems against attacks.

In Holmgren et al. (2006), the interaction between an attacker and a defender of a power system is modeled as a game. In a numerical example (using a maximum-flow lossless network model for calculating the consequences of attacks), the performance of different defense strategies against a number of attack scenarios is studied. An attack results in disabled elements in the network, which in turn may lead to loss of power for users (sink vertices). The total consequence of an attack is measured as the energy loss (MWh), which is approximated as the power loss multiplied with the recovery time.

In the model, the defender can only spend resources on increasing the component protection (e.g. fortification), and/or decreasing the recovery time after an attack (e.g. repair teams), i.e. the defense budget $c_{\text{total}} = c_{\text{prevent}} + c_{\text{recovery}}$. Every element i (vertices and edges) in the network has a protection described by the parameter p_i. This parameter corresponds to the probability that an attack against element i fails. The protection p_i of element i is a function of the resources c_i spent on protecting that element. The defender distributes the resources for protection between the N elements in the network. The repair time of element i depends on the resources spent on recovery, as well as the type of the disabled element, and the attack method. In the model, it is assumed that the defender has a basic recovery capacity for maintenance and for repairing minor failures. Thus, the relative contribution of spending extra resources on recovery is studied. In summary, the total allocation of defense resources is described by the vector $\mathbf{c} = (c_1,\ldots, c_N, c_{\text{recovery}})$.

The attack model only considers qualified antagonists. That is, determined, well-informed, and competent antagonists with access to enough resources to perform a successful attack against an electric power system. The antagonist is allowed to randomize between which targets to attack, and r_j correspond to the probability that target j is attacked (a target can consist of more than one element in the network), given that an attack is made. The vector $\mathbf{r}$ of dimension M then describes the mixed strategy, and three different classes of attack strategies are considered:

- *Worst-Case Attack:* The antagonist chooses the target that maximizes the expected negative consequences of the attack.
- *Probability-Based Attack:* The antagonist tries to maximize the probability that the outcome of an attack is over a certain magnitude q, i.e. $P(Q > q)$.

- *Random Attack:* The antagonist chooses the attack target randomly, and each target is attacked with equal probability.

An attack scenario is constructed by specifying the class of attack strategy, and a few additional parameters that captures tactics and modes of operation. The aim is to make the attack scenario more realistic by adding a few conditions and restrictions (e.g. regarding the amount of damage that can be inflicted to the targeted elements)

The interaction between the defender and the antagonist is described as a two-player zero-sum game, where, simultaneously, the defender chooses an allocation of defense resources, and the antagonist chooses a target to attack. Consequently, it is assumed that the defender's payoff is the negative value of the attacker's payoff. The situation where the attacker tries to maximize and the defender tries to minimize the total expected damage can, thus, be translated into an optimization problem. The game theory model has deliberately been kept simple, and it is assumed that both players have perfect information about the system, and the resources and preferences of the other.

In a simple numerical example (using a stylized version of the national Swedish transmission network) the performance of different defense strategies against a number of attack scenarios is studied. For this example, it is possible to find an optimal allocation between protection and recovery for the given scenarios (Fig. 3.4). This allocation depends on the total amount of resources c_{total} and the attack scenario. During an extreme situation there are more elements whose failure will cause large negative consequences compared to the normal situation. As a result, in this situation it is more effective to spend a larger proportion of the resources on recovery than during the normal situation.

It is not possible to find a *dominant defense strategy* in the numerical example. That is, a defense strategy with lower expected negative consequence than every other defense strategy against every attack scenario. A defense optimized against the Worst-Case Attack strategy will not necessarily provide an optimal defense against other attack scenarios (e.g. a scenario involving a Probability-Based Attack strategy). It is possible to use a number of statistical methods to give a ranking of the different defense strategies, and a few different ways of comparing the different defense strategies against each other are discussed in the paper.

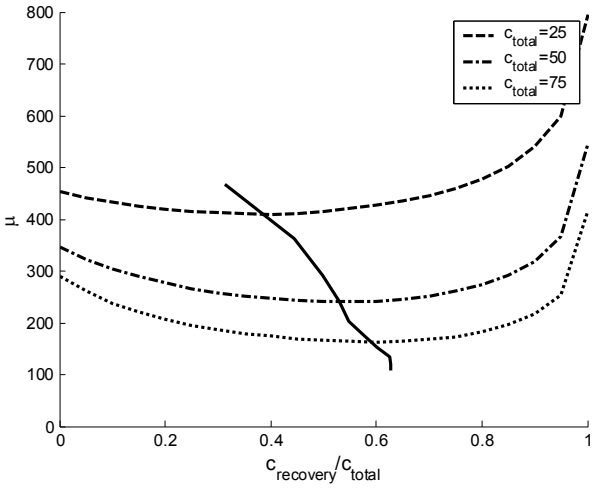

Fig. 3.4 Numerical example from a game theoretic vulnerability analysis model presented in Holmgren et al. (2006). The figure shows the balance between resources for protection and recovery for a given pair of defense and attack scenarios. The dotted lines display the expected negative consequences μ for three different total amount of resources c_{total} as a function of the fraction $c_{\text{recovery}}/c_{\text{total}}$. The solid line shows the optimal distribution between protection and recovery for different budgets c_{total}, i.e. the minimum of the dotted lines. Extra calculations have been made to find the optimal distribution for c_{total} between the horizontal lines.

In conclusion, it is well known that theoretical results in game theory depend significantly on how the game situation is modeled (the set of players, the set of strategies for each player, the choices that each player can make, the set of payoffs corresponding to the utility each player can receive etc.). Modeling antagonistic attacks against infrastructures, the information is very limited, and it becomes difficult to exactly specify the structure of the game. However, the author believes that using concepts and general models from game theory is a very powerful way of framing the problem.

3.8 Vulnerability Evaluation

3.8.1 Vulnerability Evaluation Criteria and Strategic Options

The *vulnerability evaluation* (compare with Fig. 3.1) can be based on different decision criteria:

- *Technology* based criteria (e.g. best practice or best available technology)
- *Right* based criteria (e.g. formulated in prescriptive standards or regulations given as quantitative limits)
- *Utility* based criteria (e.g. cost-benefit/cost-effectiveness analysis).
- *Combination* criteria

If the level of vulnerability cannot be accepted, there are several strategic options. It might be possible to avoid, or prohibit, certain activities (*avoidance*), or a choice, intentional or unintentional, can be made not to take any actions at all (*retention*). That is, to bear potential negative consequences within the normal activities. Further, actions or measures improving the protection of the infrastructure can be employed (*reduction*). The responsibility can also be transferred to another entity (*distribution*), e.g. via insurance, or a combination of retention and transfer (*sharing*) can be used, e.g. forming joint ventures.

An infrastructure operator might face threats with a potential of causing extremely large negative societal consequences. In a commercial contract, events such as these can be covered by a *Force Majeur* clause (if the event, and its effects, is considered to be outside the operator's possibility to control, the operator might be relieved of further responsibility). To ensure the survival of the company, and to hedge against commercial loss, a private infrastructure operator might use some insurance solution. However, to fill the gap between national security and risk management in private organizations, some form of *public commitment* is often required.

3.8.2 Options for Electric Power Systems Protection

Crisis management consists of a number of phases, for example: prevent, mitigate, response, recover, and learn. Measures for the *prevention* of failures and attacks aims at reducing the likelihood, or avoiding, that an event occurs. *Mitigation* aims at minimizing the negative consequences of an event. *Response* includes measures performed during the acute crisis phase in order to minimize the negative consequences of an event. Finally, *recovery* involves all measures carried out to bring back the system to a normal state after an event.

A general principle can be to first try to prevent a systems from degenerating into alert and emergency states, but if this does occur, it is important to minimize the disturbance, and restore normal conditions as quickly as possible. However, to prevent major power disturbances is generally considered to be complicated, and requires substantial resources. For ex-

ample, the Swedish transmission grid consists of some 15 000 km of overhead power lines, localized mainly in rural and uninhabited areas. Thus, it is *not* economically, or technically, achievable to fully eliminate the vulnerability of the Swedish power system in relation to antagonistic attacks. Consequently, for some threats, the solution can be to allocate more resources to response and recovery (compare with Sect. 3.7).

Prevention and Mitigation

Some general tactics for *prevention* and *mitigation* are: barriers (to confine/restrict a condition with potential for harm); redundancy (to improve system availability through additional, identical, components); diversity (applied to equipment, functions, and staff); training, quality control, and procedures review; preventive maintenance; monitoring, surveillance, testing and inspection (Parry 1991).

Electric power transmission grids are commonly designed and operated according to the deterministic "*N* - 1 Criterion". That is, the whole system must be capable of operating normally even when a major failure occurs. Measures to avoid failures in technical systems have traditionally been concerned with the safety perspective, but the tactics listed above are also suitable for creating physical security. Also, there is a variety of security mechanism that is designed to detect, prevent, or recover from a cyber attack, e.g. firewalls, Intrusion Detection Systems, and anti virus software.

Response and Recovery

The response to a power outage can be based on the same principles as normal electric power system operations. The *emergency control* involves automatic countermeasures to cope with instabilities in the power grid (e.g. load shedding can be implemented to manage loss of power generation), and the use of system monitoring tools (computer based early-warning systems) to keep the system from degenerating further.

Power systems *restoration* includes determining the detailed state of the system, preparing the equipment for restoration to service, reintegrating and rebuilding the system, and balancing generation and load as they, in a controlled manner, are brought back to their normal level. A general tactical choice is between the "build-down" approach (i.e. reenergizing the bulk power network before resynchronizing most generators), and the "build-up" approach (i.e. restoring islands that will then be mutually interconnected). The "build up" approach is more common and usually selected in a scenario involving a complete system collapse (Ancona 1995; Adibi and Fink 1994).

3.9 Concluding Remarks

The crisis management of large-scale power outages demands coordinated actions between countries, and is therefore of interest to the international community. The process will involve stakeholders both from public and private organizations. Even though the transnational terrorism and the cyber threats are alarming, major blackouts in recent years show that adverse weather and technical failures need consideration.

Critical infrastructure protection demands a holistic view; both technical and non-technical factors are of great importance. Thus, a vulnerability assessment methodology based on *multiple perspectives* is recommended. *Proactive work* is needed in order to assure that the infrastructure systems will be able to supply the services that a modern society relies on. A general principle can be first to try to prevent the systems from degenerating into alert and emergency states, but if this does occur, it is important to minimize the extent of the disturbance, and restore normal conditions as quickly as possible.

The preferred vulnerability analysis approach depends on the *objective of the analysis*, but also on the *available information* about the system. The traditional risk analysis offers a toolbox of well-established quantitative methods, and can to some extent be used to analyze the vulnerability of the technical systems that form the infrastructure. However, recent advances in network modeling and simulation, and also game theoretical approaches, should be taken into account.

Even if a systematic vulnerability assessment is conducted, decisions on critical infrastructure protection will involve a great deal of *uncertainty*. Commonly proposed solutions are to take decisions successively (i.e. using *adaptive strategies*), and to develop the *ability to act on unexpected situations* as they emerge (e.g. through the use of games as a learning and planning tool). Other recommendations are that uncertainties relevant to decision situations should be made explicit and understandable to the decision makers, and that a vulnerability assessment should include some form of *sensitivity analysis*.

Acknowledgements

The author would like to thank the following persons for valuable discussions and comments: T. Thedéen, S. Molin, L.-G. Mattsson, S. Arnborg, H. Christiansson, E. Jenelius, and J. Westin.

Financial support from the Swedish Emergency Management Agency (contract no. KBM 0054/2002) is gratefully acknowledged.

References

Adibi MM, Fink LH (1994) Power system restoration planning. IEEE Transactions on Power Systems 9: 22–28

Albert R, Barabási A-L (2002) Statistical mechanics of complex networks. Reviews of Modern Physics 74: 47–97

Albert R, Albert I, Nakarado GL (2004) Structural vulnerability of the North American power grid. Physical Review E 69: 025103(R)

Albert R, Jeong H, Barabási A-L (2000) Error and attack tolerance of complex networks. Nature 406: 378–381

Amaral LAN, Scala A, Barthélemy M, Stanley HE (2000) Classes of small-world networks. Proceedings of the National Academy of Sciences 97: 11149–11152

Ancona JJ (1995) A framework for power system restoration following a major power failure. IEEE Transactions on Power Systems 10: 1480–1485

Bell MGH (2003) The use of game theory to measure the vulnerability of stochastic networks. IEEE Transactions on Reliability 52: 63-68

Bier WM, Nagaraj A, Abhichandani V (2005) Protection of simple series and parallel systems with components of different values. Reliability Engineering & System Safety 87: 315-323

Carreras BA, Newman, DE, Dobson I, Poole AB (2000) Initial evidence for self-organized criticality in electric power system blackouts. Proceedings of the 33rd Hawaii International Conference on System Sciences, Hawaii

Carreras BA, Lynch VE, Dobson I, Newman DE (2004a) Complex dynamics of blackouts in power transmission systems. Chaos 14: 643-652

Carreras BA, Newman DE, Dobson I, Poole AB (2004b) Evidence for self-organized criticality in a time series of electric power system blackouts. IEEE Transactions on Circuits and Systems--I: Regular papers 51: 1733-1740

Chen J, Thorp J, Parashar M (2001) Analysis of electric power system disturbance data. Proceedings of the 34th Hawaii International Conference on System Sciences, Hawaii

Crucitti P, Latora V, Marchiori M (2004a) Model for cascading failures in complex networks. Physical Review E 69: 045104(R)

Crucitti P, Latora V, Marchiori M (2004b) A topological analysis of the Italian electric power grid. Physica A 338: 92–97

Dobson I, Carreras BA, Newman DE (2005) A loading-dependent model of probabilistic cascading failure. Probability in the Engineering and Information Sciences 19: 15-32

Dobson I, Carreras BA, Newman DE (2004) A branching process approximation to cascading load-dependent system failure. Proceedings of the 37th Hawaii International Conference on System Sciences, Hawaii

DoE (2002a) Vulnerability assessment methodology: electric power infrastructure. U.S. Department of Energy (DOE), Washington DC

DoE (2002b) Energy infrastructure risk management checklists for small and medium sized facilities. U.S. Department of Energy (DOE), Washington DC

Doorman GL, Uhlen K, Kjølle GH, Huse ES (2006) Vulnerability analysis of the Nordic Power System. IEEE Transactions on Power Systems 21: 402-410

Dorogovtsev SN, Mendes JFF (2002) Evolution of networks. Advances in Physics 51: 1079–1187

Einarsson S, Rausand M (1998) An approach to vulnerability analysis of complex industrial systems. Risk Analysis 18: 535–546

Gell-Mann M (1997) The simple and the complex. In: Alberts D, Czerwinski T (eds) Complexity, global politics, and national security. National Defense University, Washington, DC

Hansson SO, Helgesson G (2003) What is stability? Synthese 136: 219–235

Holme P, Kim BJ, Yoon CN, Han SK (2002) Attack vulnerability of complex networks. Physical Review E 65: 056109

Holmgren ÅJ (2006) Using graph models to analyze the vulnerability of electric power networks. Risk Analysis 26: 955–969

Holmgren ÅJ, Molin S (2005) Using disturbance data to assess vulnerability of electric power delivery systems. To appear (accepted October 2005) in Journal of Infrastructure Systems

Holmgren ÅJ, Thedéen T (2006) Structural vulnerability analysis of electric power networks. Submitted manuscript

Holmgren ÅJ, Jenelius E, Westin J (2006) Optimal defense of electric power networks against antagonistic attacks. To appear (accepted October 2006) in IEEE Transactions on Power Systems

Høyland 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

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

McEntire DA (2005) Why vulnerability matters: exploring the merit of an inclusive disaster reduction concept. Disaster Prevention and Management. 14: 206-222

Milano F (2005) An open source power system analysis toolbox. IEEE Transactions on Power Systems 20: 1199-1206

Motter AE, Lai Y-C (2002) Cascade-based attacks on complex networks. Physical Review E 66: 065102

Paté-Cornell E, Guikema S (2002) Probabilistic modeling of terrorist threats: a systems analysis approach to setting priorities among countermeasures. Military Operations Research 7: 5-20

Parry GW (1991) Common cause failure analysis: a critique and some suggestions. Reliability Engineering & Systems Safety 34: 309–326

Rosato V, Bologna, S, Tiriticco F (2006) Topological properties of high-voltage electrical transmission networks. Electric Power Systems Research (in Press)
Salmeron J, Wood K, Baldick R (2004) Analysis of electric grid security under terrorist threat. IEEE Transactions on Power Systems 19: 905-912
Shubik M, Weber RJ (1981) Systems defense games: Colonel Blotto, Command and Control, Naval Research Logistics Quarterly 28: 281-287
Simon HA (1962) The architecture of complexity. Proceedings of the American Philosophical Society 106: 467–482
UCTE (2003) Interim report of the investigation committee on the 28 September blackout in Italy. The Union for the Co-ordination of Transmission of Electricity (UCTE), Brussels
U.S.-Canada Task Force (2004) Final report on the August 14th 2003 blackout in the United States and Canada: causes and recommendations. U.S.-Canada Power System Outage Task Force
Watts DJ, Strogatz SH (1998) Collective dynamics of 'small-world' networks. Nature 393: 440–442
West DB (2001) Introduction to graph theory. Prentice Hall, Upper Saddle River
White House (2002) The national strategy for homeland security. Washington DC