Chapter 4
Basic Approaches

The two main outputs of a vulnerability assessment of critical infrastructures (CIs) are the quantification of system vulnerability indicators and the identification of critical elements (Chap. 2). The information they provide is complementary: while vulnerability indicators are parameters encompassing the static and/or dynamic characteristics of the whole system, the identification of critical elements comes from their ranking with respect to their individual connectivity efficiency and/or their contributions to the propagation of failures, with their effects, through the network.

A number of approaches can be undertaken for the vulnerability assessment of CIs depending on the type of system, the objective of the analysis and the available information. In this chapter, an attempt is made to defining the characteristics of these approaches, framed into categories of homogeneity (Table 4.1, including references), and to explaining them briefly. Those methods regarded as most important or promising by the authors and little described in the literature are explained in detail in Chap. 6.

4.1 Statistical Analysis

The extensive and growing use of information and telecommunication (IT) systems to capture data about CIs operation and performance (e.g., traffic delays in a transportation system, loss of power in an electric power network and signs of electronic intrusion in a banking system) provides rich data sets which can support vulnerability analyses. However, using these data effectively is difficult for a number of reasons: (i) data about CIs operation and performance generally come from a variety of past operating conditions that may not fully reflect the situations of interest at present and in the future; (ii) the relationships between the measures of the operating conditions (e.g., the loads placed on the different portions of the system) and system performance may be complicated and poorly understood; (iii) the data sets may be very large, making it difficult to draw clear insights

W. Kröger and E. Zio, *Vulnerable Systems*, DOI: 10.1007/978-0-85729-655-9_4,

Table 4.1 Categorization of the approaches for the vulnerability assessment of CIs

Approaches		Assessment steps			Outputs		Practical objectives		
	Techniques	Logic structure identification	(Inter)dependencies identification and modeling	Cascading failure analysis	System vulnerability indicators	Critical elements	Design optimization	Operation optimization	Interdiction/ protection optimization
Statistical analysis	Statistical models	No: aggregate data considered (Dekker 2005; Yamijala et al. 2009; Debon et al. 2010); different statistical models for different scenarios (Lord et al. 2005)	No	No	Yes (Dekker 2005; Yamijala et al. 2009; Debon et al. 2010)	Yes: identification of the critical parameters (Debon et al. 2010)	Yes (Debon et al. 2010)	No	No
Probabilistic modeling	Markov chains	Yes: but require enumeration of all possible combinations of components' states (Iyer et al. 2009)	No: single infrastructures are considered as monolithic entities (Sultana and Chen 2009)	Yes (Iyer et al. 2009)	Yes (Iyer et al. 2009; Guida et al. 2010)	Yes: severity of distur-bances can be obtained (Augutis et al. 2010)	No	No	No
	Markov/Petri nets	Yes: when combined with network structure (Langeron et al. 2010)	Yes: but only high level qualitative analysis (Krings and Oman 2002; Laprie et al. 2007; Sultana and Chen 2009)	No: high level qualita-tive analysis (Laprie et al. 2007)	Yes (Langeron et al. 2010)	No	No	No	No
	Probabilistic dynamics modeling	No: analytical model (Watts 2002; Dobson et al. 2005)	Yes (Newman et al. 2005)	Yes (Coffman et al. 2002; Buzna et al. 2007)	Yes (Dobson et al. 2004)	Yes: identification of the critical parameters (Coffman et al. 2002; Chen et al. 2005)	No	No	Yes (Chen et al. 2005; Buzna et al. 2007; Anghel et al. 2007)
	Bayesian networks	Yes (Doguc and Ramirez-Marquez 2009)	No	No	Yes (Doguc and Ramirez-Marquez 2009)	No	No	No	No

(continued)

Table 4.1 (continued)

Approaches		Assessment steps			Outputs		Practical objectives		
	Techniques	Logic structure identification	(Inter)dependencies identification and modeling	Cascading failure analysis	System vulnerability indicators	Critical elements	Design optimization	Operation optimization	Interdiction/ protection optimization
Risk analysis, hazop, FMEA	Quantitative assessment (PSA)	Yes (Apostolakis and Lemon 2005; Koonce et al. 2008)	Yes (Apostolakis and Lemon 2005)	Yes: using load flow simulation (Koonce et al. 2008)	Yes (Paté-Cornell and Guikema 2002; Apostolakis and Lemon 2005)	Yes (Koonce et al. 2008)	No	No	Yes (Paté-Cornell and Guikema 2002; Flammini et al. 2009)
	Tabular methods/ expert judgment	Yes (Moore 2006; Piwowar et al. 2009)	Partially: qualitatively (Moore 2006)	No	Yes: qualitatively (Moore 2006)	Yes: qualitatively (Moore 2006)	No	No	Yes (Moore 2006)
Complex network theory		Yes: topological structure analysis (Albert et al. 2000; Strogatz 2001; Crucitti et al. 2006; Rosato et al. 2007; Zio et al. 2008)	Yes (Dueñas-Osorio et al. 2007; Johansson and Jonsson 2009)	Yes (Motter and Lai 2002; Crucitti et al. 2004; Glass et al. 2004; Kinney et al. 2005)	Yes (Latora and Marchiori 2001; Chassin and Posse 2005; Zio et al. 2008)	Yes (Latora and Marchoiri 2005; Cadini et al. 2009; Hines and Blumsack 2008; Johansson and Jonsson 2009; Zio et al. 2008)	Yes (Latora and Marchoiri 2005; Zio et al. 2008)	No	Yes (Motter 2004; Dueñas-Osorio and Vemuru 2009)
Agent-based modeling and simulation		Yes (Schläpfer et al. 2008)	Yes (Panzieri et al. 2004; Casalicchio et al. 2007)	Yes (Schläpfer et al. 2008)	Yes (Schläpfer et al. 2008)	Yes (Schläpfer et al. 2008)	No	No	No
Dynamic control system theory	Transfer function	Yes (MIA 2010)	Yes (MIA 2010)	No	Yes (MIA 2010)	No	No	No	No

from them. Moreover, the structure of the CI under analysis may be hidden by the fact that the data are often presented in an aggregate form (Dekker 2005; Debon et al. 2010) so that, for example, the propagation of cascading failures may not be properly accounted for. The wealth of statistical models available for the analysis of engineered systems (Lord et al. 2005) can also be a drawback, in that a proper choice must be made of the most suitable model for the specific CI which best fits the physics of the provided service. In this sense, special emphasis must be put on comparing the accuracy and usefulness of the models by means of goodness of fit statistics.

Statistical models of differing complexity have, for example, been suggested in the literature for predicting pipe breaks in water distribution systems, from proportional hazard models (PHMs) to accelerated lifetime models (ALMs), to generalized linear models (GLMs) (Debon et al. 2010). These models were designed to show the impact on the CI of each variable describing the failure of an individual component. The "Cox regression model", also called PHM or duration model, is designed to analyze the time lapse until an event occurs or between events. One or more predictor variables, called covariates, are used to predict a status (event). The PHM has been widely used in analyzing survival data of components, for reliability modeling purposes (Cox 1972). ALMs are designed to analyze what influence the covariates have on the component failure time; they can be viewed as analogous to the PHMs; but, while in the ALMs the covariates act on the time to failure, in the PHMs it is the failure hazard that is affected by the covariates (Kleiner and Rajani 2001). GLMs are an extension of linear models for non-normal distributions of the response variable and non-linear transformations. A regression model constitutes a specification for the variable mean in terms of a small number of unknown parameters corresponding to the covariates. A GLM provides a method for estimating a function of the mean of the response variable as a linear combination of the set of predictive variables (McCullagh and Nelder 1989).

These statistical techniques have been proposed as tools for decision support in the diagnosis and rehabilitation of CIs, e.g. water supply systems (Yamijala et al. 2009), with the additional aim of identifying the systems most critical parameters.

However, criticality ranking of the systems components is not possible by resorting to statistical techniques only, because the data are typically presented in an aggregate form and no identification of the topological structure is accounted for.

4.2 Probabilistic Modeling

This approach encompasses a variety of methods used for the characterization of CIs, such as Markov chains (MCs), Markov/Petri nets (MPNs), probabilistic dynamics modeling and Bayesian networks (BNs).

MCs and MPNs rely on the definition of probabilities of transition of the system components among their reachable states; this may pose significant challenges because of the exponential growth in the number of CI configurations to be evaluated (Iyer et al. 2009). The behavior of a CI is described by its states and by

the possible transitions between these states. The system states are defined by the states of the components comprising the system. The components are not restricted to having only two possible states but rather may have a number of different states, such as functioning, in standby, completely failed and under maintenance. The various failure modes of a component may also be defined as states. However, if the system is made by several multi-state components, the number of system states increases rapidly. The state-space representation of the system behavior is, therefore, suitable only for relatively small systems. The possible transitions between the states are illustrated with the aid of a state-space diagram also known as a Markov diagram. The transitions are caused by various mechanisms and activities such as failures, repairs, replacements and switching operations. Complicated repair and switching strategies, common cause failures and other realistic aspects of system behavior can be included in the state-space model. Mathematical modeling of systems suffering from cascading failures propagation has been developed using a continuous-time Markov chain (CTMC) model of a CI operating in a randomly changing environment and as probabilistic cascading failures (Iyer et al. 2009). Probabilistic cascading is considered in the sense that the failure of a component of type *i* causes a component of type *j* to fail simultaneously with a given probability, with all the failures in a cascade being mutually independent. The model includes an environment variable that changes as a CTMC, and this allows us to model randomly changing conditions under which the system operates. The model allows for the evaluation of vulnerability indicators such as the unavailability and mean-time-to-failure (MTTF) of the service provided by the CI.

Probabilistic dynamics models can be considered to overcome the computational limitations of the previous methods; yet, their analysis is affected by the drawback that the identification of the system logical structure is not accounted for (Watts 2002; Dobson et al. 2005). Also, probabilistic dynamics models allow accounting for (inter)dependencies and interactions among several CIs (Newman et al. 2005), while MCs and MPNs have been typically used to analyze isolated systems, or to analyse the (inter)dependencies only for high level qualitative analysis (Sultana and Chen 2009). In the latter case, the actions and the effects of the (inter)dependencies among these CIs are postulated by the analyst at the global CI scale, and do not emerge as the result of the local (inter)dependencies among components of different CIs (Sultana and Chen 2009).

BN analysis is a probabilistic approach that can be used for modeling and predicting the behavior of a system, based on observed stochastic events. A BN is a model that represents the interactions among the components in a system, from a probabilistic perspective. The representation is illustrated via a directed acyclic graph, where the nodes represent the variables and the links between each pair of nodes represent the causal relationships between the variables. From a network reliability perspective, the variables of a BN are defined as the components in the network, while the links represent the interaction of the nodes leading to system ''success'' or ''failure''. A fundamental assumption for the construction of a BN is that in general, the strength of the interaction/influence among the graph nodes is uncertain, and thus this uncertainty is represented by assigning a probability of

existence to each of the links joining the different nodes. For non-trivial systems, i.e. systems not following a series, parallel or any combination of these configurations, the failure/success probability of a system usually depends on the failure/success of a non-evident collection of components. In a BN this dependency is represented as a directed link between two components, forming a child and parent relationship, so that the dependent component is called the child of the other. Therefore, the success probability of a child node is conditional on the success probabilities associated with each of its parents. The conditional probabilities of the child nodes are calculated by using the Bayes' theorem via the probability values assigned to the parent nodes. Also, the absence of a link between any two nodes of a BN indicates that these components do not interact for system failure/success, thus they are considered independent of each other and their probabilities are calculated separately. Holistic methods have been devised for constructing BN models for estimating the two-terminal reliability of abstract networks (i.e. the probability of a connection between a selected pair of source and target nodes in the network) (Doguc and Ramirez-Marquez 2009). BNs have also been shown useful in assessing the probabilistic relationships and identifying probabilistic mappings among the components of a CI. Methods exist that use historical data about the system to be modeled as a BN and provide for the automated construction of the BN model. In this respect, data mining algorithms are used for finding associations between system components, and thus building the BN model. These algorithms use a heuristic to provide efficient and accurate results while searching for associations.

4.3 Risk Analysis

This approach can be divided into two lines of analysis: the first entails the qualitative assessment of system vulnerabilities by expert judgment and tabular methods (Moore 2006; Piwowar et al. 2009), while the second entails the quantitative part (Apostolakis and Lemon 2005; Flammini et al. 2009), with the further aim of ranking systems elements according to their criticality and of assessing their cascade failure dynamics (Koonce et al. 2008). To a certain extent, the risk analysis approach to the vulnerability of CIs can be considered a general framework of analysis, since it often takes advantage of other approaches and tools, i.e. power flow analysis for electrical transmission networks (Koonce et al. 2008) and network analysis (Apostolakis and Lemon 2005).

Methods such as fault tree (FT) and event tree (ET) analysis as core methods of probabilistic risk assessment (PRA) have been applied to the vulnerability analysis of CIs for protecting the systems against malevolent actions (Piwowar et al. 2009). The approach comprises a step-by-step process typical of PRA : (1) systemic analysis, in which the system itself and its surroundings are analyzed to identify all the parameters that could interact with it; (2) analysis of the interactions between aggressors' profiles and systems, in which the systems are ranked according to the degree of risk of being attacked; (3) assessment of vulnerabilities and

determination of key points of vulnerability, in which a panel of subject matter experts and a PRA process normative expert conduct a study and weigh the importance of the system elements to qualify them according to several criteria concerning the attack; (4) building of scenarios, taking into account system functionalities, the global environment, and the geopolitical context; (5) updating the security systems, considering the results of the previous steps.

Yet, the approach presents some inconveniences related to the size of the distributed system to analyze, the number of scenarios of attack to be considered, the human subjectivity as a base for all the quantifications to assess vulnerabilities on a given CI, and the needs to be updated frequently, because of the evolving geopolitics and the introduction of new factors in the whole system (a new apparel, new ways of productivity, new entrance or exit points, etc.).

A risk-based quantitative method for the identification and prioritization of vulnerabilities in interdependent CIs has been proposed in (Apostolakis and Lemon 2005). The CI is modeled as interconnected digraphs and the graph theory is employed to identify the candidate vulnerable scenarios. These scenarios are screened for the susceptibility of their elements to a terrorist attack, and a prioritized list of elements vulnerabilities is produced. The prioritization methodology is based on multi-attribute utility theory (Morgan et al. 2000). The impact of losing infrastructure services is evaluated using a value tree that reflects the perceptions and values of the decision maker and the relevant stakeholders. These results, which are conditional on a specified threat, are provided to the decision maker for use in risk management. Interestingly, this method embeds the vulnerability quantification into the framework of the stakeholders' perspective, making it suitable for a realistic ranking of vulnerabilities in CIs.

To account for cascading failure propagation in CIs, the previous method has been extended and applied to the risk analysis of a bulk power system (Apostolakis and Lemon 2005). The analysis was complemented with a power flow simulation model to determine the likelihood and extent of power outages, when components within the system fail to perform their designed functions due to both random causes and malevolent acts. The consequences associated with these failures are determined by looking at the type and number of customers affected; stakeholder input is used to evaluate the relative importance of these consequences. The methodology provides a ranking of each system component by its risk significance to the stakeholders.

4.4 Complex Network Theory

Complex network theory methods can be applied to the analysis of CIs for (a) helping to identify preliminary vulnerabilities by topology-driven and dynamical analyses and (b) guiding and focusing further detailed analyses of critical areas.

The interconnection structure of a CI can be represented by an unweighted network, where the edges (arcs) between nodes are either present or not. The topological analysis of the corresponding representative graphs has received a

renewed enthusiasm from the works of Strogatz and Barabási, who pointed at the presence of a "selective pressure" able to determine a common growth mechanism in a number of diverse evolving complex systems (from those representing technological systems to those related to biological and social networks; Watts and Strogatz 1998; Jeong et al. 2001). Such a growth mechanism determines the development of structures toward a class of mathematical graphs labeled as "scale-free". It has been shown that those network structures possess considerable robustness against random faults but large vulnerability to deliberate attacks, with respect to randomly grown networks (Albert et al. 2000). On the practical side, it has also been shown that, quite often, large technological infrastructures do not show a clear scale-free structure, mainly due to technological constraints which limit the arbitrary growth of the nodes degrees (i.e. the number of connections pointing to the nodes) (Amaral et al. 2000).

Topological analysis based on classical graph theory can unveil relevant properties of the structure of a network system (Albert et al. 2000; Strogatz 2001) by (i) highlighting the role played by its components (nodes and connecting arcs) (Crucitti et al. 2006; Zio et al. 2008), (ii) making preliminary vulnerability assessments based on the simulation of faults (mainly represented by the removal of nodes and arcs) and the subsequent re-evaluation of the network topological properties (Rosato et al. 2007; Zio et al. 2008). In a topological analysis, a CI is represented by a graph G(N, K), in which its physical constituents (components) are mapped into N nodes connected by K unweighted edges, representing the links of physical connection among them. The focus of topological analysis is on the structural properties of the graphs on the global and local scales, e.g., as represented by their characteristic path length, L, defined as the number of arcs in the shortest path between two nodes averaged over all pairs of nodes, and average clustering coefficient, C, a measure of the extent to which nodes tend to form small groups (Watts and Strogatz 1998). Average global measures, such as L, give indications on the extent to which each node in the system is connected with any other nodes, while average local measures, like C, assess to what extent the first neighbors of each node are connected among each other. In spite of the usefulness of the topological analysis of the unweighted network of a CI and of the insights it provides, empirical results show that it cannot capture all rich and complex properties observed in real CIs, so that there is a need for extending the models beyond pure unweighted, structural topology (Boccaletti et al. 2006; Eusgeld et al. 2009).

Indeed, along with a complex topological structure, many real networks display a marked physical heterogeneity in the capacity and intensity of the connections. Examples are different impedance and reliability characteristics of overhead lines in electrical transmission networks (Hines and Blumsack 2008; Eusgeld et al. 2009), unequal traffic on roads which affects accident probability (Zio et al. 2008) or different routing capacities of the Internet links (Latora and Marchoiri 2005). To describe such heterogeneities numerical weights can be assigned to each link of the representative network, measuring the "strength" of the connection. In this way, the functional behavior of the CI is somewhat embedded into a generalized, but still simple, topological analysis framework. Global and local measures

can then be introduced for the statistical characterization of weighted networks (Latora and Marchiori 2001).

Further, in real network systems, another important dimension to add to the vulnerability characterization is the dynamics of flow of the physical quantities in the network. From the analysis point of view, this entails considering the interplay between structural characteristics and dynamical aspects, which makes the modeling very complicated since the load and capacity of each component, and the flow through the network are often highly variable quantities both in space and time. Functional models have been developed to capture the basic realistic features of CI networks within a weighted topological analysis framework, i.e. disregarding the representation of the individual dynamics of the CIs elements. These models have shed light on the way complex networks react to faults and attacks, evaluating their consequences when the dynamics of flow of the physical quantities in the network is taken into account. The response behavior often results in a dramatic cascade phenomenon due to avalanches of node breakings (Motter and Lai 2002; Motter 2004; Zio and Sansavini 2008). Abstract modeling paradigms for analyzing the system response to cascading failures have been introduced to guide successive detailed simulation focused on the most relevant physical processes and network components (Motter and Lai 2002; Motter 2004; Dobson et al. 2005; Zio and Sansavini 2008). Despite their apparent simplicity, these models provide indications on the elements criticality for the propagation process (Zio and Sansavini 2011a) and on the actions that can be performed in order to prevent or mitigate the undesired effects (Motter 2004). It is observed that improvements in network components alone do not ensure system robustness or protection against disproportionate cascading failures (Dueñas-Osorio and Vemuru 2009) instead, topological changes are needed to increase cascading robustness at realistic tolerance levels. Moreover, regardless of the nature of the events triggering the failure cascade, the additional loss of performance due to cascading failures can be orders of magnitude larger than the initial loss of performance.

Finally, the complex network theory models allow accounting for (inter)dependencies among different CIs, to assess the influences and limitations which interacting infrastructures impose on the individual systems operating conditions, for avoiding fault propagation by designing redundancies and alternative modes of operations, for detecting and recognizing threats (Zimmerman 2001; Dueñas-Osorio et al. 2007; Johansson and Jonsson 2009). In developing modeling and simulation frameworks that allow the coupling of interdependent infrastructures, it is important to know that simply linking existing infrastructure models together fails to capture the emergent behavior arising in interdependent CIs (Zio and Sansavini 2011b).

4.5 Agent-Based Modeling and Simulation

Agent-based modeling (ABM) has been shown to offer an attractive modeling paradigm for describing the dynamic system operational behavior, with close adherence

to the reality of the coupled processes involved (D'Inverno and Luck 2004). One of the major advantages of ABM for simulating CIs is the possibility to include physical laws into the simulation and to emulate the behavior of the infrastructure as it emerges from the behaviors of the individual agent and their interactions. In other words, the overall system behavior results from the interactions among the multiple single agents of different kinds which make up the system (Schläpfer et al. 2008). This modeling approach integrates the spectrum of different phenomena and mechanisms which may occur, thus generating a multitude of representative time-dependent event chains.

In order to include technical and non-technical factors and physical laws in the vulnerability assessment of a critical infrastructure, a two-layer approach can be deployed (Schläpfer et al. 2008). For example, an electric power system can be thought of as a stochastic hybrid system that can be modeled by a finite state machine (FSM) whose states involve continuous variables with uncertain dynamics; transitions in this machine correspond to outages of generation and transmission equipment. The conceptual modeling framework consists in the abstraction of the relevant components of the system as individual interacting agents. Agents are used to model both technical components (such as the electric power generators) and non-technical components (such as grid operators). The different agents interact with each other directly (e.g. generator dispatch) or indirectly, e.g. via the physical network. Each agent is modeled by attributes and rules of behavior. An example for an attribute is a technical component constraint such as the rating of a transmission line in the electric power system. The rules of behavior are represented by using FSM and include both deterministic and stochastic time-dependent, discrete events. A deterministic event is, for instance, the outage of a component when reaching a failure threshold, while stochastic processes are probabilistic component failure models simulated by Monte Carlo techniques (Billington and Li 1994; Marseguerra and Zio 2002).

ABM was used to assess the availability of bulk power systems for mid- and short-period power system planning purposes (Schläpfer et al. 2008). It was shown that the probability of cascading failures is subject to phase transitions and abrupt changes that result from only small changes in the system stress. The level of modeling detail offered by ABM allows analyzing a multitude of time-dependent availability aspects. Besides technical failures, other factors, such as natural hazards, institutional weaknesses or security-related issues can be integrated. The main problems are related to the slow simulation speed and the large number of parameters to be input in the analysis. However, by focusing on specific safety aspects, the model can be simplified and the computational burden reduced.

ABM is also a suitable approach to simulate interdependencies among CIs (Panzieri et al. 2004) by introducing interconnected agents: i.e., independent systems that autonomously elaborate information and resources in order to define their outputs; the latter become inputs for other agents, and so on (Luck et al. 2003). This approach is particularly useful for situations, as is the case of infrastructure interdependencies, with sparse or non-existent macro scale information; ABM is able to use the rich sources of micro-level data to develop interaction

forecasts. One disadvantage of these simulation models is that the complexity of the computer programs tends to obscure the underlying assumptions and the inevitable subjective inputs. Another disadvantage is the difficulty to acquire detailed information about each single infrastructure. This task appears, by its own, a difficult challenge, because this kind of information is considered very sensible by infrastructure stakeholders due to the relevance for their business. In Hopkinson et al. (2003), to partially overcome this problem, commercial simulators are integrated into a message-broker framework.

4.6 Dynamic Control System Theory

Dynamic control system theory can be applied as a quantitative analytical method to assess the (inter)dependencies among CIs using the transfer functions and the corresponding frequency responses (MIA 2010). In order to apply this method, studied infrastructure(s) need to be assumed as a linear time invariant (LTI) dynamic system.

The input/output relationship between infrastructures is able to be represented and quantified by deriving the transfer functions in the domain of Laplace (s) or the domain of frequency ($j\omega$). Mason's formula, a method determining the control function of a given control loop after identifying its corresponding signal flow graph, can be applied to define all the required transfer functions such as the transfer function for a component of one infrastructure or overall global transfer function. It should be noted that the overall transfer function is constituted by the composition of the transfer functions of each component. A final possible representation of the transfer function is in the form of poles/zeros:

$$G(s) = \frac{\mu \times \prod_j (s - z_j)}{s^g \times \prod_i (s - p_i)} \tag{4.1}$$

where $j =$ the number of zeros, $i =$ the number of poles (MIA 2010).

Based on the overall transfer function and its corresponding frequency responses, the stability of interdependencies between infrastructures can be evaluated using BODE and NYQUIST diagrams (MIA 2010).

The approach of the dynamic control system theory is a novel method, which brings the classic control system theory to the area of CI protection. Instead of using the time domain, two alternative domains (domain of Laplace and frequency) are used for the purpose of evaluation and assessment. The development of transfer functions is the most essential part of this approach and has strong influences on the accuracy of the final results, which could be further complicated due to the complexities of the studied infrastructures. Another drawback of this approach lies in the fact that hidden vulnerabilities caused by (inter)dependencies are not able to be estimated since all the links between studied infrastructures have been determined during the transfer function development. The applicability/feasibility of this approach is still under discussion and needs to be further proved.

References

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

Amaral LAN, Scala A, Barthélémy M, Stanley HE (2000) Classes of small-world networks. Proc Natl Acad Sci USA 97:11149–11152

Angel M, Werley A-K (2007) Stochastic model for power grid dynamics. In: Proceedings of the 40th Hawaii international conference on system sciences. January 3–6, 2007, Big Island, Hawaii

Apostolakis E-G, Lemon M-D (2005) A screening methodology for the identification and ranking of infrastructure vulnerabilities due to terrorism. Risk Anal 25(2):361–376

Augutis J, Krikštolaitis R, Šidlauskas K, Martišauskas L, Matuziene V (2010) Modeling of energy supply disturbances in network systems. In: Briš R, Guedes Soares C, Martorell S (eds) Reliability, risk and safety: theory and applications. Taylor and Francis, London

Billington R, Li W (1994) Reliability assessment of electric power systems using Monte Carlo methods. Plenum Press, New York

Boccaletti S, Latora V, Moreno Y, Chavez M, Hwang D-U (2006) Complex networks: structure and dynamics. Phys Rep 424:175–308

Buzna L, Peters K, Ammoser H, Kühnert C, Helbing D (2007) Efficient response to cascading disaster spreading. Phys Rev E 75(5):056107

Cadini F, Zio E, Petrescu C-A (2009) Using centrality measures to rank the importance of the components of a complex network infrastructure. In: Proceedings of CRITIS'08, 13–15 October 2008, Rome, Italy, pp 155–167

Casalicchio E, Galli E, Tucci S (2007) Federated agent-based modeling and simulation approach to study interdependencies in IT critical infrastructures. In: Proceedings of the 11th IEEE symposium on distributed simulation and real-time applications, Chania, Crete Island, Greece

Chassin P-D, Posse C (2005) Evaluating North American electric grid reliability using the Barabasi–Albert network model. Physica A 355:667–677

Chen J, Thorp S-J, Dobson I (2005) Cascading dynamics and mitigation assessment in power system disturbances via a hidden failure model. Int J Electr Power Energ Syst 27:318–326

Coffman E-G Jr, Ge Z, Misra V, Towsley D (2002) Network resilience: exploring cascading failures within BGP. In: Proceedings of the 40th annual Allerton conference on communications, computing and control, Monticello, Illinois, USA

Cox D (1972) Regression models and life tables (with discussion). J R Stat Soc Ser B 34(2): 187–220

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

Crucitti P, Latora V, Porta S (2006) Centrality in networks of urban streets. Chaos 16(1–9): 015113

D'Inverno M, Luck M (2004) Understanding agent systems. Springer, Berlin

Debon A, Carrion A, Cabrera E, Solano H (2010) Comparing risk of failure models in water supply networks using ROC curves. Reliab Eng Syst Saf 95:43–48

Dekker AH (2005) Simulating network robustness for critical infrastructure networks, conferences in research and practice in information technology. In: Estivill-Castro V (ed) Proceedings of the 28th Australasian computer science conference, the University of Newcastle, vol 38. Newcastle, Australia

Dobson I, Carreras BA, Lynch V, Newman DE (2004) Complex systems analysis of series of blackouts: cascading failure, criticality and self-organization, bulk power system dynamics and control—VI. Cortina d'Ampezzo, Italy, pp 438–451

Dobson I, Carreras BA, Newman DE (2005) A loading-dependent model of probabilistic cascading failure. Prob Eng Inform Sci 19:15–32

Doguc O, Ramirez-Marquez EJ (2009) A generic method for estimating system reliability using Bayesian networks. Reliab Eng Syst Saf 94:542–550

Dueñas-Osorio L, Vemuru S-M (2009) Cascading failures in complex infrastructure systems. Struct Saf 31:157–167

Dueñas-Osorio L, Craig IJ, Goodno JB, Bostrom A (2007) Interdependent response of networked systems. J Infrastruct Syst 13(3):185–194

Eusgeld I, Kröger W, Sansavini G, Schläpfer M, Zio E (2009) The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures. Reliab Eng Syst Saf 94(5):954–963

Flammini F, Gaglione A, Mazzocca N, Pragliola C (2009) Quantitative security risk assessment and management for railway transportation infrastructures. In: Proceedings of critical information infrastructure security, third international workshop, CRITIS 2008, Rome, Italy, October 13–15, 2008. Revised papers, LNCS, Vol. 5508. Springer-Verlag, Berlin, Heidelberg, pp 180–189

Glass JR, Beyeler EW, Stamber LK (2004) Advanced simulation for analysis of critical infrastructure: Abstract cascades, the electric power grid, and fedwire 1 (SNL paper SAND 2004-4239). Albuquerque, New Mexico 87185 and Livermore, California 94550

Guida M, Longo M, Postiglione F (2010) Reliability analysis of next generation mobile networks. In: Briš R, Guedes Soares C, Martorell S (eds) Reliability, risk and safety: theory and applications. Taylor and Francis, London

Hines P, Blumsack S (2008) A centrality measure for electrical networks. In: Proceedings of the 41st Hawaii international conference on system science, Big Island, Hawaii

Hopkinson K, Birman K, Giovanini R, Coury D, Wang X, Thorp J (2003) EPOCHS: integrated commercial off-the-shelf software for agent-based electric power and communication simulation. In: Proceedings of the 2003 winter simulation conference, New Orleans, LA, 7–10 December 2003, pp 1158–1166

Iyer MS, Nakayama KM, Gerbessiotis VA (2009) A Markovian dependability model with cascading failures. IEEE Trans Comput 58(9):1238–1249

Jeong H, Mason SP, Barabasi A-L, Oltvai ZN (2001) Lethality and centrality in protein networks. Nature 411:41–42

Johansson J, Jonsson H (2009) A model for vulnerability analysis of interdependent infrastructure networks. In: Martorell et al. (eds) Safety, reliability and risk analysis: theory, methods and applications. Proceedings of ESREL 2008 and 17th SRA Europe annual conference, 22–25 September 2008, Valencia, Spain, Taylor & Francis Group, London

Kinney R, Crucitti P, Albert R, Latora V (2005) Modeling cascading failures in the North American power grid. Eur Phys J B 46:101–107

Kleiner Y, Rajani B (2001) Comprehensive review of structural deterioration of water mains: statistical models. Urban Water 3(3):131–150

Koonce AM, Apostolakis GE, Cook BK (2008) Bulk power risk analysis: ranking infrastructure elements according to their risk significance. Int J Electr Power Energy Syst 30:169–183

Krings A, Oman P (2002) A simple GSPN for modeling common mode failures in critical infrastructures. In: Proceedings of the 36th annual Hawaii international conference on system sciences (HICSS'03), Big Island, Hawaii

Langeron Y, Barros A, Grall A, Bérenguer C (2010) Reliability assessment of network-based safety-related systems. In: Briš R, Guedes Soares C, Martorell S (eds) Reliability, risk and safety: theory and applications. Taylor and Francis, London

Laprie J-C, Kanoun K, Kaâniche M (2007) Modelling interdependencies between the electricity and information infrastructures. In: Proceedings of the 26th international conference on computer safety, reliability, and security (SAFECOMP 2007), Nuremberg, Germany, LNCS 4680/2009

Latora V, Marchiori M (2001) Efficient behavior of small-world networks. Phys Rev Lett 87(19):198701 (1–4)

Latora V, Marchoiri M (2005) Vulnerability and protection of infrastructure networks. Phys Rev E 71:015103 (1–4)

Lord D, Washington PS, Ivan NJ (2005) Poisson, Poisson-gamma and zero inflated regression models of motor vehicle crashes: balancing statistical fit and theory. Accid Anal Prev 37:35–46

Luck M, McBurney P, Preist C (2003) Agent technology: enabling next generation computing (A roadmap for agent based computing). AgentLink II. University of Southampton, Southampton, UK

Marseguerra M, Zio E (2002) Basics of the Monte Carlo method with application to system reliability. LiLoLe-Verlag GmbH, Hagen, Germany

McCullagh P, Nelder J (1989) Generalized linear models. Chapman & Hall, London

MIA (2010) Definition of a methodology for the assessment of mutual interdependencies between ICT and electricity generation/transmission infrastructures. Final report, September 2010, Italian National Agency for New Technology, Energy and Environment, Italy

Moore AD (2006) Application of the API/NPRA SVA methodology to transportation security issues. J Hazard Mater 130:107–121

Morgan MG, Florig HK, DeKay ML, Fischbeck P (2000) Categorizing risks for risk ranking. Risk Anal 20:49–58

Motter A-E (2004) Cascade control and defense in complex networks. Phys Rev Lett 93(9): 098701(1-4)

Motter A-E, Lai Y-C (2002) Cascade-based attacks on complex networks. Phys Rev E 66(1–4): 065102

Newman D-E, Nkei B, Carreras BA, Dobson I, Lynch VE, Gradney P (2005) Risk assessment in complex interacting infrastructure systems. In: Proceedings of the 38th Hawaii international conference on system sciences, Big Island, Hawaii

Panzieri S, Setolaand R, Ulivi G (2004) An agent based simulator for critical interdependent infrastructures. In: Proceedings of the 2nd international conference on critical infrastructures CRIS2004: October 25–27, 2004, Grenoble, France

Paté-Cornell ME, Guikema SD (2002) Probabilistic modeling of terrorist threats: a systems analysis approach to setting priorities among countermeasures. Mil Oper Res 7(3):5–23

Piwowar J, Chatelet E, Laclemence P (2009) An efficient process to reduce infrastructure vulnerabilities facing malevolence. Reliab Eng Syst Saf 94:1869–1877

Rosato V, Bologna S, Tiriticco F (2007) Topological properties of high-voltage electrical transmission networks. Electr Pow Syst Res 77:99–105

Schläpfer M, Kessler T, Kröger W (2008) Reliability analysis of electric power systems using an object-oriented hybrid modeling approach. In: Proceedings of the 16th power systems computation conference, Glasgow

Strogatz SH (2001) Exploring complex networks. Nature 410:268–276

Sultana S, Chen Z (2009) Modeling flood induced interdependencies among hydroelectricity generating infrastructures. J Environ Manage 90:3272–3282

Watts D-J (2002) A simple model of global cascades on random networks. Proc Natl Acad Sci USA 99(9):5766–5771

Watts D-J, Strogatz SH (1998) Collective dynamics of 'small-world' networks. Nature 39: 440–442

Yamijala S, Guikema DS, Brumbelow K (2009) Statistical models for the analysis of water distribution system pipe break data. Reliab Eng Syst Saf 94:282–293

Zimmerman R (2001) Social implications of infrastructure network interactions. J Urban Technol 8(3):97–119

Zio E, Sansavini G (2008) Modeling failure cascades in networks systems due to distributed random disturbances and targeted intentional attacks. In: Martorell et al. (eds) Safety, reliability and risk analysis: theory, methods and applications. Proceedings of ESREL 2008 and 17th SRA Europe annual conference, Valencia, Spain, Taylor & Francis Group, London, 22–25 September 2008,

Zio E, Sansavini G (2011a) Component criticality in failure cascade processes of network systems. Risk Anal. doi: 10.1111/j.1539-6924.2011.01584.x

Zio E, Sansavini G (2011b) Modeling interdependent network systems for identifying cascade-safe operating margins. IEEE Trans Reliab 60(1):94–101

Zio E, Sansavini G, Maja R, Marchionni G (2008) An analytical approach to the safety of road networks. Int J Reliab Qual Saf Eng 15(1):67–76