This article is part of the IEEE Reliability Society 2009 Annual Technology Report.

VULNERABILITY ASSESSMENT OF CRITICAL INFRASTRUCTURES

Enrico Zio
Politecnico di Milano
Email: enrico.zio@polimi.it

Wolfgang Kröger
Swiss Federal Institute of Technology Zurich (ETH)
Email: kroeger@mavt.ethz.ch

The welfare and security of modern nations rely on the continuous production and distribution of a number of essential goods (e.g. water, energy, data), and services (e.g. banking, health care), by large scale, man-made, networked systems, called *infrastructures*, mostly spanning long distances, and privately owned or operated. Such infrastructures are termed *critical*, as any incapacity or destruction would have a debilitating impact on our health, safety, security, economics, and social well being.

We offer a view on the concepts of vulnerability of *critical infrastructures* (CI), and the methods for its assessment. Such a view does not pretend to be complete nor exhaustive, but rather hopes to serve as a means for stimulating developments, and researches in this relevant field.

CI are various by nature, e.g. physically engineered, cybernetic, or organizational, and by environment/context, e.g. geo-spatial, political/legal, economic, etc. Physically engineered networked CI, often called *lifeline systems*, are the focus of interest here. Examples are those providing energy (electricity, oil & gas supply), transportation (rail, road, air, shipping), information and telecommunication (internet), and drinking water (including waste water treatment).

As shown by experienced events, CI are highly interconnected, and mutually dependent in complex ways, both physically and through a host of information and communication technologies. This leads to the concept of "systems-of-systems."

In general, the response behavior of single or interdependent CI to perturbations or stresses depends on the degree of coupling among elements within or between systems, e.g. loose or tight, and the coupling order. Identifying, understanding, and analyzing the interdependent features of CI are still major challenges, magnified by the breadth and complexity of most infrastructures.

For CI, the term vulnerability has been introduced as the hazard[1]-centric perception of disasters revealed being too limited to understand in terms of risks [1]. A hazard of low intensity could have severe consequences, while a hazard of high intensity could have negligible consequences; the level of vulnerability makes the difference [2].

The concept of vulnerability of technical systems has developed in three main steps, and finally focuses on three elements [3]:
- degree of loss, and damages due to the impact of a hazard;

[1] "A potentially damaging physical event, phenomenon and/or human activity, which may cause loss of life or injury, property damage, social and economic disruption, or environmental degradation. Hazards can be single, sequential, or combined in their origin and effects." [1]

- degree of exposure to the hazard, i.e., the likelihood of being exposed to hazards of a certain degree, and the susceptibility of an element at risk to suffer loss and damages; and
- degree of capacity of resilience[2], i.e., the ability of a system to anticipate, cope with or absorb, resist, and recover from the impact of a hazard or disaster (social).

An operational definition of vulnerability, useful for its systematic assessment, relates to the set of flaws and weaknesses in the design, implementation, operation, and/or management of an infrastructure system or its elements that renders it susceptible to destruction or incapacitation when exposed to a hazard or threat. The likelihood (frequency) of the accident scenarios, and the magnitude of their consequences can be evaluated through specific elaborations depending on the particular infrastructure considered. As an example, the vulnerability of the electric power system might be assessed in terms of the frequency of major blackouts (number per year), and associated severity (undelivered MW, or MWh). Reliability and availability of service or goods can also be used to describe the quality of infrastructure systems.

Fig. 1 presents a schematic conceptualization of the vulnerability assessment of a CI. The two main outputs of a CI vulnerability assessment are shown to be the quantification of system vulnerability indicators, and the identification of critical elements. A number of approaches can be undertaken for the vulnerability assessment of CI depending on the type of system, the objective of the analysis, and the available information.

As for statistical analysis, the extensive, growing use of IT systems to capture data about CI 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 CI 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; and iii) the data sets may be very large, making it difficult to draw clear insights 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 [4], [5] 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 [6] 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.

The probabilistic modeling approach encompasses a variety of methods that can be used for the characterization of CI, e.g. Markov chains (MC), Markov/Petri nets (MPN), probabilistic dynamics modeling, and Bayesian networks (BN). In MC and MPN, the behavior of a CI is described by its states, and by the possible transitions between these states. This model may pose

[2] Resilience generally means the ability to recover from some shock, insult, or disturbance, the quality or state of being flexible. In *physics and engineering*, it is defined as the physical property of a material that can return to its original shape or position after deformation that does not exceed its elastic limit, i.e. as its capacity to absorb energy when it is deformed, and then, upon unloading, to have this energy recovered. Regarding systems resilience, basically it is the potential to remain in a particular configuration, and to maintain its feedback and functions, and involves the ability of the system to reorganize following disturbance driven change [3].

significant challenges because of the exponential growth in the number of CI configurations to be evaluated [7].

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 [8], [9].

BN analysis is a probabilistic approach that can be used for modeling and predicting the behavior of a system based on observed stochastic events. From a network reliability perspective, the variables of a BN are the components in the network, while the links represent the interaction of the nodes leading to network system ‘‘success’’ or ‘‘failure’’. 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) [10].

The risk analysis approach to CI vulnerability assessment can be divided into two lines of analysis: the first entails the qualitative assessment of system vulnerabilities by expert judgment and tabular methods [11], [12]; the second entails the quantitative vulnerability assessment of a CI [13], [14], for ranking system elements criticality, and assessing the cascade failure dynamics [15]. To a certain extent, the risk analysis approach to the vulnerability of CI can be considered a general framework of analysis because it often takes advantage of other approaches and tools, i.e. power flow analysis for electrical transmission networks [15], and network analysis [13].

Complex network methods can be applied to the analysis of CI. The interconnection structure of a CI can be represented by an unweighted network, where the edges between nodes are either present or not. Topological analysis based on classical graph theory can unveil relevant properties of the structure of a network system [16], [17] by i) highlighting the role played by its components (nodes, and connecting arcs) [18], [19]; and 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 [20], [21]. 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 (or vertices) connected by K unweighted (all equal) edges (or arcs), 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, respectively, their characteristic path length, L (number of arcs in the shortest path between two nodes averaged over all pairs of nodes), and average clustering coefficient, C (measure of the extent to which nodes tend to form small groups) [22]. To describe the heterogeneity in the capacity and intensity of the connections (e.g. because of different impedance and reliability characteristics of overhead lines in electrical transmission networks [23], [24], unequal traffic on roads which affects accident probability [21], or different routing capacities of the Internet links [25]) a numerical weight can be assigned to each link of the representative network, to measure the ‘strength’ of the connection. In this way, the functional behavior of the CI is somewhat embedded into a generalized, simple topological analysis framework.

Another important dimension to add to the vulnerability characterization refers to modeling the dynamics of flow of the physical quantities in the network. This modeling entails considering the interplay between structural characteristics and dynamical aspects, which makes the modeling and analysis very complicated because the load and capacity of each component, and the flow through the network, are often highly variable quantities both in space, and time. The resulting functional models have shed light on the way complex networks react to faults and attacks, evaluating their consequences when the dynamics of the flow of the physical quantities in the network are taken into account. The response behavior often results in a dramatic cascade phenomenon due to avalanches of node breakings [26]–[28]. Finally, complex network theory models allow accounting for dependencies and interdependencies among different CI; this enables us to assess the influences and limitations which interacting infrastructures impose on the individual system operating conditions. The knowledge gained from the assessment may be exploited for avoiding fault propagation by designing redundancies and alternative modes of operations, and for detecting and recognizing threats [29]–[31].

Also, object-oriented modeling has been shown to offer an attractive paradigm for describing the dynamic system operational behavior, with close adherence to the reality of the coupled processes involved [32]. One of the major advantages of an object-oriented approach for modeling and simulating CI 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 objects, and their interactions. In other words, the overall system behavior results from the interactions among the multiple single objects of different kinds which make up the system [24]. This modeling achieves a close representation of the system behavior by integrating the spectrum of different stochastic phenomena which may occur, thus generating a multitude of representative stochastic, time-dependent event chains. To integrate stochastic time-dependent technical and non-technical factors into the vulnerability assessment of a CI, a two-layer object-oriented modeling approach can be deployed [33]. 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 [34]. The conceptual modeling framework consists of the abstraction of the relevant technical, and non-technical components of the system as individual interacting objects. Objects are used to model both technical components (such as generators in the electric power system), and non-technical components (such as grid operators in the electric power system). The different objects interact with each other directly (e.g. generator dispatch in the electric power system), or indirectly (e.g. via the physical network). Each object is modeled by attributes, and rules of behavior. An example of 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. Stochastic processes are probabilistic component failure models which can be simulated by Monte Carlo techniques [35], [36]. The main problems of object-oriented modeling are related to the slow simulation speed, and the large number of input parameters in the analysis [24]. However, by focusing on specific safety aspects, the model can be simplified, and the computational burden reduced.

REFERENCES

[1] United Nations International Strategy for Disaster Reduction, “Living with Risk. A Global Review of Disaster Reduction Initiatives" - 2004 Version. ISDR, Geneva, 2004.

[2] G. F. White, *Natural hazards: local, national, global,* New York: Oxford University Press, 1974.

[3] S. Bouchon, “The Vulnerability of Interdependent Critical Infrastructures Systems: Epistemological and Conceptual State-of-the Art”, EUR-report, 2006.

[4] A. H. Dekker, “Simulating Network Robustness for Critical Infrastructures”, in *Proc. of the 28th Australasian Computer Science Conference*, January 30 - February 3, The University of Newcastle, Newcastle, Australia, 2005.

[5] A. Debón, A. Carrión, E. Cabrera, H. Solano, “Comparing risk of failure models in water supply networks using ROC curves”, *Reliability Engineering and System Safety*, 95, 2010, pp. 43-48.

[6] D. Lord, S. P. Washington, J. N. Ivan, “Poisson, Poisson-gamma and zero-inflated regression models of vehicle crashes: balancing statistical fit and theory”, *Accident Analysis and Prevention*, 37, 2005, pp. 35-46.

[7] S. M. Iyer, M. K. Nakayama, A. V Gerbessiotis, “A Markovian Dependability Model with cascading Failures”, *IEEE TRANSACTION ON COMPUTERS*, vol. 58, 2009, pp. 1238-1249.

[8] D. J. Watts, “A simple model of global cascades on random networks”, *PNAS*, vol. 99, 2002, pp. 5766-5771.

[9] I. Dobson., B. A. Carreras, D. E. Newman, “A loading-dependent model of probabilistic cascading failures”, *Probability in the Engineering and Informational Sciences*, 19, 2005, pp. 15–32.

[10] O. Doguc, and J. E. Ramirez-Marquez, “A generic method for estimating system reliability using Bayesian networks”, *Reliability Engineering and System Safety*, vol. 94, 2009, pp. 542– 550.

[11] D. A. Moore, “Application of the API/NPRA SVA methodology to transportation security issues”, *Journal of Hazardous Materials*, vol. 130, 2006, pp. 107–121.

[12] J. Piwowar, E. Châtelet, and P. Laclémence, “An efficient process to reduce infrastructure vulnerabilities facing malevolenze”, *Reliability Engineering and System Safety*, vol. 94, 2009, pp. 1869–1877.

[13] G. E. Apostolakis and D. M. Lemon, “A Screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities Due to Terrorism”, *Risk Analysis*, vol. 25, 2005, pp. 361-376.

[14] F. Flammini, A. Gaglione, N. Mazzocca, C. Pragliola, “Quantitative Security Risk Assessment and Management for Railway Transportation Infrastructures”, CRITIS 2008, LNCS 5508, 2009, pp. 180–189.

[15] A. M. Koonce, G. E. Apostolakis, B. K. Cook, “Bulk power risk analysis: Ranking infrastructure elements according to their risk significance”, *Electrical Power and Energy Systems*, vol. 30, 2008, pp. 169–183.

[16] R. Albert, H. Jeong, A. -L. Barabási, “Error and attack tolerance of complex networks”, *Nature*, vol. 406, 2000, pp. 378-382.

[17] S. H. Strogatz, “Exploring complex networks”, *Nature*, Vol. 410, pp. 268-276, 2001.

[18] P. Crucitti, V. Latora, S. Porta, “Centrality in networks of urban streets”, *Chaos*, 16, pp. 015113 (1-9), 2006.

[19] E. Zio and G. Sansavini, “A systematic procedure for analyzing network systems”, International Journal of Critical Infrastructures, Volume 4, Numbers 1-2, 5 , 172-184(13), 2007.

[20] V. Rosato, S. Bologna, F. Tiriticco, “Topological properties of high-voltage electrical transmission networks”, Electric Power System Research, vol. 77, pp. 99-105, 2007.

[21] E. Zio, G. Sansavini, R. Maja, G. Marchionni, “An analytical approach to the safety of road networks”, International Journal of Reliability, Quality and Safety Engineering, Vol. 15 Issue: 1, Page: 67 - 76 February 2008.

[22] D. J. Watts and S. H. Strogatz, “Collective dynamics of ‘small-world’ networks”, Nature, Vol. 393, pp. 440-442, 1998.

[23] P. Hines and S. Blumsack, “A centrality measure for electrical networks”, Proceedings of the 41st Hawaii International Conference on system Science, 2008.

[24] I. Eusgeld, W. Kröger, G. Sansavini, M. Schläpfer, E. Zio, “The role of network theory and object-oriented modeling within a framework for the vulnerability analysis of critical infrastructures”, Reliability Engineering & Systems Safety, Vol. 94, No 5, pp. 954-963, 2009.

[25] V. Latora and M. Marchoiri, “Vulnerability and protection of infrastructure networks”, Physical Review E, 71, 015103 (1-4), 2005.

[26] A. E. Motter, Y. C. Lai, “Cascade-based attacks on complex networks”, Physical Review E, 66, pp. 065102(1-4), 2002.

[27] A. E. Motter, “Cascade control and defense in complex Networks”, Physical Review Letters, vol. 93, nr 9, pp. 098701(1-4), 2004.

[28] E. Zio and G. Sansavini, “Modeling failure cascades in networks systems due to distributed random disturbances and targeted intentional attacks”, Safety, Reliability and Risk Analysis: Theory, Methods and Applications – Martorell et al. (eds), Proceedings of ESREL 2008 and 17th SRA Europe Annual Conference, 22-25 September 2008, Valencia, Spain, Taylor & Francis Group, London, 2009.

[29] R. Zimmerman, “Social Implications of Infrastructure Network Interactions”, Journal of Urban Technology, Volume 8, Number 3, pages 97-119, 2001.

[30] L. Duenas-Osorio and S. M. Vemuru, “Cascading failures in complex infrastructure systems”, Structural Safety, Vol.31, pp. 157-167, 2009.

[31] J. Johansson and H. Jönsson, “A model for vulnerability analysis of interdependent infrastructure networks”, Safety, Reliability and Risk Analysis: Theory, Methods and Applications – Martorell et al. (eds), Taylor & Francis Group, London, 2009.

[32] M. D'Inverno and M. Luck, Understanding Agent Systems, Springer, Berlin, 2004.

[33] M. Schläpfer, T. W. Kessler, W. Kröger, "Reliability Analysis of Electric Power Systems Using an Object-oriented Hybrid Modeling Approach,", Proceedings of the 16th Power Systems Computation Conference, Glasgow, 2008.

[34] P. Hines, H. Liao, D. Jia, S. Talukdar, “Autonomous Agents and Cooperation for the Control of Cascading Failures in Electric Grids”, Proceedings of the IEEE Conference on Networking, Sensing, and Control, Tucson, AZ, March 2005.

[35] R. Billinton and W. Li, “A system state transition sampling method for composite system reliability evaluation”, IEEE Transactions on Power Systems, 8(3), 761-770, 1993.

[36] M. Marsegurra and E. Zio, Basics of the Monte Carlo Method with Application to System Reliability, LiLoLe-Verlag GmbH, Hagen, 2002.

CONCEPTUALIZATION OF CRITICAL INFRASTRUCTURE VULNERABILITY ASSESSMENT

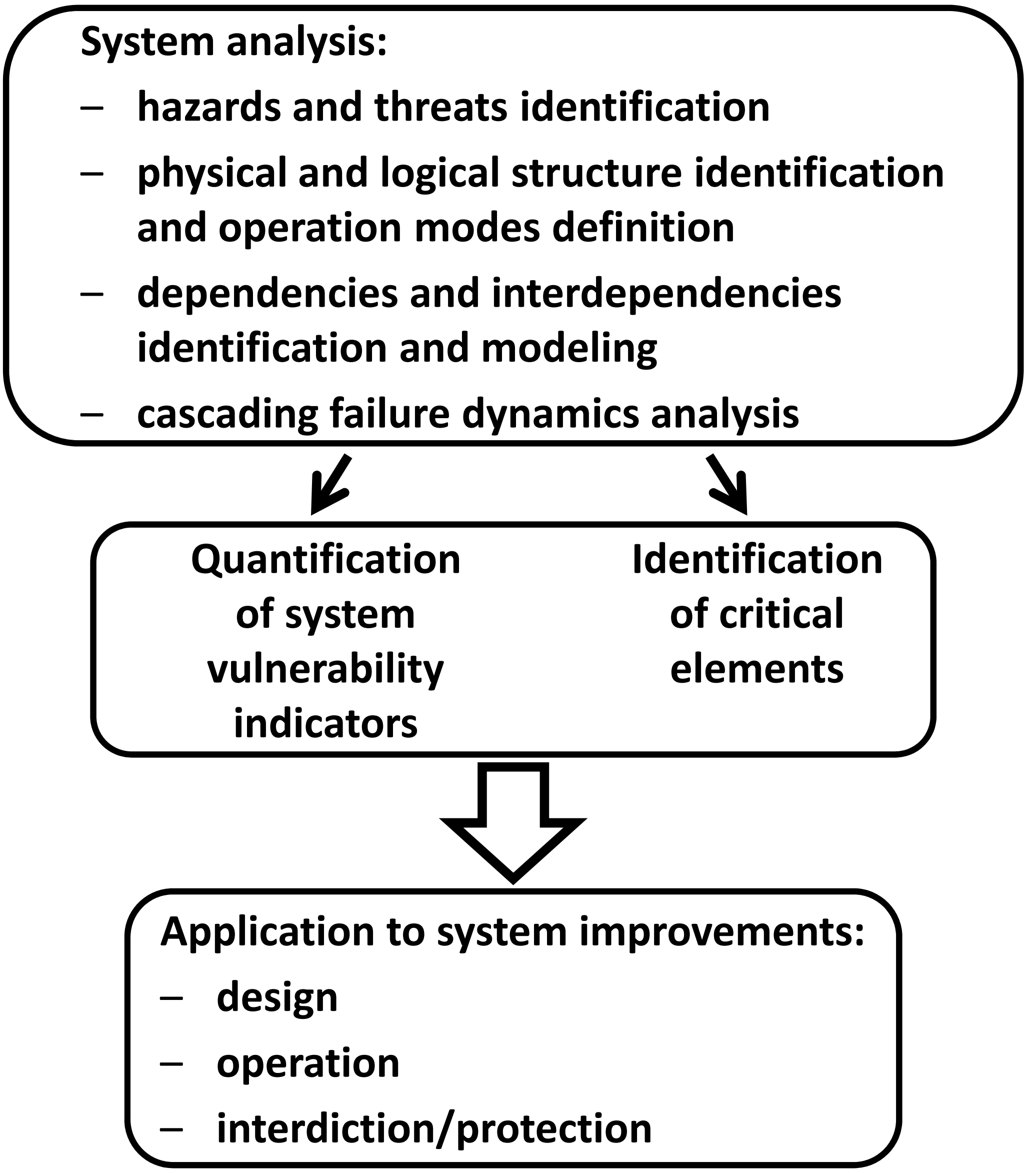
System analysis:
– hazards and threats identification
– physical and logical structure identification and operation modes definition
– dependencies and interdependencies identification and modeling
– cascading failure dynamics analysis
Quantification of system vulnerability indicators
Identification of critical elements
Application to system improvements:
– design
– operation
– interdiction/protection

Fig. 1 Conceptualization of vulnerability assessment