This article is part of the IEEE Reliability Society 2007 Annual Technology Report.

Reliability Analysis of Complex Network Systems: Research and Practice in Need

Enrico Zio
Polytechnic of Milan
Email: enrico.zio@polimi.it

System reliability methods have been originally tailored to deal with 'fixed', localized systems and plants which can be rationally represented by logical/functional structures of components, albeit complex. In this representation, the failures of the components are seen with respect to their consequence on the system function.

On the other hand, nowadays many systems of distributed service exist (the so called *infrastructures*), constituted by networks of components. In these systems, there is an additional dimension of complexity related to the difficulty of representing, modeling and quantifying the effects on the system of a failure of a component.

A number of these systems are considered critical for the social welfare of modern societies and thus need priority protection (CNIP, 2006; Birchmeier, 2007). While the EU and other national and transnational administrations are recognizing the importance of this safety issue with specific directives and programs (OHS, 2002; EU 2005 and 2006; IRGC, 2006), it seems that the classical methods of reliability and risk analysis fail to provide the proper instruments of analysis.

Indeed, there is an emerging feeling in the community of experts in risk, safety, reliability and security that a new paradigm is needed for analyzing and managing the complex distributed systems and critical infrastructures which constitute the backbone of modern Industry and Society (e.g. computer and communication systems (Aggarwal, 1975; Kubat, 1989; Samad, 1987), power transmission and distribution systems (Jane et al., 1993; Yeh and Revised, 1998), rail and road transportation systems (Aven, 1987), oil /gas systems (Aven, 1987 and 1988)). Identifying and quantifying the vulnerabilities of such systems is crucial for designing the adequate protections, mitigation and emergency actions against their failures (CNIP, 2006; Rocco et al., 2007; Vulnerability ESREL, 2007). These needs are enhanced in a World where deregulation of the services is favored and malevolent acts of terrorism and sabotage are a serious threat (CNIP, 2006; Rocco et al., 2007; Vulnerability ESREL, 2007).

The current methodologies of reliability engineering, risk assessment and management (possibly sophisticated) are applied successfully on man-machine-environment systems (even 'complicated') with well-defined rigid boundaries, with single, well-specified targets of the hazard and for which historical or actuarial data (e.g. accident initiators and components failure rates and empirical data on accident consequences) exist in support to robust quantification models which account for the uncertainties deriving from both random variations in the behavior of the elements of the system under analysis and from lack of knowledge of the system itself (Apostolakis and Lemon, 2005).

In the current framework, reliability engineering aims at searching for the causal links among the system elements (components, structures, people, etc.) and modeling and integrating their behavior so as to quantify that of the system as a whole.

On the other hand, risk management aims at achieving rational, risk-informed decisions by carrying out an optimization process aimed at maximizing specified preferential objectives in presence of uncertainty. The simplest example of such process is the classical cost-benefit analysis.

This approach to reliability engineering and risk analysis (assessment and management) of complicated technological systems (Kastenberg, 2005):

- assumes that the system has fixed boundaries, there is a fixed well-defined target and there are actuarial data available to support the quantification models,
- is sustained by the classical Newtonian/Cartesian view of the World, which is founded on the following creeds on the system behavior:
  1. it can be understood from the behavior of its constitutive elements (reductionism) and their causal links (cause-and-effect);
  2. it can be determined from objective empirical observations (subject/object dualism).

As illustrated in (Kastenberg, 2005), the above framework of analysis may not be fully apt to deal with many existing complex network systems which, on the contrary, are characterized by a behavior which:

- emerges as a whole and hence cannot be understood and properly described by looking at its constitutive parts, which do not exhibit such behavior when taken by themselves (emergent/holistic property),
- may change significantly for small changes in the input (chaotic),
- can partly be described only subjectively (subjective).

The above characteristics of the newly arising complex network systems are such that societal and environmental impacts of accidents and attacks are no longer geographically local (e.g. a blackout in a power transmission and distribution network or a malevolent attack to a transportation network) nor clearly perceptible in time because either spreading very quickly (a virus in the Internet) or very slowly (an accident in a radioactive waste deposit whose consequences may affect future generations).

The new risk scenario of modern Industry and Society briefly depicted above creates some unprecedented challenges to research and practice, such that a new paradigm of risk may be in order and new methods for reliability and risk analysis needed.

In particular, an innovative and promising approach to the analysis of complex technological network systems and infrastructures comes from the findings of Complexity Science (Kauffman, 1993; Capra, 1996; Science, 1999; Bar-Yam, 1997; Barabasi, 2002). Recent advances in this field indicate that many complex systems, technological, natural and even social, are hierarchies of networks of components (also called nodes, vertices or elements) interacting through links (also called edges, arcs or connections). Although the properties of the individual components can usually be characterized in laboratory, these isolated measurements bring relatively little information on the behavior of the large scale interconnected systems in which they are embedded. This is due to the fact that it is from the local interaction of the components in the interconnected network that the system behavior emerges as a whole.

The apparent ubiquity of networks leads to a fascinating set of problems common to biological, ecological, technological and social complex systems, regarding how the underlying network topology influences the system behavior and its characteristics of stability and robustness to faults and attacks. For example, the topology of the power grid affects the robustness and stability of power transmission (Carreras et al, 2002; Crucitti et al, 2004; CNIP, 2006; Jonsson et al. 2007; Rosato et al., 2007).

In this view, the actual structure of the network of interconnections among the components is a critical feature of the system: the stability and robustness of these systems depend on the redundant wiring of the functional web interconnecting the system's components; yet, error tolerance and attack robustness are not shared by all redundant networks (Albert et al., 2000).

For these analyses to be of use at the decision making level, efforts must be made to bring into the picture the characteristic safety and reliability attributes of the network components to analyze the properties that emerge at the system level (Zio, 2007a). The indicators thereby developed can be exploited for the analysis of the vulnerabilities of network systems and thus for their optimal design, operation and management.

The above analyses must be corroborated by detailed system modeling of a limited set of design and accident scenarios, e.g. by agent-based and Monte Carlo simulation (CNIP, 2006).

Furthermore, dependences need to be adequately modeled to investigate the interactions among complex infrastructure systems, leading to the so called *systems of systems* (Carreras et al., 2002; CNIP, 2006; Bologna, 2007). Communication, power, transportation networks are complex infrastructure systems which interact with each other in even more complex ways: from these interactions increased risks of failures may arise in the individual systems from unexpected emergent behavior. To investigate this issue, new approaches and paradigms of dependence analysis need to be formulated.

References

(Aggarwal, 1975) Aggarwal K.K., *A simple method for reliability evaluation of a communication system.* IEEE Trans Communication 1975; COM-23: 563-5.

(Albert et al., 2000) Albert R., Jeonh H. and Barabasi A.-L., *Error and Attack Tolerance of Complex Networks*, Nature, Vol. 406, 2000, pp. 378-382.

(Apostolakis and Lemon, 2005) Apostolakis G.E., and Lemon D.M., *A Screening Methodology for the Identification and Ranking of Infrastructure Vulnerabilities due to Terrorism*, Risk Analysis, 25, 2005, pp. 361-376.

(Aven, 1987) Avent T., *Availability evaluation of oil/gas production and transportation systems*. Reliability Engineering and System Safety, 1987;18:35-44.

(Aven, 1988) Avent T., *Some considerations on reliability theory and its applications*, Reliability Engineering and System Safety, 1988;21:215-23.

(Aven, 1993) Aven, T., *On performance measures for multistate monotone systems*, Reliab. Eng. and Sys. Safety, 1993; 41; 259-266.

(Barabasi, 2002) Barabasi, A.L., *Linked: The New Science of Networks*, Perseus Publishing, Cambridge, Massachussetts, 2002.

(Bar-Yam, 2000) Bar-Yam, Y., *Dynamics of Complex Systems*, Westview Press, 2002.

(Birchmeier, 2007) Birchmeier J., *Systematic Assessment of the Degree of Criticality of Infrastructures*, Proceedings of ESREL 2007, Stavanger, Norway, 25-27 June 2007, Volume 1, pp. 859-864.

(Bologna, 2007) Bologna S., *Security of Wide Technological Networks with Particular Reference to Inter-Dependences*, City& Security, Rome, March 30 2007.

(Capra, 1996) Capra F., *The Web of Life*, Doubleday, New York, 1996.

(Carreras et al., 2002) Carreras B.A., Lynch V., Dobson I., Newman D.E., *Critical Points and Transitions in an Electric Power Transmission Model for Cascading Failure Blackouts*, Chaos, Volume 12, N0. 4, 2002, pp. 985-994)

(CNIP, 2006) CNIP'06, *Proceedings of the International Workshop on Complex Network and Infrastructure Protection*, Rome, Italy, 28-29 March 2006.

(Crucitti et al., 2004) Crucitti, P., Latora, V. and Marchiori M., *A Topological Analysis of the Italian Electric Power Grid*, Physica A Vol. 338, 2004, pp. 92-97.

(EU, 2005) *Green Paper on a European Programme for Critical Infrastructure Protection*, COM(2005) 576 Final, Brussels, EU, 2005.

(EU, 2006) *European Union Directive Draft*, COM(2006) 787, Brussels, EU, 2006.

(IRGC, 2006) *White Paper on Managing and Reducing Social Vulnerabilities from Coupled Critical Infrastructures*. International Risk Governance Council, Geneva, 2006.

(Jane et al., 1993) Jane CC, Lin JS, Yuan J., *Reliability evaluation of a limited-flow network in terms of MC sets*, IEEE Trans Reliability, 1993;R-42:354-61.

(Jonsson et al. 2007) Jonsson H., Johansson J. and Joansson H., *Identifying Critical Components in Electric Power Systems: A Network Analytic Approach*, Proceedings of ESREL 2007, Stavanger, Norway, pp. 889-897.

(Kastenberg, 2005) Kastenberg, W.E., *Assessing and Managing the Security of Complex Systems: Shifting the RAMS Paradigm*, Proceedings of the 29th ESReDA Seminar on Systems Analysis for a more Secure World, JRC-IPSC, Ispra, Italy, October 25-26, 2005, pp. 111-126.

(Kauffman, 1993) Kauffman, S.A., *The Origins of Order*, Oxford University Press, 1993.

(Kubat, 1989) Kubat P., *Estimation of reliability for communication/computer networks simulation/analytical approach*. IEEE Trans Communication, 1989; 37:927-33.

(OHS, 2002) *National Strategy for Homeland Security*, US Office of Homeland Security, Washington, 2002.

(Rocco et al., 2007) Rocco C. M., Zio E. and Salazar D.E., *Multi-objective Evolutionary Optimisation of the Protection of Complex Networks Exposed to Terrorist Hazard*, Proceedings of ESREL 2007, Stavanger, Norway, 25-27 June 2007, Volume 1, pp. 899-905.

(Rosato et al., 2007) Rosato V., Bologna S. and Tiriticco F., *Topological Properties of High-Voltage Electrical Transmission Networks*, Electric Power Systems Research, 77, 2007, pp. 99-105.

(Samad, 1987) Samad MA., *An efficient algorithm for simultaneously deducing MPs as well as cuts of a communication network*. Microelectronic Reliability, 1987; 27:437-41.

(Schneeweiss, 2004) Schneeweiss W.G., *Petri Net Picture Book*, LiLoLe-Verlag GmbH, 2004.

(Science, 1999) Science, *Special Section on Complex Systems*, Volume 284, No. 5411, April 2, 1999, pp. 79-109.

(Vulnerability ESREL, 2007) *Vulnerability, Reliability and safety of Complex Networks and Critical Infrastructures*, Special Sessions I and II, Proceedings of ESREL 2007, Stavanger, Norway, 25-27 June 2007, Volume 1.

(Yeh and Revised, 1998) Yeh W.C., Revised A., *Layered-network algorithm to search for all d-minpaths of a limited-flow acyclic network*. IEEE Trans Reliability, 1998; R-46:436-42.

(Zio, 2007) Zio E., *From complexity science to reliability efficiency: a new way of looking at complex network systems and critical infrastructures*, Int. J. Critical Infrastructures, Vol. 3, Nos. 3/4, 2007, pp. 488-508.