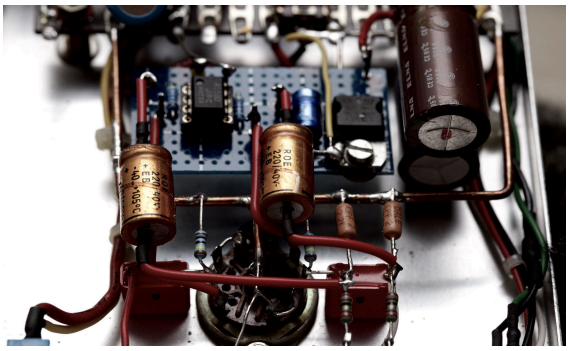
Reliability Analysis of Systems of Systems



Enrico Zio
Chair System Science and the Energy Challenge, Fondation Electricite' de France (EDF), CentraleSupélec, Université Paris-Saclay, France
enrico.zio@centralesupelec.fr
Dipartimento di Energia, Politecnico di Milan, Italy
enrico.zio@polimi.it

Abstract - In this paper, some reflections are provided on the reliability analysis of systems of systems and the challenges posed by their specific characteristics of interdependence and complexity. Such characteristics generate dynamic system behaviors that are difficult to represent and model by classical decomposition/re-composition approaches. Different approaches need to be integrated, that look at the system of systems from different perspectives, including structural, dynamic, control-based, logic-based.

Keywords - systems of systems, complexity, interdependence, reliability analysis, vulnerability, risk, resilience, uncertainty, electric power grids, smart grids

1. RELIABILITY ANALYSIS OF SYSTEMS OF SYSTEMS: CHALLENGES

Reliability is a fundamental attribute for the safe and profitable operation of any technological system. Reliability analysis aims at studying the failure mechanisms of a system (and of its protective barriers, for what concerns accident development) and at quantifying the associated likelihoods. The outcomes of the analysis serve to identify design solutions and maintenance actions for preventing the failures (hardware, software, human and organizational) from occurring, and protective barriers for mitigating the consequences of the failures.

A fundamental issue in reliability analysis is the stochastic (aleatory) uncertainty in the system failure occurrences and associated consequences, and the (epistemic) uncertainty in the models used for their quantification. For the objectives of safety and business continuity, the system must, then, be protected robustly with respect to the uncertainties [1].

Methods of reliability analysis have been developed for (localized) systems, which are modeled by logic or functional structures of components (e.g., reliability block diagrams, fault trees, Markov chains, etc.). The failure event of the system is represented by the structure of the logic relations at the components level. By such a modeling framework, system reliability analysis implies searching for the causal logic links among the system elements (components, structures, human operators, etc.), modeling their failure behaviors and integrating them into that of the system as a whole.

Nowadays, many systems of distributed services exist (the so-called infrastructures, e.g. computer and communication systems, electric power transmission and distribution systems, rail and road transportation systems, water/oil/gas distribution systems), which are networks of components strongly interconnected on very large spatial scales. A number of these network systems are critical for the social welfare of modern societies (so-called critical infrastructures), and thus are subject to great attention for priority protection [2]-[7]. Indeed, the EU and other national and transnational administrations have recognized the importance of this issue with specific directives and programs [8]-[14].

Dependences in these systems introduce a degree of complexity that makes it difficult to use the classical system reliability analysis methods for representing, modeling and quantifying the causal effects of the components failures onto the system function. It, thus, becomes a challenge to perform the reliability analysis, whose outcomes are used to identify and design adequate solutions of protection, mitigation and emergency, for overall system resilience [5][15]-[18].

The difficulties come particularly from the fact that the response behavior of these systems to perturbations:

- emerges as a whole from the nonlinear combination of the individual behaviors of the components: (emergent/holistic property);
- may change significantly for small changes in the input (chaotic behavior);
- can partly be described only subjectively

With regards to the spatial scale of the problem, the dimension and complexity of these systems extend beyond the usual single plant boundaries. Then, the 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 or a cyber-physical system).

With respect to the temporal scale of the problem, the impacts of accidents and attacks can either spread very quickly (a virus in the Internet) or very slowly (an accident in a radioactive waste deposit whose consequences may affect future generations).

The spatial ubiquity and temporal indeterminacy of the behavior of network systems lead to a set of questions regarding the role that the underlying network structure plays in influencing the system behavior, its stability, robustness and resilience to faults and attacks. These problems are general and common to biological, ecological, technological and social complex systems.

The structure of the network of interconnections is, thus, a critical feature of the system [23]. Dependences and inter-dependences, then need to be adequately identified and modeled to investigate the interactions in and between complex infrastructure systems, leading to the consideration of the so-called systems of systems [5] [19][24]-[27].

For example, the topology of the power grid affects the robustness and stability of power transmission [5][19]-[22]. The European electric power supply system serves as a particularly good example. Following the liberalization of the electric markets, the network is experiencing increasing and tighter integration, with allocation of renewable, intermittent power sources. It is also interconnected with several other critical infrastructures to which it provides energy (transportation, banking, etc.) and is trending towards a significant integration with the information and communication network, under the developing perspective of smart grids.

The interconnected communication, power, transportation and other networks form a complex architecture of critical infrastructure systems, which interact in complex ways. Increased risk of failures and accident propagation may arise through these interactions, due to local failures effects spreading across the system boundaries.

The investigation of the risks and vulnerabilities of these systems of systems must, then, go beyond the usual cause/consequence analysis to focus on spill-over effects of failures [28][29].

The analysis serves the scope of verifying that the capacities allocated by design to a given system are adequate to support the future occurring demands, in this scenario of greater integration among critical infrastructures and of market deregulation, and that the safety margins (extra capacities) preventively designed are sufficient to cope with the expected and unexpected stresses arriving onto the system. As observed earlier, large uncertainties exist in the characterization of the failure behavior of the elements of a complex system, and of the dynamics that emerge from it through interconnections and interactions; this makes predictions difficult to achieve confidently [30]. Emergent behaviors may arise in these systems in collective ways difficult to predict from the superposition of the behavior of the individual elements. Particularly, system-level breakdowns may emerge from small, local perturbations followed by cascades and large-scale, border-crossing consequences, spreading through the existing (inter-)dependences.

Undoubtedly, this modern industrial and societal scenario strongly relying on systems of systems composed of interdependent critical infrastructures brings substantial challenges to reliability analysis. Methods for such analysis should include those of complexity science for the initial identification and screening of vulnerabilities in networks (and networks-of-networks) [31]-[33], logic methods for quantitative system analysis [34]-[40], and dynamic flow and control modeling methods for scenario assessment [41]-[43].

2. SYSTEMS OF SYSTEMS

To lead the way to a systematic discussion on methods and approaches for the reliability analysis of systems of systems, it is useful to first recall some basic common definitions.

System: group of interacting elements (or subsystems) having an internal structure, which links them into a unified whole.

Complex system: a system made by many components interacting in a network structure. Most often, the components are physically and functionally heterogeneous, and organized in a hierarchy of subsystems that contribute to the system function. This leads to both structural and dynamic complexity.
Structural complexity derives from:

- heterogeneity of components across different technological domains, due to increased integration among systems;
- scale and dimensionality of connectivity, characterized by a large number of components (nodes) highly interconnected through dependences and interdependences (the former are unidirectional relationships: component i depends on j through a link, but j does not depend on i through the same link; the latter represent bidirectional relationships: component i depends on j through some links, and j likewise depends on i through the same and/or other links).

Dynamic complexity manifests through the emergence of (even unexpected) system behavior in response to (even small) changes in the environmental and operational conditions of its components.

Taking again the electric power grid as example, this is a system made of a large number of interconnected elements (wires and machines) which eventually link the power generators to the customers, for satisfaction of their objectives. Structural complexity arises in these systems from:

- heterogeneity of the components across different technological domains (electrical components, information technology components, etc.), integrated

in the power system, which is itself becoming strongly interconnected with other critical infrastructures;
- scale of connectivity (interactions among several components) and dimensionality (large number of nodes highly interconnected also with other neighboring power systems, distributed energy sources, storage and electrical vehicles, etc.).

System of systems: a large-scale, distributed system, the components of which are complex systems themselves [49]. In principle, linking systems into a joint system of systems through designed interdependences allows for the exploitation of interoperability and synergism, at the benefit of economic, reliable and safe operation and service.

Let us continue the example of the electric power grid. This system is evolving from its original development of a loosely interconnected network of local systems to a configuration extended on large scales, across regional and national boundaries. Emergent behavior may arise in such system, in ways that are difficult to predict from the superposition of the behavior of the individual elements. For this reason, the re-definition of the electric power grid for allowing decentralized generation with integration of large shares of renewable sources (most of all solar and wind energies) at the most suitable sites (e.g. desert solar and offshore wind farms), must be accompanied by a "smart" system comprising smart metering, new devices for improved controllability, with self-healing capacity etc. This is leading to the transformation of the existing power grid from the original static infrastructure intended to be operated as designed, into a flexible and adaptive infrastructure operated dynamically through the foundational layers of power and energy, communication and IT/computer. This is a typical example of system of systems, in which the individual systems are interconnected in a collaborative infrastructure, with a management scheme that aims at meeting both the individual objectives and those of the whole system of systems [27]. However, the interdependences and complexities therein may lead to new and unexpected hazards and vulnerabilities. For example, the growing integration of Information and Communication Technology (ICT) for the operation of the power grid introduces the issue of cyber-security, which must be considered from the outset in the design of smart grids, as recent incidents have shown that ICT systems can be vulnerable to cyber-attacks and that such attacks can lead to disruption of physical systems and networks.

3. RELIABILITY ANALYSIS OF SYSTEMS OF SYSTEMS: METHODS AND APPROACHES

The reliability analysis of a system of systems entails the analysis of the constitutive systems, their parts and their interactions through dependences and interdependences. The analysis must account for the environment which the systems live and operate in, and starting from the systems objectives explores possible variations and deviations in their behaviors [42]. In turn, the behavior at system level is the result of the collective emergence through the structure of interdependences underlying the system of systems. This can be quite difficult to predict, even if the behavior of the individual components is understood reasonably well.

Given the different aspects that play a role in determining the system behavior, a holistic framework is needed that integrates methods capable of analyzing the system-of-system reliability from different perspectives and at different levels of detail, while accounting throughout for the existing uncertainties [44]:

- structural methods based on complexity science, graph theory, statistical physics, etc., capable of modeling the interdependent connectivity of a complex system of systems, for analyzing its effects on system functionality and on the process of propagation of an initial failure onto a cascade of failures that may lead to partial or complete dysfunctionality of the system of systems. The role of the interdependent network of connections needs also to be analyzed with respect to the system function recovery process, within a perspective of resilience that includes the identification of the central elements of the system that must be most attentively controlled and protected because of their leading role on the system connectivity which supports system recovery;
- logical methods based on system analysis, hierarchical logic trees, etc., for analyzing the logic of functioning/dysfunctioning of the system of systems, also identifying the combinations of failures of elements (hardware, software and human) which lead to the loss of the system function;
- phenomenological/functional methods, to represent by transfer functions the dynamic input-output relations, with or without]adequate control; these methods can be for example based on agent-based modeling to describe the interrelated operation between heterogeneous system-of-system elements (hardware, software and human), within federated computational architectures for simulating their interacting dynamics and analyzing the behavior that emerges for the system of systems;
- flow methods, based on detailed, mechanistic models (and computer codes) of the physical processes occurring in the system of systems, for describing the physics of system operation, its monitoring and control.

The analysis of the system of systems behaviors emerging from the different initiating events, for reliability analysis purposes can be quite challenging in practical cases, due to the high dimension of the system state-space and the computational effort correspondingly needed to explore the possible system evolutions in search of the interesting (and typically very rare) ones of failure. Advanced simulation techniques for cascading failure scenario analysis can help probing the space of event sequences, adaptively and intelligently allocating the simulation efforts preferably on those sequences leading to

outcomes of interest for the objectives of the reliability analysis. Note that in this case, the aim of simulation is neither of completeness of the set of scenarios nor of accuracy of scenario probability estimation, but rather of enabling the generation of "surprising" scenarios to get useful insights about what could happen, and enable proper decisions on how to protect the system of systems [45]. Interpretation of these scenarios is critical if one is to identify also these otherwise surprising scenarios [46]-[49].

4. CONCLUSION

We live, work and produce in a Society, whose functioning depends on a pool of interconnected critical infrastructures, which provide essential products and services. The reliability of these systems of systems has become a national and international priority. The high degree of inter- and intra-connectedness that characterizes these systems of systems can introduce unexpected vulnerabilities, which can lead to extended disruption when exposed to hazards of various nature, from random mechanical/physical/material failures to natural events, software failures, intentional malevolent attacks, human and organizational errors. It is widely recognized that this broader spectrum of hazards and threats, calls for an all-hazards approach for the understanding of the failure behavior of such systems, for the effective protection of their reliability.

Given, the complexity of these systems of systems, the characterization of the hazards, and the evaluation of their consequences and probabilities, require an integrated analysis, tackling the problem from different perspectives that consider the structural, functional, logic and dynamic characteristics and properties.

Possibly, a unifying conceptual framework of analysis can be defined, whereby accidents are seen to occur due to variations in the components behaviors beyond their designed capacities and operated safety barriers. Concepts of "common-cause variation" and "special-cause variation", and the continuous focus on learning and updating for improvement in observability and controllability, could be introduced to comprehensively capture "normal" system variations, but also "unusual" variations and unexpected surprises [50]-[52]. Within such conceptual framework, advanced simulation techniques for exploring the system state-space are needed to identify otherwise unrevealed sequences of events, possibly leading to surprising consequences.

REFERENCES

[1] Zio E. "Reliability Engineering: Old Problems and New Challenges." Reliability Engineering and System Safety, Volume 94, Issue 2, 2009, pp. 125–141.

[2] Clinton, W. "Presidential Decision Directive PDD-63, Protecting America's Critical Infrastructures," Washington, D.C, 1998.

[3] Bush, G.W. "Homeland Security Presidential Directive-3 (HSPD-3)," Washington, D.C, 2002.

[4] Bush, G.W. "Homeland Security Presidential Directive-7 (HSPD-7)," Washington, D.C, 2003.

[5] CNIP'06, Proceedings of the International Workshop on Complex Network and Infrastructure Protection, Rome, Italy, 28-29 March 2006.

[6] Lewis, T. G. Critical Infrastructure Protection in Homeland Security: Defending a Networked Nation, Wiley, 2006.

[7] 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.

[8] EPCIP. "European Programme for Critical Infrastructure Protection."

[9] National Strategy for Homeland Security, US Office of Homeland Security, Washington, 2002.

[10] Green Paper on a European Programme for Critical Infrastructure Protection, COM 576 Final, Brussels, EU, 2005.

[11] European Union Directive Draft, COM(2006) 787, Brussels, EU, 2006.

[12] White Paper on Managing and Reducing Social Vulnerabilities from Coupled Critical Infrastructures. International Risk Governance Council, Geneva, 2006.

[13] U.S. Department of Homeland Security. "National infrastructure protection plan - Partnering to enhance protection and resiliency", 2009.

[14] Obama, B. "Presidential Policy Directive 21: Critical Infrastructure Security and Resilience," Washington, D.C, 2013.

[15] 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.

[16] Pursiainen, C. "The Challenges for European Critical Infrastructure Ottino J. M. (2004). "Engineering complex systems." Nature, 427(6973), 399-399, 2009.

[17] Cimellaro, G. P., Reinhorn, A. M., and Bruneau, M. (2010). "Framework for analytical quantification of disaster resilience." Engineering Structures, 32(11), pp. 3639-3649.

[18] Moteff, J. D. "Critical Infrastructure Resilience: The Evolution of Policy and Programs and Issues for Congress." Congressional Research Service, 2012.

[19] 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)

[20] Crucitti, P., Latora, V. and Marchiori M., A Topological Analysis of the Italian Electric Power Grid, Physica A Vol. 338, 2004, pp. 92-97.

[21] 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.

[22] Rosato V., Bologna S. and Tiriticco F., Topological Properties of High-Voltage Electrical Transmission Networks, Electric Power Systems Research, 77, 2007, pp. 99-105.

[23] Albert R., Jeonh H. and Barabasi A.-L., Error and Attack Tolerance of Complex Networks, Nature, Vol. 406, 2000, pp. 378-382.

[24] Bologna S., Security of Wide Technological Networks with Particular Reference to Inter-Dependences, City& Security, Rome, March 30 2007.

[25] Eusgeld, I., Nan, C., and Dietz, S. "System-of-systems" approach for interdependent critical infrastructures." Reliability Engineering & System Safety, 96(6), 2011, pp. 679-686.

[26] Johansson, J., and Hassel, H. "An approach for modelling interdependent infrastructures in the context of vulnerability analysis." Reliability Engineering & System Safety, 95(12), 2010, pp. 1335-1344.

[27] Zio E., and Sansavini G. "Modeling interdependent network systems for identifying cascade-safe operating margins." Reliability, IEEE Transactions on, 60(1), 2011, pp. 94-101.

[28] Eusgeld, I. And Kroger W., Towards a Framework for Vulnerability Analysis of Interconnected Infrastructures, Proceedings of the 9th Probabilistic Safety Assessment and Methodology

[29] Zio, E., and Sansavini, G. "Vulnerability of Smart Grids With Variable Generation and Consumption: A System of Systems Perspective." IEEE Transactions on Systems Man Cybernetics-Systems, 43(3), 2013, pp. 477-487.

[30] Zio E., and Aven T. "Uncertainties in smart grids behavior and modeling: What are the risks and vulnerabilities? How to analyze them?" Energy Policy, 39(10), 2011, pp. 6308-6320.

[31] Fang, Y., and Zio, E. "Hierarchical Modeling by Recursive Unsupervised Spectral Clustering and Network Extended Importance Measures to Analyze the Reliability Characteristics of Complex Network Systems." American Journal of Operations Research, 3(1A), 2013, pp. 101-112.

[32] Alipour, Z., Monfared, M. A. S., and Zio, E. "Comparing topological and reliability-based vulnerability analysis of Iran power transmission network." Proceedings of the Institution of Mechanical Engineers Part O-Journal of Risk and Reliability, 228(2), 2014, pp. 139-151.

[33] Li, D., Zhang, Q., Zio, E., Havlin, S., Kang, R., Network reliability analysis based on percolation theory, Reliability Engineering & System Safety, Volume 142, October 2015, pp. 556–562.

[34] Haarla, L., Pulkkinen, U., Koskinen M. And Jyrinsalo J., A Method for Analysing the Reliability of a Transmission Grid, Reliability Engineering and System Safety, 93, 2008, pp. 277-287.

[35] Koonce, A.M., Apostolakis, G.E. and Cook, B.K., Bulk Power Risk Analysis: Ranking Infrastructure Elements According to their Risk Significance, Electricap Power and Energy Systems, 2007.

[36] Bier, V.M., Gratz, E.M., Haphuriwat, N.J., Magua W. and Wierzibcki K.R., Methodology for Identifying Near-Optimal Interdiction Strategies for a Power Transmission System, Reliability Engineering and System Safety,92, 2007, pp. 1155-1161.

[37] Michaud, D. and Apostolakis G.E., Methodology for Ranking the Elements of Water-Supply Networks, Journal of Infrastructure Systems, 2006, pp. 230-242.

[38] Patterson, S.A. and Apostolakis, G.E., Identification of Critical Locations across Multiple Infrastructures for Terrorist Actions, Reliability Engineering and System Safety, 92, 2007, pp. 1183-1203.

[39] Salmeron, J., Wood, K. and Baldick R., Analysis of Electric Grid Security Under Terrorist Threat, IEEE Trans. On Power Systems, Vol. 19, No. 2, 2004, pp. 905-912.

[40] Bobbio, A., Bonanni, G., Ciancamerla, E., Clemente, R., Iacomini, A., Minichino, M., Scarlatti, A., Terruggia, R., and Zendri, E.. "Unavailability of critical SCADA communication links interconnecting a power grid and a Telco network." Reliability Engineering & System Safety, 95(12), 2010, pp. 1345-1357.

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

[42] Kroger W., and Zio E. "Vulnerable Systems", Springer, 2011.

[43] Sansavini, G., Piccinelli, R., Golea, L. R., and Zio, E. "A stochastic framework for uncertainty analysis in electric power transmission systems with wind generation." Renewable Energy, 64, 2014, pp. 71-81.

[44] Ouyang, M. "Review on modeling and simulation of interdependent critical infrastructure systems." Reliability Engineering & System Safety, 121, 2014, pp. 43-60.

[45] Turati, P., Pedroni, N. and Zio, E., An entropy-driven method for exploring extreme and unexpected accident scenarios in the risk assessment of dynamic engineered systems, ESREL 2015 7-10, Sep, 2015, Zurich, Switzerland.

[46] Aven T., "A conceptual foundation for assessing and managing risk, surprises and black swans", Paper presented at the Network Safety Conference, Toulouse 21-23 November, 2013.

[47] Aven T., and Krohn B.S. "A new perspective on how to understand, assess and manage risk and the unforeseen", Reliability Engineering and System Safety, 121, 2013, pp. 1-10.

[48] Kaplan, S., Visnepolschi, S., Zlotin, B. and Zusman, A. "New Tools for Failure and Risk Analysis: Anticipatory Failure Determination (AFD) and the Theory of Scenario Structuring". Ideation International Inc., Southfield, MI, 1999.

[49] Kotov, V. "Systems-of-Systems as Communicating Structures," Hewlett Packard Computer Systems Laboratory Paper HPL-97-124, (1997), pp. 1–15.
[50] Leveson, N., Engineering a Safer World, The MIT Press, Cambridge, UK, 2011.
[51] Bergman, B., "Conceptualistic Pragmatism: A framework for Bayesian analysis?" IIE Transactions, 41(1), 2009, 86-93.
[52] Deming, W. E., The New Economics, 2nd ed. MIT CAES, Cambridge, MA, 2000).

AUTHOR BIOGRAPHY

Enrico Zio (M'06–SM' 09) received the MSc degree in nuclear engineering from Politecnico di Milano in 1991 and in mechanical engineering from UCLA in 1995, and the Ph.D. degree in nuclear engineering from Politecnico di Milano and MIT in 1996 and 1998, respectively. He is currently Director of the Chair on Systems Science and the Energetic Challenge of the Foundation Electricité de France (EDF) at CentraleSupélec, Paris, France, full professor and President of the Alumni Association at Politecnico di Milano, adjunct professor at University of Stavanger, Norway, City University of Hong Kong, Beihang University and Wuhan University, China and Co-Director of the Center for REliability and Safety of Critical Infrastructures (CRESCI), China. His research focuses on the modeling of the failure-repair-maintenance behavior of components and complex systems, for the analysis of their reliability, maintainability, prognostics, safety, vulnerability, resilience and security characteristics, and on the development and use of Monte Carlo simulation methods, soft computing techniques and optimization heuristics.