Editorial

Roberto Setola*

Complex Systems and Security Lab,
Università Campus Bio-Medico di Roma,
via À. del Portillo, 21, 00128 Roma, Italy
E-mail: r.setola@unicampus.it
*Corresponding author

Enrico Zio

Chair Systems Science and Energy Challenge,
Ecole Centrale Paris and Supelec,
Grande Voies des Vignes,
92295 Chatenay-Malabry Cedex, France
E-mail: enrico.zio@ecp.fr
E-mail: enrico.zio@supelec.fr

Biographical notes: Roberto Setola received his Laurea in Electronic Engineering (1992) and PhD in Computer Science (1996) from the University of Naples. Since 2004, he has been with the University Campus Bio-Medico where he is currently an Associate Professor of Automatic Control, Director of the Complex System and Security Lab, and Director of the second-level Master in Homeland Security. He wrote three books about simulation of the dynamic systems, and is the editor of three books on homeland security and critical infrastructures. He is the author of more than 100 scientific papers about modelling and control of complex systems (electro-mechanical, biological and social) and critical infrastructure protection.

Enrico Zio received his MSc in Mechanical Engineering at UCLA and PhDs in Nuclear Engineering at Politecnico di Milano and at MIT. He is the Director of the Chair in Complex Systems and the Energetic Challenge of Ecole Centrale Paris and Supelec (funded by the European Foundation for the Energy of Tomorrow of Electricite' de France); Full Professor of Reliability, Safety and Risk Analysis at Politecnico di Milano; Adjunct Professor at the University of Stavanger, Norway and Universidad Federico Santa Maria, Chile, Chairman of the European Safety and Reliability Association. He is the co-author of five books and more than 170 journal papers.

Modern societies are strongly dependent on services provided by infrastructures characterised by tight integration, e.g., by means of pervasive use of modern information and communication technology (ICT), changing operational environments, e.g., market liberalisation and growing mutual dependencies. Failures of these systems can then be quite costly, as inconveniences and risks can be unacceptable and financial losses huge, as shown, e.g., by the August 14, 2003 blackout in North America which affected 50 million people and led to 3 billion USD insurance claims.

Additional societal concerns are brought into the picture by the threats coming from malicious/terrorist attacks and the hazards induced by extreme events (i.e., low probability, high impact events).

The infrastructures are highly complex systems whose behaviour is hard to understand or predict, as shown by research on complex networks that revealed the fact that system behaviours emerge from patterns of local responses, that some elements (nodes) can evolve to become more important and some structures (topologies) are more susceptible against random failures or targeted attacks than others. Control and reduction of infrastructure vulnerabilities call for good system understanding and preventive analyses, efforts for which established frameworks and methods seem to be still missing or, if available, are not properly applied.

The application of classical risk analysis methods for the study of the vulnerabilities of infrastructures stands on the equation:

$$R = P \times C \times V \tag{1}$$

where P is the probability of a given damaging event (being it the failure of a component or an earthquake), C are its consequences with respect to the scenarios which develop from the event and V measures the vulnerability of the infrastructure/system to the considered event. The 'first' factor, P, can in principle be 'quantified' on the basis of past experience and historical data. However, this is not trivial for critical infrastructures and the hazards and threats they are exposed to, especially malicious attacks.

This is due to the fact that in a very short period of time, about five to ten years, as a consequence of market globalisation, we moved from monolithic infrastructure architectures, where a monopolistic owner managed vertically integrated and isolated solutions, to a situation characterised by a parcelled and shared ownership, bringing an exponential increment in the point-of-contacts with outside entities of quite diverse sizes (e.g., the electric market in Italy until 2000 was substantially managed by the national operator ENEL, whereas nowadays it is shared by more than 3,000 interacting players). This has imposed to the operators the obligation to give up in-house or 'exclusive' service providers to apply to the open market with the consequences that the different services (even if more economic and efficient) are less tailored on the operators' needs and, for some aspects, more fragile. These phenomena were quite significant for ICT services. Indeed in this sector, due also to the need to overcome the millennium bug, there was a change from legacy (largely proprietary) systems to architecture based on off-the-shelf components. An immediate consequence of this is that no operator is able to guarantee by itself its own survivability, as it needs services provided by others.

From a risk analysis point of view, this represents a new challenge. Indeed, besides the 'specific' risks, each operator is exposed to interdependent risks and 'global threats'.

Here, with the term interdependencies, we refer to domino effects, i.e., an event occurred in a location/infrastructure cascading onto other locations/infrastructures and by so doing amplifying its negative impacts. On the other side, the term 'global threats' indicates the fact that an attack to a specific target can be conducted via a remote action, where remote has to be intended both in the geographic sense and in the sense that the attack can be performed on a supplier (or a supplier of the supplier) of the target.

The above considerations lead to the need for a change in approaching the problem of vulnerability of critical infrastructures. An analysis aimed at identifying the causes of damage or disruption of services in such systems requires an *all-hazard approach*, encompassing a more general view on the hazards targeting the systems. In particular, the approach must handle also malevolent acts, which differ from natural or other man-made hazards and lack of a well-established methodology for uncertainty assessment. The all-hazard approach can provide the basis for addressing unexpected events of any kind. This requires the capability of identifying the vulnerability sources and issues, given the infrastructure's technical and physical features and the dependencies and interdependencies on other systems, and evaluating the susceptibility to the different hazards, including threats of malevolent acts. Whereas the susceptibility to hazards leading to random failures can be quantified in terms of probability, the susceptibility to intentional malevolent acts lacks a well-established framework for the evaluation.

In this scenario, this special issue aims at setting the state of the art, both in research and application, by providing an opportunity for presenting recent achievements with regards to the development and application of models and techniques for the analysis of the vulnerability, reliability and safety of distributed networks, systems and critical infrastructures. To this end, some methodological papers illustrating different approaches of analysis are blended with contributions of application to illustrative case studies. Specifically, the first paper, by H. Medal et al., surveys the paradigm of risk analysis for critical infrastructures, describing modelling approaches and classifying them in terms of several characteristics.

The paper by M. Theoharidou et al. considers the problem to provide to policy makers tools able to prioritise national investments on security; a method is illustrated for qualitative risk estimation, focusing on the consequences to the society. On a more operational level, tools such as fuzzy cognitive maps can be adopted as suggested by M. Ferrari et al., by way of an example of analysis of the vulnerabilities of supply chains and their related infrastructures.

However, to move towards quantitative instruments, there is the need to introduce metrics. To this end, the paper of G.A. Coles et al. provides resilience measures for critical infrastructures using the probabilities of attack or hazardous events and considering the resilience of the system along different dimensions.

In F. Baiardi et al. the implications of unbounded impacts to the practice of risk mitigation for billing infrastructures are discussed, while the paper from F. Flammini et al. shows how to design security systems using genetic algorithms for the optimisation of some parameters.

As a concrete case study, the article by J. Yliskylä-Peuralahti et al., analyses the vulnerabilities in the transport sector, on the basis of a series of interviews regarding the impact on Finnish companies of the 16-day long port closure due to a stevedore strike occurred in March 2010.

Starting from the accident occurred in Pirkka Water (Finland), A-M. Heikkilä et al. present the problem of the protection of critical infrastructures, and in particular the interconnection of threats. Finally, C.W. Karvetski et al. provide an analysis of the vulnerabilities of the Alaskan coastal system due to climatic changes.

At the conclusion of the efforts for setting up this special issue, relieved by the end of the work, we would like to thank all the persons that in different ways have been involved in this accomplishment and in particular all the contributors and the reviewers.

Finally, a special thanks goes to Maria Carla De Maggio: without her precious support in the handling and management of the contributions and reviews, this special issue would not have been possible.