Foreword

Claude Chaudet and Gwendal Le Grand

Telecom Paristech
Paris, France
E-mail: claude.chaudet@enst.fr
E-mail: gwendal.legrand@enst.fr

Vittorio Rosato*

Ente per le Nuove Tecnologie, l'Energia e l'Ambiente (ENEA)
Rome, Italy
and
Ylichron Srl., Rome, Italy
E-mail: rosato@casaccia.enea.it
*Corresponding author

Biographical notes: Dr. Claude Chaudet is currently an Associate Professor at Telecom Paristech, formerly the Ecole Nationale Superieure de Telecommunications (ENST), in the INFRES department. His research activities are focused on *ad hoc* and sensor networks and on critical infrastructures protection (modelling and simulation of abnormal behaviour).

Dr. Gwendal Le Grand is an Associate Professor at Telecom Paristech, formerly the Ecole Nationale Superieure de Telecommunications (ENST). His main research areas are the security models for critical infrastructures and the analysis of the quality of the services of networks, particularly when connected to infrastructures.

Dr. Vittorio Rosato is a Senior Staff Scientist at ENEA. His main research areas are complex systems models of critical infrastructures and methods for high-performance computing. He is also the co-founder of a high-tech company (Ylichron Srl) active in the field of solutions for high-performance computing.

1 Introduction

Critical Infrastructures (CIs) are often defined as large technological systems deeply entangled with the life and well-being of people. Transportation systems, energy provision (including gas and electricity), or even communication networks such as telephone or the internet fall into this category. Indeed, failures of such systems have potentially serious sociological and economical consequences.

In the past few years, several serious failures such as electrical blackouts or the spread of internet viruses have occurred, depriving users of fundamental services during a noticeable period. As the threat of malicious and intelligent attacks becomes an increasing concern, ensuring the safety and robustness of these systems has become a

priority of governments. Several research initiatives have been launched to characterise CIs and their vulnerabilities and to devise efficient solutions against the potential threats they might face. In the USA, reinforced by President Clinton's presidential directive in 1998 and President Bush's directive in 2003, a large-scale national programme called Critical Infrastructures Protection was launched in 1996 to keep under control 13 types of infrastructures. In Europe, aside from national programmes, several research projects have been launched since the Fifth Framework Program (FP5, 1998 to 2002).

CIs are often large systems, serving a great number of heterogeneous users. If in the past they were operated by one single operator or sometimes very few operators, the advent of liberalisation in the services markets is going to define a completely new scenario, where many different competing companies and public institutions, across political state borders, operate parts of the large-scale infrastructures. This will impose a change in the current analysis and control strategies in favour of new and decentralised methods. New technological trends (such as electrical microgeneration) will further impose this radical change.

The analysis of these systems is complex due to the scale factor and to mutual dependencies between CIs. If relationships between competing operators of the same domain are difficult to be characterised, partly due to economic reasons, the existence of dependencies between different types of CIs introduce another dimension within this complexity. Interdependencies are at the origin of cascade effects, which spread perturbations and inoperability from one infrastructure to the others. Cascade effects and long-range perturbations could be seen as 'emergent' phenomena as they are often triggered by the simultaneous coexistence of different inputs. For all these reasons, large and heterogeneous systems such as CIs can thus be considered excellent metaphors of Complex Systems (CSs).

As a recent example of the increased awareness of these problems and the expectancy of the scientific community on the impact of the CS, paradigm on this matter, we can look at the satellite workshop entitled 'Critical Infrastructures as Complex Systems', organised as a side event of the 2007 European Conference on Complex Systems. The aim was to bring together computer scientists and technological operators of CIs to foster new, and unconventional, collaborations on themes related to the analysis and the control of these systems. It follows the directions identified by the IRRIIS FP6 integrated project[1] which aims at increasing the dependability, survivability and resilience of information-based infrastructures by the specification and development of a middleware layer and a global simulator to allow joint modelling and optimisation starting from electrical and telecommunication infrastructures. The outcome of the workshop confirmed that many questions regarding the protection of these infrastructures remain open.

In this special issue, much in the same spirit as the previously described workshop, we have intended to put together a number of contributions coming from different areas of CSs, from that modelling infrastructure topology, to that focusing on either physical or functional models of CIs, to that identifying and characterising failure scenarios, including the effects of interdependencies between infrastructures, in order to identify and build the appropriate components to perform early detection of cascading failures. Mitigation and resolution of the failures' effects, either through decision support systems or through fast and reliable reconfiguration mechanisms, are also attracting several scientists.

The contribution of Schmitz (IABG, Germany) describes tools for Critical Infrastructure Protection and how to design infrastructures as fault-tolerant systems. Although redundancy and self-healing are approved design principles, they imply increasing costs, which cannot always be afforded by the private sector. However, since the security of CIs has a high societal importance, new business models and security technologies have to be introduced that fulfil the interests of the private enterprises and the state.

The contribution of Salzano (University of Salerno, Italy) concerns the effect of globalisation on network nodes of different structural characteristics. The proposed simulation model could provide a better understanding of the onset of financial extreme events in the globalisation scenario.

Kajitani and Sagai (CRIEPI, Japan) present a model for describing and predicting interdependencies of CIs during natural disasters. While most interdependency studies remain at the qualitative level, they propose a quantitative analysis to estimate the service level of each CI at each location and each instance of a failure as well as their consequences (in terms of social and economic losses).

Balderer *et al.* (ETH Zurich, Switzerland) propose the outcome of their study on repair strategies for minimising the risks of cascading failures in electricity networks. A power operator generally does not have enough time to repair failed lines once a cascade has started, because cascading failures typically evolve in time scales of seconds and minutes. Consequently, their paper focuses on repair strategies during normal operation, when there are typically some lines that are not functioning due to random failures or maintenance work.

Issacharoff *et al.* (TU Dresden, Germany) present the evolution of a high-voltage electricity networks topology, which represents an example of an evolving complex system. This paper discusses the growth of the French electricity transmission network from 1960 to 2000. The growth of the network is compared to economic and demographic indicators to identify factors that correlate with the growth rate of the electricity network. The evolution of other parameters like code connectivity degree and information centrality is observed through time.

De Porcellinis *et al.* (University Campus Biomedico and RomaTre, Rome, Italy) discuss a Mixed Holistic Reductionistic (MHR) model that fuses into a single model the positive characteristics of both holistic and reductionism approaches. MHR adopts macrocomponents decomposition but analyse the atomic behaviour of these components on the base of the characteristics and services provided by the different infrastructures managed as a single entity. Specifically, in this model, each infrastructure is decomposed into its macrocomponents and each one is described with a 'reductionistic' philosophy on the base of the availability of resources, services and taking into account the presence of failures. However, to describe how these resources/failures are provided to each single macrocomponent, MHR considers a holistic model of the different infrastructures where global parameters are evaluated and used. The authors also demonstrate how MHR can be successfully applied to model real test-bed scenarios focused on an Italian region where the electric power grid and wireless and wired communication networks are tightly coupled.

Delamare *et al.* (ENST, France) present a high-level modelling of CIs interdependencies. They study the effect of interdependencies on the telecommunication networks and the electricity networks. In some cases, self-healing mechanisms may be misled by a wrong interpretation of information. For instance, the lack of reception of monitoring messages for a part of an electric infrastructure may indicate either a real electrical failure or a failure of the telecommunication network. These two causes are indistinguishable and lead to the same response. The authors study these cascading phenomena from a high level of abstraction, using classical modelling tools such as graph theory. They also analyse, on potential topologies, the effect of simple failures, and derive potential risk scenarios and guidelines for some strategies that operators may apply to prevent such cascading failures.

Gadomski (ENEA, Rome) proposes a contribution related to a modelling methodology of complex, 'real-world', human-technology aggregates. This domain is a new subfield of 'systemics', and requires a strong interdisciplinary perspective. The main attention is on large human organisations whose mission is emergency and high-risk management. In such circumstances, the vulnerability of human decision networks is a main cause of serious human and organisation errors. The systemic sociocognitive engineering paradigms and the framework of the Top-down Object-based Goal-oriented Approach (TOGA) meta-theory is presented and applied as a meta-ontological platform, basic computational formalisation and knowledge-ordering tool.

We hope that these contributions will further strengthen the links between the CS community and that of CI technological operators, with the aim of developing new methods and tools to increase the infrastructures' resilience for ensuring their survivability under faults or attack scenarios.

Note

1 See http://www.irriis.org.