Editorial

Claudio Balducelli

National Agency for New Technologies
Energy and Environment (ENEA)
Via Anguillarese 301, 00062 Rome, Italy
E-mail: claudio.balducelli@casaccia.enea.it

Biographical notes: Claudio Balducelli has a Master's degree in Physics and has been a Senior Scientist working at ENEA as Project Manager since 1983 in the field of AI technologies applied to operator decision support systems for industrial accidents management and critical infrastructure protection. His interests include operator models, knowledge formalisation, planning, computerised procedures, plant diagnosis, case-based reasoning, learning and fuzzy algorithms.

1 Critical infrastructure protection and emergency management

This issue of the *International Journal of Emergency Management* is dedicated to the theme 'Critical infrastructures protection'. It is a new theme for the emergency management community, and its significance has increased during the last years, since governments and citizens became aware that services furnished by power distribution networks, telecommunication networks, transport infrastructures and other key resources are actually more critical than in the past. To maintain their style of living, modern societies are more dependent on their critical infrastructures; but, ironically, critical infrastructures seem to be less stable than in the past. These new types of vulnerabilities are candidates to having a strong impact in the future emergency management practices and social security strategies.

The need for protecting critical infrastructures becomes more important also as a consequence of the so-called 'cascading effect', caused by the mutual 'interdependencies' of the networks. There are different causes and external conditions that contribute to augmenting such type of interdependency. When we consider critical infrastructures, we have to take into account that they are not simply 'physical' plants and networks. In fact, they contain not only a physical layer, but are also made of 'cyber' components and systems, and include human organisations to manage and supervise the daily operations of the infrastructure.

2 Cyber instabilities

Cyber and organisational layers control the physical parts of the infrastructures, and, first of all, have to consider and try to reduce the potential instabilities of the physical network. But the globalisation of the markets and the competition make both computer systems and human organisations more vulnerable and exposed to external threats.

To improve information support for the citizens, information technology components have become more complex, and their communication and interoperability capacities increased. But the vulnerability points of the computer systems and their attack possibilities have also increased, as cyber-attackers can exploit the remote automation mechanisms of the systems.

Sources of instabilities in the cyber layers are also caused by loss of employees or industry operators with critical skills. The introduction of a new generation of information/control systems often requires more knowledge/expertise about these new technologies. But frequently, the companies are afraid about the introduction of new technologies, and at the same time, the oldest ones are not competitive anymore.

To reduce personnel cost, many energy distribution companies promote the utilisation of 'remote' maintenance of devices and cyber components utilising the internet connectivity. But this new type of connectivity can be used also by malicious users or cyber-terrorists to damage the network functionality.

3 Organisational instabilities

Instabilities also increase inside the human organisations' managing infrastructures. To compete with the new transition economy countries, it is often necessary to reduce the organisational costs, which for a company are determined by the competition with other similar companies.

For electricity companies, new deregulation strategies impose operating inside an energy market in which energy can be imported at lower costs from different countries. The same energy production plants become less competitive than in the past, and the organisational costs must be reduced. One of the main reasons of the electrical network instability, which in September 2003 generated the collapse of the Italian grid, came from the large amount of energy imported by Italy from France. The cost of this energy is lower if transferred in the night period. This determines a higher amount of power flow coming from France to Italy during the night. But in such condition, when fewer generators are in operation, the total voltage stability margin is narrow, and the network has less degrees of freedom to manage potential instabilities caused by the high cross-border power flow.

The increasing cost of oil induced many countries to promote the installation of new generation plants based on renewable energy production. But the supervisory and control systems of the actual transmission electrical network are 'not prepared' to properly manage these new types of autonomous plants. The consequence of the serious incident, which originated in the North German electrical grid during the night of 6 November 2006, was simply the European grid separation in three large islands, but, on this occasion, Europe risked a very large blackout, involving a lot of countries. One of the reasons of this incident was also attributed to voltage instabilities caused by the wind energy production plants, installed in the North of Germany by autonomous energy providers.

4 Final remarks

From the previous analyses, it is possible to recognise that many physical systems instabilities could be better understood considering the past emergency scenarios, and the possible future trend of infrastructures vulnerability may also be evaluated.

New types of instabilities that arise from the cyber and organisational layers must also be better understood in the future. Risk and dependability analyses not only have to deal with physical systems but must also be applied to socio-technical systems. This new type of risk analysis have to deal with the interdependency problem typical of complex systems. It is necessary to have a better understanding of how some vulnerabilities or attacks inside the cyber and organisational layer could generate or amplify instabilities in the physical systems. At the same time, it is necessary to know how stable a physical system must be, against possible collapse in the presence of instabilities coming from the cyber/organisational layers.

5 The March 2006 International Workshop CNIP06 in Rome (Italy)

In March 2006, the Italian Agency for New Technology, Energy and Environment (ENEA) decided to organise, in collaboration with The International Emergency Management Society (TIEMS), an international workshop on Complex Network & Critical Infrastructure Protection (CNIP06), to explore new challenges and promote a multidisciplinary approach within the scientific community to protect critical infrastructures against new threats, vulnerabilities and interdependency problems.

Following the indications coming from this workshop, eight papers are presented in this issue that could answer the following questions:

1 How to evaluate critical infrastructure vulnerabilities and recognise the causes of interdependencies (J. and H. Johansonn and H. Jonsson; C.W. Johnson)

2 How to define mitigation and recovery strategies (C. Flaherty; J. Hollman, J. Martì, J. Jatskevich and K.D. Srivastava)

3 How to build operative solutions and defence systems (R. Minciardi, R. Sacile and E. Trasforini; N. Mladineo, S. Knezic and N. Jajac; C. Balducelli, L. Lavalle and G. Vicoli)

4 How to mitigate vulnerabilities coming from human and organisational structures (C. Uhr and H. Johansson).