Foreword

Sandro Bologna

Italian National Agency for New Technology
Energy and the Environment (ENEA), Italy
Via Anguillarese, 301
00123 S. Maria di Galeria, Rome, Italy
E-mail: bologna@casaccia.enea.it

Biographical notes: Sandro Bologna received a degree in Physics from the University of Rome 'La Sapienza'. He has about 30 years' experience at ENEA and abroad, where he has covered different positions as Researcher, Head of Research Units and Head of Research Projects at national and international levels. His main research activities deal with the achievement and assessment of computer-based system safety and reliability, large networks vulnerability analysis and critical infrastructure protection. In these fields, he has co-authored several scientific publications and books and served in the editorial board of different international journals.

The Italian National Agency for New Technology, Energy and the Environment (ENEA), in cooperation with The International Emergency Management Society (TIMES), organised a conference entitled *Complex Network and Infrastructure Protection* (CNIP06), on 28–29 March 2006. This Conference brought together over 200 delegates of different nationalities representing research centres, universities, private sectors, governments and international organisations. Its goal was to have a complete picture of what was going on in this subject in Europe, USA, Australia and Canada. This initiative is in keeping with the primary function of ENEA, which is to deal with emerging and challenging industrial R&D topics.

The motto of the conference can be summarised in the statement 'Interdependence is the *big deal* of the new century'. Critical Infrastructure Interdependence will be a major problem, which nations should be able to face from hereon. Unfortunately, this has been proven and confirmed from the many blackouts in the last few years.

Major blackouts that paralysed the electrical grid on the US East Coast and in different countries in Europe from the year 2003 onwards, and more recently the so-called 'gas crises' in several European countries, are just examples of the increasing interdependence of energy infrastructures. The same applies, with an even potentially stronger impact on societies, with communication and information infrastructures. Faults or attacks to the cyber layers controlling the interconnected telecommunication networks could block communications for many hours. A fault on a telecommunications satellite could block all the cellular telephones in a fairly wide area. The fact that information technology is pervading all other infrastructures just like electricity supply – on which it is, in turn, strongly dependent – does make for closer interdependence.

Copyright © 2008 Inderscience Enterprises Ltd.

Control systems constitute the central nervous system of energy infrastructures. They include large networks of interconnected electronic devices that are essential in monitoring and controlling the production and distribution of energy through the electrical grid and the oil and gas transportation networks. The ability of these cyber systems to provide remote control over a large, dispersed network of assets and components has helped to create the highly reliable and flexible energy management infrastructure we have today. However, this span of control requires control systems to communicate with thousands of nodes and numerous information systems, thus exposing energy systems and other dependent infrastructures to potential harm from natural disasters, malevolent attacks conducted via physical or cyber initiatives, as well as hardware or software malfunctions. Major stakeholders of the energy sector and the same national governments have recognised the need to invest resources and efforts to improve control system security as an essential component of the global effort for infrastructure protection.

Information and communication networks today play a central role for each domain of activity and are used to control all other critical infrastructures. Their strong interconnection, however, leads these systems to be surprisingly vulnerable, also because public communication networks, both cabled and wireless, are becoming widely used instead of proprietary networks. A long-term vision for the control of modern critical infrastructures will require a vigorous programme of fundamental research to explore basic scientific aspects and technological efforts necessary to develop new strategies to increase systems' resilience, for their real-time analysis and control and for their self-healing, and to go beyond the simple protection from outside attacks. This strongly imposes a multidisciplinary R&D approach to handle the new challenges.

Although the risk of negative interactions between technological networks and consequent blackouts will always be possible, a general rule to be applied to reduce this threat is that of a better *integration*: between adjacent systems, of public and private decisions and plans, between academia and industry, and of nations and continents. But there are no simple rules for wide-ranging interdisciplinary, international integration. This is a challenge requiring intelligence and dramatic upgrading of cultural levels – above all, among people that have the responsibility to steer and look ahead in the future.