Foreword

Sandro Bologna

AIIC – Italian Association of Critical Infrastructures Experts,
Piazza dell'Esquilino 29, 00185 Roma, Italy
E-mail: s.bologna@infrastrutturecritiche.it

Biographical notes: Sandro Bologna received his degree in Physics from the University of Rome 'La Sapienza'. He has more than 40 years experience with the Italian National Agency for New Technologies, Energy and Sustainable Economic Development (ENEA) and abroad, where he has covered different positions as Researcher, Head of Research Units, 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 this field, he has co-authored several scientific publications and books and served in the editorial board of different international journals. Currently, he is the President of the Italian Association of Critical Infrastructures Experts.

This special issue is based on papers selected from the 6th International Conference on Critical Information Infrastructures Security, held in Lucerne, Switzerland, September 8th and 9th, 2011, in short CRITIS'11. All papers in this special issue were completely rewrote and thoroughly reviewed by several distinguished experts in a blind review process and have been revised to reflect these reviews.

The papers selected reflects the breadth of on-going research in the field, ranging from a worldwide survey of nations that have already issued a cyber security plan to the problem of interdependence and cascading effects, different aspects of SCADA cyber security and resilience.

The scale and complexity of present and future cyber – physical systems (e.g., communication networks, smart grids, cloud computing), along with its increased connectivity and automation, make the task of their protection very challenging. Recently, security researchers and standards bodies have begun to develop socio-technical requirements and potential solutions for protecting complex cyber – physical systems. However, their protection remains very challenging. Important questions arise when identifying priorities for design and protection: Which components, if compromised, can lead to significant service delivery disruption? What topologies are inherently robust to classes of cyber attack? How to do dependencies analysis of critical services and impact assessment of possible cascading failures? A key research challenge in addressing these fundamental questions lies in the effective understanding of the cyber-physical synergy. This gives rise to the problem of protecting cyber-physical systems. In this special issue, we present a number of complementary approaches to address the problem.

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 and cascading effects.

Control systems constitute the central nervous system of any modern infrastructure. They include large networks of interconnected electronic devices that are essential in monitoring and controlling the functioning of the infrastructure. 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 infrastructures management we have today. However, this span of control requires control systems to communicate with thousands of nodes and numerous information systems, thus exposing any large infrastructure to potential harm from natural disasters, malevolent attacks conducted via physical or cyber initiatives, as well as hardware or software malfunctions. Major stakeholders of critical infrastructures 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 infrastructure will require a vigorous programme of fundamental research to explore basic scientific aspects and technological efforts necessary to develop new strategies to increase system's resilience, for their real-time analysis and control, for their self-healing, to go beyond the simple protection from outside attacks. This strongly imposes a multidisciplinary R&D approach to handle the new challenges. This special issue wish to be just a small contribution in this direction.

The guest editor would like to thank all the authors, and also all the others that have made an important contribution to the development of the special issue, listed as follows.