Introduction

Christian Esposito*

Institute for High Performance Computing and
Networking of the Italian National Research Council (ICAR-CNR),
Via Pietro Castellino 111 – 80131, Napoli, Italy
E-mail: christian.esposito@na.icar.cnr.it
*Corresponding author

Marco Platania

Department of Computer Science,
Johns Hopkins University,
3400 North Charles Street, Baltimore, MD 21218, USA
E-mail: platania@cs.jhu.edu

Francesco Brancati

Resiltech,
Piazza Iotti, 25, 56025 – Pontedera (PI), Italy
E-mail: francesco.brancati@resiltech.com

Large-scale complex critical infrastructures (LCCIs), such as water and power supply plants, transport infrastructures (e.g., airports and seaports) or distributed health information systems, play a key role into several fundamental human activities. It is easy to think about their economic and social impact: the consequences of an outage can be catastrophic in terms of efficiency, economical losses, consumer dissatisfaction, and even indirect harm to people and deaths.

Currently, the extensive usage of information and communications technology (ICT) (e.g., computing systems, communication networks, and sensing hardware), is at the base of future LCCI development like smart grids for energy control and distribution, or mobile cyber-physical infrastructures. These type of systems rely on software systems for advanced monitoring and control facilities in order to assure LCCIs interconnection, control, and management. These systems have to be highly resilient in order to reduce the risk of LCCI catastrophic failures. Nevertheless, the resiliency of current and future LCCIs is compromised by several factors, which can be intentional and unintentional. First, these systems are more and more conceived as the composition of several off-the-shelf (OTS) items and/or legacy subsystems, increasing the probability of failure occurrences, due to unexpected or erroneous modes of operation. Second, they have been designed without considering that their size would have significantly grown, crossing national boundaries, and that their operational environment, originally planned to be 'closed', would become 'open' to the world to allow interoperability among LCCIs and remote access and control. This implies that both accidental events and malicious attacks should be taken into account.

The novel challenges imposed by LCCI cause the unsuitability of the current solutions. In fact, existing solutions are usually applied to simpler and closed system. The innovative and challenging aspect is to apply these available strategies, or to define novel ones, in the context of complex, evolvable, and extremely heterogeneous systems, which will compose future LCCI systems. It is needed to define novel middleware technologies, models, and methods to assure and assess the resiliency level of current and future OTS-based LCCIs, to diagnose faults in real time, and to tolerate them by means of dynamic reconfiguration. Assuring the resiliency level of LCCIs is crucial to reduce, with known probabilities, the occurrence of catastrophic failures, and consequently, to adopt proper diagnosis and reconfiguration strategies.

This special section hosts three research papers in the dependability and security for LCCIs. They are the result of a selection from manuscripts in response to an open call for papers following the 1st International Workshop on Dependable and Secure Computing for Large-Scale Complex Critical Infrastructures (DESEC4LCCI), which took place in Magdeburg (Germany) in 2012 jointly to SAFECOMP 2012. All papers received peer reviews by expert referees and three papers were selected for inclusion in this special section.

The first paper is entitled 'Stochastic assessment of power systems in presence of heterogeneity' and is authored by Silvano Chiaradonna, Felicita Di Giandomenico and Nicola Nostro. Power grids are seen as a critical part for several national assets with an impact on security, national economic security, national public health or safety. To accommodate recent demands for higher safety and efficiency, they are undergoing a radical rethinking where the traditional electric control systems are coupled with more advanced ICT infrastructures. The paper studies the interdependencies between the traditional electric power grid and of the cyber control infrastructure in critical scenarios by means of models.

The second paper is entitled 'Secure healthcare data sharing among federated health information systems' and is authored by Mario Sicuranza, Mario Ciampi, Giuseppe De Pietro and Christian Esposito. Health information systems are considered critical system, requiring reliable and secure messaging over wide-area networks. The current debate around these systems is their progressive integration due to the increase of patient mobility, which requires a proper exchange of medical data. This paper shows how federated Health Information Systems can offer security properties by adopting proper mechanisms to protect the exchanged data and the provided functionalities from malicious manipulations.

The last paper is entitled 'SIREN: a feasible moving target defence framework for securing resource-constrained embedded nodes' and is authored by Ermanno Battista, Valentina Casola, Antonino Mazzeo and Nicola Mazzocca. Pervasive wireless sensor nodes are being used within the context of several innovative critical monitoring applications, such as smart grid monitoring, crowd-source sensing and mobile cyber-physical infrastructure. Due to their importance of their role, sensors have to be protected from different attacks and failures, which could limit their functionality. The paper provides the application of techniques for embedded nodes to autonomously reconfigure the system, so as to improve the provided security level.

In conclusion, our special thanks go to the Editor-in-Chief, Dr. Francesco Flammini, for providing us the opportunity to have a special section on 'Section on dependable and secure computing for large-scale complex critical infrastructures' hosted by the *International Journal of Critical Computer-Based Systems*.

We thank all of the authors who submitted to this special section and the anonymous reviewers for their deep and constructive evaluations of the manuscripts.