Introduction

Stefano Marrone*

Dipartimento di Matematica e Fisica,
Università della Campania 'Luigi Vanvitelli',
viale Lincoln, 5, 81100 Caserta, Italy
Email: stefano.marrone@unicampania.it
*Corresponding author

Ricardo J. Rodríguez

Centro Universitario de la Defensa,
General Military Academy,
Carr. de Huesca s/n, 50090 Zaragoza, Spain
Email: rjrodriguez@unizar.es

Biographical notes: Stefano Marrone is an Assistant Professor in Computer Engineering at the Università della Campania 'Luigi Vanvitelli'. His interests include the definition of model driven processes for the design and the analysis of transportation control systems, complex communication networks and critical infrastructures and in the use of formal methods to critical systems design. He is involved in research projects with both academic and industrial partners. He has authored more than 50 papers appeared in international proceedings of conferences and journals.

Ricardo J. Rodríguez is an Assistant Professor at the Centro Universitario de la Defensa, General Military Academy, Zaragoza, Spain. His research interests include survivability analysis, computer forensics, and industrial cybersecurity. His professional experience includes the participation in several research projects from public and competitive national and international fundings, as well as from private fundings. He is involved in reviewing tasks for international conferences and journals and has authored more than 40 papers appeared in peer-reviewed international conference proceedings and indexed journals.

Modern society relies on large, heterogeneous, and complex software-intensive systems to support all kinds of daily activities. Services such as urban transportation, logistics, healthcare, data communication, railway, aerospace, and power distribution, among others, are becoming heavily dependent on the availability of such systems. Furthermore, any service discontinuity may lead to a loss in people's livelihoods, from severe financial losses to fatalities or injuries. The causes of these discontinuities may be very diverse, from human errors or unexpected acts of nature to intentional attacks like sabotage or terrorism. Safety and security (S&S) assessments in critical infrastructures measure how these disruptions are handled and quantify the impact suffered by the critical infrastructure under abnormal operation.

This special issue is devoted to the research advancements on the methods for the design and the assessment of dependability, safety, and security in these infrastructures.

While traditional assessment methods are based on analytical or simulation techniques, often addressing one single specific aspect at a time, new methods are due which study these infrastructures in a holistic manner and integrate the assessment methods with emerging data-driven paradigms.

Kaur and Sharma propose a systematic and quantitative process to model and rank non-functional requirements (NFRs). As society needs more and more reliable computer applications, a tool for managing NFRs is paramount importance to allocate budgets and to identify conflicts between such requirements.

Breuer and Bowen introduce an architecture for a high-performance microprocessor based on the principle that non-standard arithmetic generates encrypted processing. The paper focuses on the standard OpenRISC instruction set and a demonstration of the security of the proposed platform is provided in conjunction with an evaluation of processors performance.

The paper of Howard, Butler, Colley and Sassone aims to enable designers/assessors for an integrated S&S analysis of cyber-physical systems, particularly in a critical infrastructure context. An STPA-like methodology is presented in this paper, based on the well-known formal method of Event-B.

This special issue also incorporates two surveys about dynamical updating and software patching of software, framing the same problem from two different points of view.

Lounas, Mezghiche and Lanet focus on the theoretical frameworks that enable us to formally guarantee the safety and the security in systems where patches and updates must be installed without shutting down the system itself (dynamic software updating – DSU). The paper ends highlighting some challenges to this new trend in software dependability: taking into account DSU problem in the early phases of the system design and defining proper methods to understand the most suitable methods in relation to the different DSU process acceptance criteria.

In the last paper, Gentile and Serio deal with the problem of patch management standards applicable in the field of industrial control systems (ICSs). The paper ends proposing a patch management workflow, formalised in the BPMN language and currently adopted in one of the most complex industrial setting: the CERN laboratory in Geneve (Switzerland).

Some of the papers appearing in this special issue extend papers submitted and presented in two editions of the S4CIP workshops: the 1st Workshop on Safety & Security aSSurance for Critical Infrastructures Protection (S4CIP'16) and 2nd Workshop on Safety & Security aSSurance for Critical Infrastructures Protection (S4CIP'17).

As guest editors of this special issue, as well as S4CIP workshop co-chairs, we would like to thank all the PC members and external reviewers that helped us to improve the quality of the presented papers. We would like also to thank the Editor-in-Chief Dr. Francesco Flammini for hosting this special issue.