Guest editorial: special issue on emerging challenges in software certification and verification

Luigi De Simone[1] · **Nuno Laranjeiro**[2] · **Domenico Cotroneo**[1]

Software is pervasive in our society: its scope is widening more and more in many critical domains such as avionics, space, railway, automotive, nuclear, medical, air traffic control, and more recently in domains such as 5G networks in the telecom industry, and smart factories in Industry 4.0. Applications in these domains must adhere to stringent safety, security, and privacy requirements, which are imposed by regulations and by market expectations. Despite several standards for the certification of safety and security being proposed and matured over the years, we are facing new challenges towards the certification and verification of modern software systems.

This special issue of the *Software Quality Journal* presents innovative, high-quality papers which address challenges depicted above from different perspectives.

The first group of papers analyzes certification aspects when machine learning (ML) approaches are used. *Stirbu et al.* use the DevOps paradigm in ML-based medical systems to comply with the regulatory frameworks for medical device certification. *Borg et al.* report a safety assurance analysis of an ML-based pedestrian automatic emergency braking system by presenting their experience within an industry-academia collaboration in the application of high-level guidance for the assurance of ML in autonomous systems.

The second group of papers focuses on autonomous driving safety, testing embedded systems, and formal verification in the automotive domain. *Alcon et al.* provide a mapping between safety requirements and the implementation of ISO 26262 *dynamic views* of an autonomous driving framework, by proposing new execution views in the context of Multiprocessor System on a Chip (MPSoC) targets. *Song et al.* develop an approach to prioritize critical test scenarios in real industry-related autonomous driving systems. *Dirim et al.* propose heuristics and integer linear programming algorithms to improve test case prioritization for the certification of real smart TV applications. *Haur et al.* propose a novel

✉ Luigi De Simone
luigi.desimone@unina.it

Nuno Laranjeiro
cnl@dei.uc.pt

Domenico Cotroneo
cotroneo@unina.it

1 Dipartimento di Ingegneria Elettrica e delle Tecnologie dell'Informazione (DIETI), Università degli Studi di Napoli Federico II, Naples, Italy

2 Centre for Informatics and Systems of the University of Coimbra, Department of Informatics Engineering, University of Coimbra, Coimbra, Portugal

method to formally verify real-time OSes according to AUTOSAR specification by using colored Petri nets.

The third group of papers addresses quality traceability and use of modeling languages in safety-critical applications. Specifically, *Sharifi et al.* target software quality attributes by proposing a novel approach based on architectural patterns and tactics, with the aim to trace runtime quality attributes. *Micskei et al.* contribute into the context of the assessment of the specification of modeling language semantics by analyzing the *Precise Semantics of UML State Machines (PSSM)*.

Finally, *Lombardi et al.* present an extended version of the *DevSecOps* model by integrating cybersecurity aspects, i.e., additional activities for vulnerability assessment and analysis of software dependencies in the context of security standards.

We are grateful to the authors that contributed to this editorial initiative with their valuable work, and to the anonymous peer reviewers that helped us to select the best papers and to improve them over two rounds of reviews. Moreover, we are grateful to SQJ Editor-in-Chief Rachel Harrison for her support and cooperation, and Vincent Salvo for timely and continuous support.