Quality of information and communication technology introduction

Marion Lepmets¹ · Marjan Mernik² · Miguel Abrunhosa de Brito³

Published online: 25 February 2021

© The Author(s), under exclusive licence to Springer Science+Business Media, LLC part of Springer Nature 2021

1 Introduction

This Special Issue of Quality of Information and Communication Technology presents papers on advanced methods, techniques, and tools for supporting quality approaches to ICT engineering and management.

Software safety and security are increasingly important topics today as more and more software is embedded into our homes, cars, trains, airplanes, and hospitals each day.

Most software developers have to consider safety and security requirements in their work to ensure that the systems around us will support our everyday lives and not harm us. New approaches are being developed and international standards updated to ensure the safety of these software systems before they are delivered.

Safety-critical domains such as automotive, healthcare and medical devices, space and nuclear energy all have a number of common challenges when software is being developed and embedded into their systems. Namely, adopting a safety- and risk-centric approach to the software and system development while facing the very same commercial demands of speed and access to market as generic software developers. How then can agile software development methods be used efficiently while meeting the safety, interoperability, and security demands of the safety-critical software systems? How can we ensure that software in safety-critical systems is interoperable with the rest of the system and without any internal or external security vulnerabilities? This special issue addresses the issues of software safety and security, interoperability, and risk-centric software development approach in the papers it contains.

The first paper of the special issue is written by Michaela Bunke and Karsten Sohr titled “Towards supporting software assurance assessments by detecting security patterns.” It describes a program comprehension approach to detecting security patterns in mobile applications that supports the implementation of security features in code. The approach

✉ Marion Lepmets
marion@softcomply.com

¹ SoftComply LTD, Bavariaring 24, 80336 Munich, Germany

² Faculty of Electrical Engineering and Computer Science (FERI), University of Maribor, Koroška cesta 46, Maribor, Slovenia

³ Information Systems Department School of Engineering, University of Minho, Campus de Azurém, P-4800-058 Guimarães, Portugal

is based on connected object process graphs (COPGs) containing interacting objects described by security patterns.

The second paper, written by Hamish Sadler titled “ER2C SDMLC: enterprise release risk centric systems development and maintenance life cycle,” proposes a novel systems development and maintenance life cycle model that models the life of a system as a sequence of releases under a unified consistent governance model. The paper proposes applying different levels of rigor depending on analyzed release risks via the enforcement of different thresholds to a set of metrics that are extracted from release artifacts. The proposed life cycle model supports iterative development and is conformant to ISO 15288:2015.

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.