Thesis for The Degree of Doctor of Philosophy
in Computer Science and Engineering

Understanding, Implementing, and Supporting Security Assurance Cases in Safety-Critical Domains

Mazen Mohamad

Department of Computer Science and Engineering

The thesis will be defended in public
on Wednesday, June 14th 2023 at 1pm
in Room Alfa, Saga Building, Hörselgången 4,
Campus Lindholmen, Gothenburg

Faculty opponent: Professor Arosha K. Bandara,
The Open University, Great Britain

UNIVERSITY OF GOTHENBURG

University of Gothenburg
SE-405 30 Gothenburg, Sweden
Phone: +46 31 786 0000

Abstract:

The increasing demand for connectivity in safety-critical domains has made security assurance a crucial consideration. In safety-critical industry, software, and connectivity have become integral to meeting market expectations. Regulatory bodies now require security assurance cases (SAC) to verify compliance, as demonstrated in ISO/SAE-21434 for automotive. However, existing approaches for creating SACs do not adequately address industry-specific constraints and requirements.

In this thesis, we present CASCADE, an approach for creating SACs that aligns with ISO/SAE-21434 and integrates quality assurance measures. CASCADE is developed based on insights from industry needs and a systematic literature review. We explore various factors driving SAC adoption, both internal and external to companies in safety-critical domains and identify gaps in the existing literature.

Our approach addresses these gaps and focuses on asset-driven methodology and quality assurance. We provide an illustrative example and evaluate CASCADE's suitability and scalability in an automotive OEM. We evaluate the generalizability of CASCADE in the medical domain, highlighting its benefits and necessary adaptations.

Furthermore, we support the creation and management of SACs by developing a machine-learning model to classify security-related requirements and investigating the management of security evidence. We identify deficiencies in evidence management practices and propose potential areas for automation. Finally, our work contributes to the advancement of security assurance practices and provides practical support for practitioners in creating and managing SACs.

Keywords:
Security, Assurance case, Safety-critical, Automotive systems, Arguments, Evidence, Security claims

ISBN: 978-91-8069-329-5 (PRINT)
ISBN: 978-91-8069-330-1 (PDF)