Lecture Notes in Computer Science 12852

More information about this subseries at http://www.springer.com/series/7408

Ibrahim Habli · Mark Sujan ·
Friedemann Bitsch (Eds.)

Computer Safety, Reliability, and Security

40th International Conference, SAFECOMP 2021
York, UK, September 8–10, 2021
Proceedings

Springer

Editors

Ibrahim Habli
University of York
York, UK

Mark Sujan
Human Factors Everywhere Ltd.
Woking, UK

Friedemann Bitsch
Thales Deutschland GmbH
Ditzingen, Germany

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-83902-4 ISBN 978-3-030-83903-1 (eBook)
https://doi.org/10.1007/978-3-030-83903-1

LNCS Sublibrary: SL2 – Programming and Software Engineering

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This volume (LNCS 12852) contains the proceedings of the 40th International Conference on Computer Safety, Reliability and Security (SAFECOMP 2021) held during September 8–10, 2021. Due to the continued COVID-19 pandemic, SAFECOMP 2021 took place as a hybrid event, offering both in-person presentations and limited attendance at the University of York, UK, in accordance with suggested precautions, as well as the opportunity to present and attend online. The conference series was established in 1979 by the European Workshop on Industrial Computer Systems, Technical Committee 7 on Reliability, Safety and Security (EWICS TC7). Since then, SAFECOMP has contributed to progressing the state of the art of dependable computer systems and their application in safety-critical and security-critical systems. SAFECOMP covers all areas of dependable systems, including embedded systems, cyber-physical systems, Internet of Things, systems-of-systems, cybersecurity, digital society, and many more. In recent years, autonomous systems, particularly those that incorporate machine learning models, have become increasingly important topics, and, in line with this development, the assurance of the safety and security of such systems in real-world applications is one of the highest and most challenging priorities. This is reflected in the keynote presentations as well as in the key theme of SAFECOMP 2021, which was “Safe Human – Robotic & Autonomous Systems Interaction”.

The International Program Committee consisted of 51 members from 18 countries. The review process was thorough, single-blind (i.e., authors did not know the reviewers’ identity), and each manuscript was reviewed by at least three independent reviewers. The merits of each paper were evaluated by the Program Committee members during a virtual meeting in April 2021. In total, after desk-rejecting papers that were beyond the scope of the conference or did not meet the essential formatting requitements, 76 submissions were peer-reviewed, and 17 manuscripts were selected for presentation and inclusion in the proceedings (an acceptance rate of 22%). We would like to thank all the reviewers and sub-reviewers for their contributions to ensuring an interesting and high-quality conference program.

We were pleased to host three stimulating keynote presentations. Prof. Adnan Darwiche (UCLA, USA) talked about “Empowering data with knowledge and reasoning”. Prof. Neville Stanton (Southampton University, UK) gave a provocative presentation about “Driver reactions to autonomous vehicles”. Prof. Sadie Creese (University of Oxford, UK) shared with the audience “Thoughts for a cybersecurity framework for protecting machine learning/AI systems”.

As in previous years, SAFECOMP was organized as a single-track event to enable participants to attend all sessions, and to allow for networking during breaks and social events, both in person as well as via the electronic conference platform. The main conference was preceded by a day of topical workshops. This year, there were five workshops: 16th International Workshop on Dependable Smart Embedded Cyber-Physical Systems and Systems-of-Systems (DECSoS 2021); 2nd International

Workshop on Dependable Development-Operation Continuum Methods for Dependable Cyber-Physical Systems (DepDevOps 2021); 1st International Workshop on Multi-concern Assurance Practices in Software Design (MAPSOD 2021); 2nd International Workshop on Underpinnings for Safe Distributed AI (USDAI 2021); and 4th International Workshop on Artificial Intelligence Safety Engineering (WAISE 2021). The papers presented at these workshops are published in a separate LNCS volume (12853).

We would like to express our sincere gratitude to the many people whose contributions made SAFECOMP 2021 possible: the authors who submitted manuscripts; the invited keynote speakers; Prof. John McDermid as conference chair; the Program Committee members and external reviewers; EWICS TC7 and chair person Prof. Francesca Saglietti; the conference sponsors and supporting organisations; Friedemann Bitsch as the publications chair; Erwin Schoitsch and Simos Gerasimu as workshop co-chairs; Simon Burton as the industry chair; and the local Organization Committee members Sarah Heathwood, Dawn Forrester, and Alex King, who managed all of the practical arrangements and who ensured that the conference was an interesting experience for all.

We hope that readers will find these conference proceedings interesting and thought provoking.

September 2021

Ibrahim Habli
Mark Sujan

Organization

EWICS TC7 Chair

Francesca Saglietti	University of Erlangen-Nuremberg, Germany

General Chair

John McDermid	University of York, UK

Program Co-chairs

Ibrahim Habli	University of York, UK
Mark Sujan	Human Factors Everywhere, UK

General Workshop Co-chairs

Simos Gerasimou	University of York, UK
Erwin Schoitsch	AIT Austrian Institute of Technology, Austria

Publication Chair

Friedemann Bitsch	Thales Deutschland GmbH, Germany

Local Organizing Committee

Dawn Forrester	University of York, UK
Sarah Heathwood	University of York, UK
Alex King	University of York, UK

Industry Chair

Simon Burton	Fraunhofer IKS, Germany

International Program Committee

Uwe Becker	Draeger Medical GmbH, Germany
Peter G. Bishop	Adelard, UK
Friedemann Bitsch	Thales Deutschland GmbH, Germany
Sandro Bologna	Associazione Italiana Esperti Infrastrutture Critiche, Italy
Andrea Bondavalli	University of Florence, Italy
Jens Braband	Siemens AG, Germany

Simon Burton	Robert Bosch GmbH, Germany
António Casimiro	University of Lisbon, Portugal
Peter Daniel	EWICS TC7, UK
Ewen Denney	SGT/NASA Ames Research Center, USA
Felicita Di Giandomenico	ISTI-CNR, Italy
Wolfgang Ehrenberger	University of Applied Science Fulda, Germany
John Favaro	Intecs, Italy
Massimo Felici	Deloitte Consulting & Advisory, Belgium
Francesco Flammini	Linnaeus University, Sweden
Simon Fuerst	BMW Group, Germany
Barbara Gallina	Mälardalen University, Sweden
Bruno Gonçalves	GMVIS Skysoft SA, Portugal
Janusz Górski	Gdańsk University of Technology, Poland
Jérémie Guiochet	LAAS-CNRS, France
Maritta Heisel	University of Duisburg-Essen, Germany
Joost-Pieter Katoen	RWTH Aachen University, Germany
Gulsum Kubra Kaya	Istanbul Medeniyet University, Turkey
Phil Koopman	Carnegie Mellon University, USA
Mark Lawford	McMaster University, Canada
Farah Magrabi	Macquarie University, Australia
Frank Ortmeier	Otto-von-Guericke University, Germany
Ganesh Pai	KBR/NASA Ames Research Center, USA
Philippe Palanque	ICS-IRIT, University Toulouse, France
Michael Paulitsch	Intel, Austria
Holger Pfeifer	Technical University of Munich, Germany
Peter Popov	City University London, UK
Andrew Rae	Griffith University, Australia
Alexander Romanovsky	Newcastle University, UK
Matteo Rossi	Politecnico di Milano, Italy
Francesca Saglietti	University of Erlangen-Nuremberg, Germany
Behrooz Sangchoolie	RISE Research Institutes of Sweden
Christoph Schmitz	Zühlke Engineering AG, Switzerland
Daniel Schneider	Fraunhofer Institute for Experimental Software Engineering IESE, Germany
Erwin Schoitsch	AIT Austrian Institute of Technology, Austria
Christel Seguin	Office National d'Etudes et Recherches Aérospatiales, France
Oleg Sokolsky	University of Pennsylvania, USA
Wilfried Steiner	TTTech Computertechnik AG, Austria
Kenji Taguchi	CAV Technologies Co., Ltd., Japan
Stefano Tonetta	Fondazione Bruno Kessler, Italy
Martin Törngren	KTH Royal Institute of Technology, Sweden
Mario Trapp	Fraunhofer Institute for Cognitive Systems IKS, Germany

Elena Troubitsyna	KTH Royal Institute of Technology, Sweden
Marcel Verhoef	European Space Agency, The Netherlands
Marcus Völp	University of Luxembourg, Luxembourg
Hélène Waeselynck	LAAS-CNRS, France

Sub-reviewers

Victor Bandur	McMaster University, Canada
Jana Berger	RWTH Aachen University, Germany
Andrea Ceccarelli	University of Florence, Italy
Lorenzo De Donato	University of Naples Federico II, Italy
José M. Gaspar Sánchez	KTH Royal Institute of Technology, Sweden
Magnus Gyllenhammar	Zenseact, Sweden
Richard Hawkins	University of York, UK
Yassir Idmessaoud	LAAS-CNRS, France
Shahid Khan	RWTH Aachen University, Germany
Ryo Kurachi	Nagoya University, Japan
Stefano Marrone	University of Naples Federico II, Italy
Yutaka Matsuno	Nihon University, Japan
Roberto Nardone	Università Mediterranea Di Reggio Calabria, Italy
Mark Nicholson	University of York, UK
Thomas Noll	RWTH Aachen University, Germany
Vera Pantelic	McMaster University, Canada
Michael Parsons	University of York, UK
Colin Paterson	University of York, UK
Chiara Picardi	University of York, UK
Muhammad Rusyadi Ramli	KTH Royal Institute of Technology, Sweden
Jan Reich	Fraunhofer Institute for Experimental Software Engineering, Germany
Toru Sakon	CAV Technologies Co., Ltd., Japan
Mehdi Saman Azari	Linnaeus University, Sweden
Thomas Santen	TU Berlin, Germany
Andreas Schmidt	Fraunhofer Institute for Experimental Software Engineering IESE, Germany
Kaustubh Sridhar	University of Pennsylvania, USA
Lifei Tang	KTH Royal Institute of Technology, Sweden
Maryam Zahid	Mälardalen University, Sweden

Gold Sponsor

Intel

Supporting Institutions

European Workshop on Industrial Computer Systems – Reliability, Safety and Security

University of York

Assuring Autonomy International Programme

Human Factors Everywhere Ltd

Austrian Institute of Technology

Thales Deutschland GmbH

Lecture Notes in Computer Science (LNCS), Springer Nature

Chartered Institute of Ergonomics & Human Factors

European Training Network for Safer Autonomous Systems

Safety-Critical Systems Club

European Network of Clubs for Reliability and Safety of Software-Intensive Systems

German Computer Society

Informationstechnische Gesellschaft

Electronic Components and Systems for European Leadership - Austria	ECSEL Austria
ARTEMIS Industry Association	ARTEMIS Industry Association
Verband Österreichischer Software Industrie	VÖSI VERBAND ÖSTERREICHISCHER SOFTWARE INDUSTRIE
Austrian Computer Society	OESTERREICHISCHE COMPUTER GESELLSCHAFT ® AUSTRIAN COMPUTER SOCIETY
European Research Consortium for Informatics and Mathematics	ERCIM European Research Consortium for Informatics and Mathematics

Contents

Machine Learning Safety Assurance

DeepCert: Verification of Contextually Relevant Robustness for Neural Network Image Classifiers 3
Colin Paterson, Haoze Wu, John Grese, Radu Calinescu, Corina S. Păsăreanu, and Clark Barrett

Could We Relieve AI/ML Models of the Responsibility of Providing Dependable Uncertainty Estimates? A Study on Outside-Model Uncertainty Estimates 18
Lisa Jöckel and Michael Kläs

Towards Certification of a Reduced Footprint ACAS-Xu System: A Hybrid ML-Based Solution 34
Mathieu Damour, Florence De Grancey, Christophe Gabreau, Adrien Gauffriau, Jean-Brice Ginestet, Alexandre Hervieu, Thomas Huraux, Claire Pagetti, Ludovic Ponsolle, and Arthur Clavière

Security Engineering

IT Design for Resiliency Using Extreme Value Analysis 51
Szilárd Bozóki and András Pataricza

Evaluation Framework for Performance Limitation of Autonomous Systems Under Sensor Attack 67
Koichi Shimizu, Daisuke Suzuki, Ryo Muramatsu, Hisashi Mori, Tomoyuki Nagatsuka, and Tsutomu Matsumoto

ISO/SAE 21434-Based Risk Assessment of Security Incidents in Automated Road Vehicles 82
Dominik Püllen, Jonas Liske, and Stefan Katzenbeisser

Safety and Assurance Cases

Automating the Assembly of Security Assurance Case Fragments 101
Baoluo Meng, Saswata Paul, Abha Moitra, Kit Siu, and Michael Durling

Safety Case Maintenance: A Systematic Literature Review 115
Carmen Cârlan, Barbara Gallina, and Liana Soima

Towards Certified Analysis of Software Product Line Safety Cases 130
Ramy Shahin, Sahar Kokaly, and Marsha Chechik

Machine Learning Applications

Safety Assurance of Machine Learning for Chassis Control Functions 149
Simon Burton, Iwo Kurzidem, Adrian Schwaiger, Philipp Schleiss, Michael Unterreiner, Torben Graeber, and Philipp Becker

Safe Interaction of Automated Forklifts and Humans at Blind Corners in a Warehouse with Infrastructure Sensors 163
Christian Drabek, Anna Kosmalska, Gereon Weiss, Tasuku Ishigooka, Satoshi Otsuka, and Mariko Mizuochi

Machine Learning-Based Fault Injection for Hazard Analysis and Risk Assessment 178
Bentley James Oakes, Mehrdad Moradi, Simon Van Mierlo, Hans Vangheluwe, and Joachim Denil

Safety Validation and Simulation

SASSI: Safety Analysis Using Simulation-Based Situation Coverage for Cobot Systems. 195
Benjamin Lesage and Rob Alexander

Attack and Fault Injection in Self-driving Agents on the Carla Simulator – *Experience Report* 210
Niccolò Piazzesi, Massimo Hong, and Andrea Ceccarelli

A Framework for Automated Quality Assurance and Documentation for Pharma 4.0 226
Andreas Schmidt, Joshua Frey, Daniel Hillen, Jessica Horbelt, Markus Schandar, Daniel Schneider, and Ioannis Sorokos

Fault Tolerance

A Modular Approach to Non-deterministic Dynamic Fault Trees. 243
Sascha Müller, Adeline Jordon, Andreas Gerndt, and Thomas Noll

Composition of Fault Forests 258
Danielle Stewart, Michael Whalen, Mats Heimdahl, Jing (Janet) Liu, and Darren Cofer

Author Index 277