Lecture Notes in Computer Science 11698

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

Alexander Romanovsky ·
Elena Troubitsyna · Friedemann Bitsch (Eds.)

Computer Safety, Reliability, and Security

38th International Conference, SAFECOMP 2019
Turku, Finland, September 11–13, 2019
Proceedings

Springer

Editors

Alexander Romanovsky
Newcastle University
Newcastle upon Tyne, UK

Elena Troubitsyna
Åbo Akademi University
Turku, Finland

Friedemann Bitsch
Thales Deutschland GmbH
Ditzingen, Germany

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-26600-4 ISBN 978-3-030-26601-1 (eBook)
https://doi.org/10.1007/978-3-030-26601-1

LNCS Sublibrary: SL2 – Programming and Software Engineering

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.
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 contains the proceedings of the 38th International Conference on Computer Safety, Reliability, and Security (SAFECOMP 2019) held during September 10–13, 2019, in Turku, Finland. The European Workshop on Industrial Computer Systems, Technical Committee 7 on Reliability, Safety, and Security (EWICS TC7), established the SAFECOMP conference series in 1979. It has since contributed considerably to the progress of the state of the art of dependable computer systems and their application in safety-related and safety-critical systems, for the benefit of industry, transport, space systems, health, energy production and distribution, communications, smart environments, buildings, and living. It covers all areas of dependable systems in the Smart World of Things, influencing our everyday life. Embedded systems, cyber-physical systems, (industrial) Internet of Things, autonomous systems, systems-of-systems, safety and cybersecurity, digital society, and transformation are some of the keywords. For all of the ICT upcoming trends, safety, reliability, and security are indispensable, and SAFECOMP addresses them properly from a technical, engineering, and scientific point of view, showing its increasing relevance for today's technology advancements. The special themes of SAFECOMP 2019 were Safety and Security of Autonomous Systems.

We received a good number of high-quality submissions (65), and the international Program Committee (more than 50 members from 14 countries) worked hard to select 21 papers for presentation and publication in the SAFECOMP 2019 proceedings (Springer LNCS 11698). The review process was thorough and each paper was reviewed by at least three independent reviewers. The merits of each paper were evaluated by the Program Committee members during the on-line discussions and face-to-face meetings. Three renowned speakers from the international community were invited to give keynotes: Marco Vieira (University of Coimbra, Portugal) "Trustworthiness Benchmarking of Safety Critical Systems"; Ross Anderson (University of Cambridge, UK) "The Sustainability of Safety, Security and Privacy"; and Jack Weast (Intel, USA) "An Open, Transparent, Industry-Driven Approach to AV Safety". Following tradition, the conference was organized as a single-track event, allowing for intensive networking during breaks and social events, and participation in all presentations and discussions. This year again we had five high-quality workshops running in parallel the day before the main conference: SASSUR – International Workshop on Next Generation of System Assurance Approaches for Safety-Critical Systems, DECSoS – International ERCIM/EWICS/ARTEMIS Workshop on Dependable Smart Embedded Cyber-Physical Systems and Systems-of-Systems, STRIVE – International Workshop on Safety, Security, and Privacy In Automotive systems, WAISE – International Workshop on Artificial Intelligence Safety Engineering, and ASSURE – International Workshop on Assurance Cases for Software-intensive Systems. These workshops covered a diverse range of topics related to safety and security. The proceedings of the workshops are published in a separate SAFECOMP workshop proceedings volume (LNCS 11699).

We would like to express our sincere gratitude to many people whose contributions made SAFECOMP 2019 possible: the authors of the submitted papers and the invited speakers; the Program Committee members and external reviewers; EWICS and the supporting organizations; the sponsors; and last but not least, the local Organization Committee, who took care of the local arrangements, the web-master, and the Publication Chair for finalizing this volume. We hope that the reader will find these proceedings interesting and thought provoking.

September 2019

Alexander Romanovsky
Elena Troubitsyna

Organization

Committees

EWICS TC7 Chair

Francesca Saglietti	University of Erlangen-Nuremberg, Germany

General Chairs and Program Co-chairs

Alexander Romanovsky	Newcastle University, UK
Elena Troubitsyna	KTH Royal Institute of Technology, Sweden and Åbo Akademi, Finland

General Workshop Chairs

Ilir Gashi	CSR, City University London, UK
Erwin Schoitsch	AIT Austrian Institute of Technology, Austria

Publication Chair

Friedemann Bitsch	Thales Deutschland GmbH, Germany

Local Organizing Committee

Elena Troubitsyna	Åbo Akademi, Finland
Minna Carla	Åbo Akademi, Finland
Christel Engblom	Åbo Akademi, Finland
Inna Vistbackka	Åbo Akademi, Finland

International Program Committee

Uwe Becker	Draeger Medical GmbH, Germany
Peter G. Bishop	Adelard, UK
Friedemann Bitsch	Thales Deutschland GmbH, Germany
Jean-Paul Blanquart	Airbus Defence and Space, France
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
Mads Dam	KTH Royal Institute of Technology, Sweden
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
Francesco Flammini	Linnaeus University, Sweden
Simon Fuerst	BMW Group, Germany
Barbara Gallina	Mälardalen University, Sweden
Ilir Gashi	CSR, City University London, UK
Anatoliy Gorbenko	National Aerospace University, KhAI, UK
Janusz Górski	Gdańsk University of Technology, Poland
Jérémie Guiochet	LAAS-CNRS, France
Hans Hansson	Mälardalen University, Sweden
Mats Heimdahl	University of Minnesota, USA
Maritta Heisel	University of Duisburg-Essen, Germany
Constance Heitmeyer	Naval Research Laboratory, USA
Alexei Iliasov	Newcastle University, UK
Christopher Johnson	University of Glasgow, UK
Rajeev Joshi	Automated Reasoning Group, Amazon Web Services, USA
Karama Kanoun	LAAS-CNRS, France
Joost-Pieter Katoen	RWTH Aachen University, Germany
Phil Koopman	Carnegie-Mellon University, USA
Peter Ladkin	University of Bielefeld, Germany
Timo Latvala	Space Systems Finland Ltd., Finland
Simin Nadjm-Tehrani	Linköping University, Sweden
Mattias Nyberg	Scania, Linköping University, Sweden
Frank Ortmeier	Otto-von-Guericke Universität Magdeburg, Germany
Philippe Palanque	ICS-IRIT, University Toulouse, France
Michael Paulitsch	Intel, Austria
Holger Pfeifer	Technical University of Munich, Germany
Peter Popov	City University London, UK
Laurent Rioux	Thales R&T, France
Matteo Rossi	Politecnico di Milano, Italy
Francesca Saglietti	University of Erlangen-Nuremberg, Germany
Christoph Schmitz	Zühlke Engineering AG, Switzerland
Erwin Schoitsch	AIT Austrian Institute of Technology, Austria
Christel Seguin	Office National d'Etudes et Recherches Aérospatiales, France
Håkan Sivencrona	Zenuity AB, Sweden
Oleg Sokolsky	University of Pennsylvania, USA
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 Experimental Software Engineering, Germany
Tullio Vardanega	University of Padua, Italy
Marcel Verhoef	European Space Agency, The Netherlands
Jonny Vinter	RISE Research Institutes of Sweden, Sweden
Hélène Waeselynck	LAAS-CNRS, France

Sub-reviewers

Mehrnoosh Askarpour	Politecnico di Milano, Italy
Zeinab Bakhshi	Mälardalen University, Sweden
Philipp Berger	RWTH Aachen University, Germany
Matthew Fernandez	Intel, Austria
Peter Folkesson	RISE Research Institutes of Sweden, Sweden
Jelena Frtunikj	BMW Group, Germany
Mohammad Gharib	University of Florence, Italy
Tim Gonschorek	Otto-von-Guericke Universität Magdeburg, Germany
Robert Heumüller	Otto-von-Guericke Universität Magdeburg, Germany
Dubravka Ilic	Space Systems Finland Ltd., Finland
Ramneet Kaur	University of Pennsylvania, USA
Björn Leander	Mälardalen University, Sweden
Naveen Mohan	KTH Royal Institute of Technology, Sweden
Sebastian Nielebock	Otto-von-Guericke Universität Magdeburg, Germany
Thomas Noll	RWTH Aachen University, Germany
Viorel Preoteasa	Space Systems Finland Ltd., Finland
Ashur Rafiev	Newcastle University, UK
Clément Robert	LAAS-CNRS, France
Ivan Ruchkin	University of Pennsylvania, USA
Behrooz Sangchoolie	RISE Research Institutes of Sweden, Sweden
Rishad Shafik	Newcastle University, UK
Irfan Sljivo	Mälardalen University, Sweden
Joel Svensson	RISE Research Institutes of Sweden, Sweden
Lars Svensson	KTH Royal Institute of Technology, Sweden
Xin Tao	KTH Royal Institute of Technology, Sweden
Kimmo Varpaaniemi	Space Systems Finland Ltd., Finland
Inna Vistbakka	Åbo Akademi, Finland
Fredrik Warg	RISE Research Institutes of Sweden, Sweden
Teng Zhang	University of Pennsylvania, USA
Xinhai Zhang	KTH Royal Institute of Technology, Sweden

Supporting Institutions

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

Kungliga Tekniska högskolan –
Royal Institute of Technology

Newcastle University

Åbo Akademi

Austrian Institute of Technology

City University London

Thales Deutschland GmbH

Intel

Lecture Notes
in Computer Science (LNCS),
Springer Science + Business Media

Austrian Computer Society

ARTEMIS Industry Association

Electronic Components and Systems
for European Leadership - Austria

Verband österreichischer
Software Industrie

verband
österreichischer
software
industrie

European Research
Consortium for Informatics
and Mathematics

ERCIM
European Research Consortium
for Informatics and Mathematics

Invited Talks

Trustworthiness Benchmarking of Safety Critical Systems

Marco Vieira

University of Coimbra, Portugal
mvieira@dei.uc.pt

Abstract. Some recent incidents and analyses have indicated that possibly the vulnerability of IT systems in railway automation is increasing. Due to several trends, such as digitalization or the use of commercial IT and communication systems the threat potential has increased. This paper discusses the way forward for the railway sector, how many advantages of digitalization can be realized without compromising safety. In particular topics like standardization or certification are covered, but also technical issues like software update.

The Sustainability of Safety, Security and Privacy

Ross Anderson

University of Cambridge, UK
ross.anderson@cl.cam.ac.uk

Abstract. Now that we are putting software and network connections into cars and medical devices, we will have to patch vulnerabilities, as we do with phones. But we can't let vendors stop patching them after three years, as they do with phones. So in May, the EU passed Directive 2019/771 on the sale of goods. This gives consumers the right to software updates for goods with digital elements, for the time period the consumer might reasonably expect. In this talk I'll describe the background, including a study we did for the European Commission in 2016, and the likely future effects. As sustainable safety, security and privacy become a legal mandate, this will create real tension with existing business models and supply chains. It will also pose a grand challenge for computer scientists. What sort of tools and methodologies should you use to write software for a car that will go on sale in 2023, if you have to support security patches and safety upgrades till 2043?

An Open, Transparent, Industry-Driven Approach to AV Safety

Jack Weast

Intel, USA
jack.weast@intel.com

Abstract. At Intel and Mobileye, saving lives drives us. But in the world of automated driving, we believe safety is not merely an impact of AD, but the bedrock on which we all build this industry. And so we proposed Responsibility-Sensitive Safety (RSS), a formal model to define safe driving and what rules an automated vehicle, independent of brand or policy, should abide to always keep its passengers safe. We intend this open, non-proprietary model to drive cross-industry discussion; let's come together as an industry and use RSS as a starting point to clarify safety today, to enable the autonomous tomorrow.

Contents

Formal Verification

Autonomous Driving

Safety and Reliability Modeling

Security Engineering and Risk Assessment

Safety Argumentation

Verification and Validation of Autonomous Systems

Interactive Systems and Design Validation