Lecture Notes in Computer Science 10488

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

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

Stefano Tonetta · Erwin Schoitsch
Friedemann Bitsch (Eds.)

Computer Safety, Reliability, and Security

36th International Conference, SAFECOMP 2017
Trento, Italy, September 13–15, 2017
Proceedings

Springer

Editors
Stefano Tonetta
Fondazione Bruno Kessler
Trento
Italy

Friedemann Bitsch
Thales Deutschland GmbH
Ditzingen
Germany

Erwin Schoitsch
AIT Austrian Institute of Technology
Vienna
Austria

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-66265-7 ISBN 978-3-319-66266-4 (eBook)
DOI 10.1007/978-3-319-66266-4

Library of Congress Control Number: 2017949512

LNCS Sublibrary: SL2 – Programming and Software Engineering

Printed on acid-free paper

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

Preface

This volume contains the papers presented at SAFECOMP 2017, the 36th International Conference on Computer Safety, Reliability, and Security, held in Trento, Italy, in September 2017.

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 then 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 the upcoming megatrends, safety, reliability, and security are indispensable – SAFECOMP addresses them properly from a technical, engineering, and scientific point of view, showing its increasing relevance for today's technology advancements.

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 22 for presentation and for publication in the SAFECOMP 2017 proceedings (Springer LNCS 10488). The review process was thorough with at least three reviewers with ensured independency. Three renowned speakers from the international community were invited to give a keynote: Marcel Verhoef, "From Documents to Models: Towards Digital Continuity"; John McDermid, "Safety of Autonomy: Challenges and Strategies"; and Radu Grosu, "CPS/IoT: Drivers of the Next IT Revolution". As in previous years, the conference was organized as a single-track event, allowing intensive networking during breaks and social events, and participation in all presentations and discussions.

This year we had again five high-quality workshops in parallel the day before the main conference, ASSURE, DECSoS, SASSUR, TELERISE (for the first time co-located with SAFECOMP), and TIPS. These workshops differed according to the topic, goals, and organizing group(s), and are published in a separate SAFECOMP workshop proceedings volume (LNCS 10489).

We would like to express our gratitude and thanks to all those who contributed to making this conference possible: the authors of submitted papers and the invited speakers; the Program Committee members and external reviewers; EWICS and the supporting organizations; and last but not least, the Local Organization Committee, who took care of the local arrangements, and the Publication Chair for finalizing this volume.

We hope that the reader will find these proceedings interesting and stimulating.

September 2017

Erwin Schoitsch
Stefano Tonetta

Organization

EWICS TC7 Chair

Francesca Saglietti	University of Erlangen-Nuremberg, Germany

Conference Co-chairs

Stefano Tonetta	FBK Fondazione Bruno Kessler, Italy
Erwin Schoitsch	AIT Austrian Institute of Technology, Austria

Program Co-chairs

Erwin Schoitsch	AIT Austrian Institute of Technology, Austria
Stefano Tonetta	FBK Fondazione Bruno Kessler, Italy

Publication Chair

Friedemann Bitsch	Thales Deutschland GmbH, Germany

Local Organizing Committee

Annalisa Armani	FBK Fondazione Bruno Kessler, Italy
Silvia Malesardi	FBK Fondazione Bruno Kessler, Italy
Stefano Tonetta	FBK Fondazione Bruno Kessler, Italy

Workshop Chair

Erwin Schoitsch	AIT Austrian Institute of Technology, Austria

International Program Committee

Thomas Arts	Quviq, Sweden
Peter G. Bishop	Adelard, UK
Friedemann Bitsch	Thales Deutschland GmbH, Germany
Jean-Paul Blanquart	Airbus Defence and Space, France
Sandro Bologna	Associazione Italiana esperti in Infrastrutture Critiche (AIIC), Italy
Andrea Bondavalli	University of Florence, Italy
Jens Braband	Siemens AG, 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	Hochschule Fulda, Germany
John Favaro	Intecs SpA, Italy
Alberto Ferrari	United Technologies Research Center (UTRC) – Advanced Laboratory on Embedded Systems (ALES), Italy
Francesco Flammini	Federico II University of Naples, Italy
Barbara Gallina	Mälardalen University, Sweden
Ilir Gashi	CSR, City University London, UK
Janusz Górski	Gdansk University of Technology, Poland
Jérémie Guiochet	LAAS-CNRS, France
Wolfgang Halang	Fernuniversität Hagen, Germany
Maritta Heisel	University of Duisburg-Essen, Germany
Chris Johnson	University of Glasgow, UK
Bernhard Kaiser	Berner&Mattner, Germany
Karama Kanoun	LAAS-CNRS, France
Joost-Pieter Katoen	RWTH Aachen University, Germany
Tim Kelly	University of York, UK
Floor Koornneef	Delft University of Technology, The Netherlands
Timo Latvala	Space Systems Finland Ltd., Finland
Zhendong Ma	AIT Austrian Institute of Technology, Austria
Silvia Mazzini	Intecs, Italy
John McDermid	University of York, UK
Frank Ortmeier	Otto-von-Guericke Universität Magdeburg, Germany
Philippe Palanque	University Toulouse, IRIT, France
Michael Paulitsch	Thales Austria GmbH, Austria
Holger Pfeifer	fortiss GmbH, Germany
Thomas Pfeiffenberger	Salzburg Research Forschungsgesellschaft m.b.H, Austria
Peter Popov	City University London, UK
Laurent Rioux	Thales R&T, France
Alexander Romanovsky	Newcastle University, UK
Matteo Rossi	Politecnico di Milano, Italy
Kristin Yvonne Rozier	Iowa State University, USA
John Rushby	SRI International, USA
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
Amund Skavhaug	The Norwegian University of Science and Technology, Norway
Oleg Sokolsky	University of Pennsylvania, USA
Wilfried Steiner	TTTech Computertechnik AG, Austria
Mark-Alexander Sujan	University of Warwick, UK
Stefano Tonetta	Fondazione Bruno Kessler, Italy

Martin Törngren	KTH Royal Institute of Technology, Stockholm, Sweden
Mario Trapp	Fraunhofer Institute for Experimental Software Engineering, Germany
Elena Troubitsyna	Åbo Akademi University, Finland
Tullio Vardanega	University of Padua, Italy
Marcel Verhoef	European Space Agency, The Netherlands
Helene Waeselynck	LAAS-CNRS, France

Sub-reviewers

Rob Alexander	University of York, UK
Mehrnoosh Askarpour	Politecnico di Milano, Italy
Philipp Berger	RWTH Aachen University, Germany
Pierre Bieber	Office National d'Etudes et Recherches Aérospatiales, France
Sofia Cassel	KTH Royal Institute of Technology, Stockholm, Sweden
Luigi Di Guglielmo	United Technologies Research Center (UTRC), Italy
Orlando Ferrante	United Technologies Research Center (UTRC), Italy
Simon Foster	University of York, UK
Robert Heumüller	Otto-von-Guericke Universität Magdeburg, Germany
Dubravka Ilic	Space Systems Finland Ltd., Finland
Sebastian Junges	RWTH Aachen University, Germany
Romain Laborde	University Toulouse, IRIT, France
Lola Masson	LAAS-CNRS, France
Behrang Monajemi	Berner&Mattner, Germany
Sebastian Nielebock	Otto-von-Guericke Universität Magdeburg, Germany
Robert Palin	University of York, UK
Junkil Park	University of Pennsylvania, USA
Masoumeh Parseh	KTH Royal Institute of Technology, Stockholm, Sweden
Stephane Paul	Thales R&T, France
Inna Pereverzeva	Åbo Akademi University, Finland
Irum Rauf	Åbo Akademi University, Finland
Thomas Santen	Technische Universität Berlin, Germany
Valerio Senni	United Technologies Research Center (UTRC), Italy
Thierry Sotiropoulos	LAAS-CNRS, France
Lars Svensson	KTH Royal Institute of Technology, Stockholm, Sweden
Thanassis Tsiodras	European Space Agency, The Netherlands
Nelufar Ulfat-Bunyadi	University of Duisburg-Essen, Germany
Pieter van Gelder	Delft University of Technology, The Netherlands
Kimmo Varpaaniemi	Space Systems Finland Ltd., Finland
Eugene Vasserman	Kansas State University, USA
Matthias Volk	RWTH Aachen University, Germany

Supporting Institutions

European Workshop on Industrial Computer Systems Reliability, Safety and Security

Fondazione Bruno Kessler

Austrian Institute of Technology

Thales Deutschland GmbH

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

European Space Agency

Austrian Association for Research in IT

Austrian Computer Society

European Research Consortium
for Informatics and Mathematics

ARTEMIS Industry Association

Electronic Components and Systems
for European Leadership - Austria

German Computer Society

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

IEEE SMC Technical Committee on
Homeland Security (TCHS)

Associazione Italiana per l'Informatica e il
Calcolo Automatico

Verband österreichischer Software Industrie –
Austrian Software Industry Association

Invited Talks

Safety of Autonomy: Challenges and Strategies

John McDermid

University of York, UK
`john.mcdermid@cs.york.ac.uk`

Abstract. Robots and autonomous systems have been in use for some time - for example in factories and in urban railways. However there is now an unprecedented level of activity in robotics and autonomy, with applications ranging from domestic and healthcare robots to driverless cars. Whilst, in some cases, safety is being assessed thoroughly, in many situations these applications cannot effectively be addressed using standard methods. Challenges include demonstrating the safety of artificial intelligence (AI), especially learning or adaptive systems and the effectiveness of image analysis and scene understanding. At a broader level there are difficulties for standards and regulations that, in some cases, have historically sought to exclude the use of AI. The talk will discuss some of these challenges and consider solution strategies, including approaches to dynamic assessment of safety.

CPS/IoT: Drivers of the Next IT Revolution

Radu Grosu

Institute of Computer Engineering, Vienna University of Technology, Austria
`radu.grosu@tuwien.ac.at`

Abstract. Looking back at the time Bill Gates was one of his brilliant students, Christos Papadimitriou a Harvard professor and world-renowned computer scientist, concluded that one of the greatest challenges of the academic community is to recognising when an IT revolution is on its way. He did not see the PC revolution coming, but his student did. Since then several others happened, such as the Internet and the Mobiles revolutions. Another imminent one is in the making: The CPS/IoT revolution.

Cyber-physical systems (CPS) are spatially-distributed, time-sensitive, and multi-scale, networked embedded systems, connecting the physical world to the cyber world through sensors and actuators. The Internet of Things (IoT) is the backbone of CPS. It connects the swarm of Sensors and Actuators to the nearby Gateways through various protocols, and the Gateways to the Fog and the Cloud. The Fog resembles the human spine, providing fast and adequate response to imminent situations. The Cloud resembles the human brain, providing large storage and analytic capabilities.

Four pillars, Connectivity, Monitoring, Prediction, and Optimisation drive the CPS/IoT. The first two have been already enabled by the technological developments over the past years. The last two, are expected to radically change every aspect of our society,. The huge number of sensors to be deployed in areas such as manufacturing, transportation, energy and utilities, buildings and urban planning, health care, environment, or jointly in smart cities, will allow the collection of terabytes of information (Big-Data), which can be processed for predictive purposes. The huge number of actuators will enable the optimal control of these areas and drive market advantages.

Despite of all these optimistic predictions, a main question still lingers: Are we ready for the CPS/IoT revolution? In this talk, I will address the grand challenges that stand in our way, but also point out, the great opportunities of CPS/IoT.

Contents

Dynamic Fault Trees

Model-Based Safety Analysis for Vehicle Guidance Systems 3
Majdi Ghadhab, Sebastian Junges, Joost-Pieter Katoen, Matthias Kuntz, and Matthias Volk

Rare Event Simulation for Dynamic Fault Trees 20
Enno Ruijters, Daniël Reijsbergen, Pieter-Tjerk de Boer, and Mariëlle Stoelinga

Safety Case and Argumentation

Arguing on Software-Level Verification Techniques Appropriateness. 39
Carmen Cârlan, Barbara Gallina, Severin Kacianka, and Ruth Breu

Confidence Assessment Framework for Safety Arguments 55
Rui Wang, Jérémie Guiochet, and Gilles Motet

Safety Case Impact Assessment in Automotive Software Systems: An Improved Model-Based Approach 69
Sahar Kokaly, Rick Salay, Marsha Chechik, Mark Lawford, and Tom Maibaum

Formal Verification

Modeling Operator Behavior in the Safety Analysis of Collaborative Robotic Applications 89
Mehrnoosh Askarpour, Dino Mandrioli, Matteo Rossi, and Federico Vicentini

Development and Verification of a Flight Stack for a High-Altitude Glider in Ada/SPARK 2014 105
Martin Becker, Emanuel Regnath, and Samarjit Chakraborty

A Simplex Architecture for Hybrid Systems Using Barrier Certificates 117
Junxing Yang, Md. Ariful Islam, Abhishek Murthy, Scott A. Smolka, and Scott D. Stoller

Autonomous Systems

A Conceptual Safety Supervisor Definition and Evaluation Framework for Autonomous Systems 135
Patrik Feth, Daniel Schneider, and Rasmus Adler

A Strategy for Assessing Safe Use of Sensors in Autonomous Road Vehicles 149
Rolf Johansson, Samieh Alissa, Staffan Bengtsson, Carl Bergenhem, Olof Bridal, Anders Cassel, De-Jiu Chen, Martin Gassilewski, Jonas Nilsson, Anders Sandberg, Stig Ursing, Fredrik Warg, and Anders Werneman

Modeling the Safety Architecture of UAS Flight Operations 162
Ewen Denney, Ganesh Pai, and Iain Whiteside

Generic Management of Availability in Fail-Operational Automotive Systems 179
Philipp Schleiss, Christian Drabek, Gereon Weiss, and Bernhard Bauer

Static Analysis and Testing

Benchmarking Static Code Analyzers 197
Jörg Herter, Daniel Kästner, Christoph Mallon, and Reinhard Wilhelm

Automatic Estimation of Verified Floating-Point Round-Off Errors via Static Analysis 213
Mariano Moscato, Laura Titolo, Aaron Dutle, and César A. Muñoz

Classification Tree Method with Parameter Shielding 230
Takashi Kitamura, Akihisa Yamada, Goro Hatayama, Shinya Sakuragi, Eun-Hye Choi, and Cyrille Artho

Safety Analysis and Assessment

ErrorSim: A Tool for Error Propagation Analysis of Simulink Models 245
Mustafa Saraoğlu, Andrey Morozov, Mehmet Turan Söylemez, and Klaus Janschek

Early Safety Assessment of Automotive Systems Using Sabotage Simulation-Based Fault Injection Framework 255
Garazi Juez, Estíbaliz Amparan, Ray Lattarulo, Alejandra Ruíz, Joshué Pérez, and Huáscar Espinoza

Towards a Sensor Failure-Dependent Performance Adaptation Using the Validity Concept 270
Juliane Höbel, Georg Jäger, Sebastian Zug, and Andreas Wendemuth

SMT-Based Synthesis of Fault-Tolerant Architectures 287
Kevin Delmas, Rémi Delmas, and Claire Pagetti

Safety and Security

A Lightweight Threat Analysis Approach Intertwining Safety and Security for the Automotive Domain 305
Jürgen Dürrwang, Kristian Beckers, and Reiner Kriesten

A Security Architecture for Railway Signalling. 320
Christian Schlehuber, Markus Heinrich, Tsvetoslava Vateva-Gurova, Stefan Katzenbeisser, and Neeraj Suri

Systematic Pattern Approach for Safety and Security Co-engineering in the Automotive Domain 329
Tiago Amorim, Helmut Martin, Zhendong Ma, Christoph Schmittner, Daniel Schneider, Georg Macher, Bernhard Winkler, Martin Krammer, and Christian Kreiner

Author Index 343