

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Zurich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology Madras, Chennai, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbrücken, Germany

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


Barbara Gallina · Amund Skavhaug
Friedemann Bitsch (Eds.)

Computer Safety, Reliability, and Security

37th International Conference, SAFECOMP 2018
Västerås, Sweden, September 19–21, 2018
Proceedings

Editors

Barbara Gallina 
Mälardalen University
Västerås
Sweden

Friedemann Bitsch 
Thales Deutschland GmbH
Ditzingen
Germany

Amund Skavhaug
Norwegian University of Science
and Technology
Trondheim
Norway

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-99129-0 ISBN 978-3-319-99130-6 (eBook)
<https://doi.org/10.1007/978-3-319-99130-6>

Library of Congress Control Number: 2018950937

LNCS Sublibrary: SL2 – Programming and Software Engineering

© Springer Nature Switzerland AG 2018

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

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, express 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 37th International Conference on Computer Safety, Reliability and Security (SAFECOMP 2018) held during September 19–21, 2018, in Västerås, Sweden. Since 1979, when the conference was established by the European Workshop on Industrial Computer Systems, Technical Committee 7 on Reliability, Safety and Security (EWICS TC7), it has contributed to the state of the art through knowledge dissemination and discussions of important aspects of computer systems of our everyday life. With the proliferation of embedded systems, the omnipresence of the Internet of Things, and the commodity of advanced real-time control systems, our dependence on safe and correct behavior is increasing. Currently, we are witnessing the beginning of the area of truly autonomous systems, perhaps with driverless cars as the most well-known example to the non-specialist, where the safety and correctness of their computer systems are already being discussed in the mainstream media. In this context, it is clear that the relevance of the SAFECOMP conference series is increasing.

The international Program Committee (PC), consisting of 56 members from 15 countries, received 63 papers from 24 nations. Of these, 20 papers were selected to be presented at the conference resulting in an acceptance rate of 31.7%. The review process was thorough with at least three reviewers, which ensured independency, and 20 of these reviewers met in person in Munich, Germany in April 2018 for the final discussion and selection. Our warm thanks go to reviewers who offered their time and competence in the PC work. We are grateful for the support we received from the PC member Mario Trapp, Fraunhofer ESK, who generously hosted the PC meeting.

The conference featured three keynotes: “Software Engineering for Safety in Molecular Programmed Systems” by Robyn Lutz, Professor of Computer Science at Iowa State University; “Reviews?! We Do That! Cross-Domain Reuse of Engineering Knowledge and Evidence” by Uma Ferrell, Software and Airborne Electronic Hardware Designated Engineering Representative for the US Federal Aviation Administration; “Experiences from the Industry, Design and Application of a Control System Platform for Safety of Machinery” by Richard Hendeberg, Specialist in Functional Safety at Epiroc Rock Drills AB.

As in the previous years, the conference was organized as a single-track conference, allowing intensive networking during breaks and social events, and participation in all presentations and discussions. The conference also included a fast abstracts session, giving the opportunity for new ideas and work in progress to bloom in a fertile soil. The Fast Abstracts proceedings are published in the HAL repository.

Finally, the conference also included a panel session, focusing on stimulating an interactive discussion with the audience around the main theme of SAFECOMP 2018, i.e., “Cross- and Intra-Domain Reuse of Engineering and Certification Artefacts: Challenges and Opportunities.”

As has been the tradition for many years, the day before the main track of the conference was dedicated to five regular workshops: DECSoS, ASSURE, SASSUR, STRIVE, WAISE. Papers from these workshops are published in a separate LNCS volume (11094).

We would like to express our gratitude to the many people who helped with the preparations and running of the conference, especially Friedemann Bitsch as publication chair, Erwin Schoitsch as workshop chair, Jérémie Guiochet as fast abstracts chair, Alexander Romanovsky as publicity chair, and not to be forgotten the local organization and support staff, Irfan Sljivo, Lena Jonsson, Martina Pettersson, Elena Rivani, Linda Claesson, and Gunnar Widforss.

For its support, we wish to thank Mälardalen University, represented by the School of Innovation, Design, and Engineering and, more specifically, by the research group Certifiable Evidences and Justification Engineering. We also wish to thank all other supporting institutions.

Without the support from the EWICS TC7 headed by Francesca Saglietti, this event could not have happened. We wish the EWICS TC7 organization continued success, and we are looking forward to being part of this in the future.

Finally, the most important people to whom we want to express our gratitude are the authors and participants. Your dedication, effort, and knowledge are the foundation of the scientific progress. We hope you had fruitful discussions, gained new insights, and had a memorable time in Västerås.

September 2018

Barbara Gallina
Amund Skavhaug

Organization

EWICS TC7 Chair

Francesca Saglietti University of Erlangen-Nuremberg, Germany

General Chair

Barbara Gallina Mälardalen University, Sweden

Program Co-chairs

Barbara Gallina Mälardalen University, Sweden
Amund Skavhaug The Norwegian University of Science and Technology,
Norway

Workshop Chair

Erwin Schoitsch AIT Austrian Institute of Technology, Austria

Publication Chair

Friedemann Bitsch Thales Deutschland GmbH, Germany

Organizing Committee

Irfan Sljivo Mälardalen University, Sweden
Lena Jonsson Mälardalen University, Sweden
Martina Pettersson Mälardalen University, Sweden
Elena Rivani Mälardalen University, Sweden
Linda Claesson Mälardalen University, Sweden
Gunnar Widforss Mälardalen University, Sweden

Publicity Chair

Alexander Romanovsky Newcastle University, UK

Fast Abstracts Chair

Jérémie Guiochet LAAS-CNRS, University of Toulouse, France

Program Committee

Uwe Becker	Draeger Medical GmbH, Germany
Peter G. Bishop	Adelard, UK
Friedemann Bitsch	Thales Deutschland GmbH, Germany
Robin Bloomfield	City University London, UK
Sandro Bologna	Associazione Italiana Esperti Infrastrutture Critiche, Italy
Andrea Bondavalli	University of Florence, Italy
Jens Braband	Siemens AG, Germany
Anna Carlsson	OHB Sweden, Sweden
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
Massimo Felici	Deloitte Consulting & Advisory, Belgium
Uma Ferrell	MITRE Corporation, USA
Francesco Flammini	Linnaeus University, Sweden
Barbara Gallina	Mälardalen University, Sweden
Ilir Gashi	CSR, City University London, UK
Janusz Górski	Gdańsk University of Technology, Poland
Jérémie Guiochet	LAAS-CNRS, France
Maritta Heisel	University of Duisburg-Essen, Germany
Chris Johnson	University of Glasgow, UK
Bernhard Kaiser	Assystem Germany GmbH, Germany
Karama Kanoun	LAAS-CNRS, France
Johan Karlsson	Chalmers University of Technology, Sweden
Phil Koopman	Carnegie Mellon University, USA
Floor Koornneef	Delft University of Technology, The Netherlands
Timo Latvala	Space Systems Finland Ltd., Finland
Bev Littlewood	City University London, UK
Silvia Mazzini	Intecs, Italy
John McDermid	University of York, UK
Frank Ortmeier	Otto-von-Guericke Universität Magdeburg, Germany
Michael Paulitsch	Intel, Austria
Holger Pfeifer	Technical University of Munich, 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
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
Mark-Alexander Sujan	University of Warwick, UK
Kenji Taguchi	CAV Technologies Co., Ltd., Japan
Stefano Tonetta	Fondazione Bruno Kessler, Italy
Mario Trapp	Fraunhofer Institute for Experimental Software Engineering, Germany
Elena Troubitsyna	Åbo Akademi University, Finland
Fredrik Törner	Volvo Car Corporation, Sweden
Martin Törngren	KTH Royal Institute of Technology, Sweden
Pieter van Gelder	Delft University of Technology, The Netherlands
Marcel Verhoef	European Space Agency, The Netherlands
Jonny Vinter	RISE Research Institutes of Sweden
Helene Waeselynck	LAAS-CNRS, France

Additional Reviewers

Matthieu Amy	LAAS-CNRS, France
Milan Battelino	OHB Sweden, Sweden
Victor Bos	Space Systems Finland Ltd., Finland
Bill Drozd	Carnegie Mellon University, USA
Sam George	Adelard, UK
Didem Gürdür	KTH Royal Institute of Technology, Sweden
Denis Hatebur	University of Duisburg-Essen, Germany
Dubravka Ilic	Space Systems Finland Ltd., Finland
Lola Masson	LAAS-CNRS, France
Viorel Preoteasa	Space Systems Finland Ltd., Finland
Irum Rauf	Åbo Akademi University, Finland
Behrooz Sangchoolie	RISE Research Institutes of Sweden
Paulius Stankaitis	Newcastle University, UK
Kimmo Varpaaniemi	Space Systems Finland Ltd., Finland
Inna Vistbakka	Åbo Akademi University, Finland
Andrzej Wardziński	Gdańsk University of Technology, Poland
Xinhai Zhang	KTH Royal Institute of Technology, Sweden

Supporting Institutions

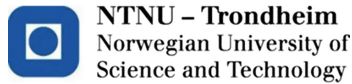
European Workshop on Industrial
Computer Systems Reliability,
Safety and Security



Mälardalen University, Sweden



Norwegian University of Science
and Technology



Austrian Institute of Technology



Thales Deutschland GmbH



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



Austrian Computer Society



ARTEMIS Industry Association



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

European
Network of
Clubs for
REliability and
Safety of
Software

German Computer Society



Electronic Components and
Systems for European
Leadership - Austria



Verband österreichischer
Software Industrie



XII Organization

European Research
Consortium for Informatics
and Mathematics



IEEE SMC Technical
Committee on Homeland
Security (TCHS)



Invited Talks

Software Engineering for Safety in Programmed Molecular Systems

Robyn R. Lutz

Iowa State University, Ames, IA 50011, USA
rlutz@iastate.edu

Abstract. Molecular programming uses the computational power of DNA and other biomolecules to create nanoscale systems. Many of these envisioned nano-systems are safety-critical, such as diagnostic biosensors that detect contaminants, drug capsules that dispense medicine when they encounter diseased cells, and configurable nano-robots. Challenges to the safety engineering of the nano-systems include their probabilistic behavior, their very small size, the very large number of them that execute at once, and the dynamic environment in which they operate. Designs need to assure safe outcomes from highly fault-prone devices, hampered by the difficulty of defining the limits of their safe operation.

I organize the talk around our interdisciplinary team's development of an essential safety building block for programmed molecular systems – an embeddable, reusable, molecular Runtime Fault Detector. I describe how we harnessed goal-oriented requirements and risk analyses, reaction network modeling, and probabilistic model checking to specify, analyze, and verify the safety requirements and design for this new nano-system. Finally, I suggest that a similar approach also may be helpful in the safety engineering of non-molecular systems composed of highly distributed, autonomous, fault-prone components operating in dynamic environments.

Keywords: Software safety · Molecular programming · Software engineering
Chemical reaction networks

Acknowledgments. This research was supported in part by National Science Foundation Grant 1545028.

Reviews?! We do that! Cross-Domain Reuse of Engineering Knowledge and Evidence

Uma Ferrell

MITRE Corporation, 7515 Colshire Drive, McLean VA 22102, USA

Abstract. Both industry and certification authorities have reason to be excited about the benefits and opportunities of reusing and building products for more than one domain such as aviation and automobiles. Cross-domain reuse in an increasingly complex world can inject novel technologies to conventional domains to increase safety. Such opportunities come with social and ethical responsibilities for the safe use of a product in the target environment, not just whether the product and evidence are acceptable to certification authorities. The evidence may be wrongly presented based only on the equivalency in the use of expected language in pertinent standards. The evidence should be based on the actual accomplishments met and whether those accomplishments are applicable towards design assurance and safety in the target domain and environment.

Cross-domain reuse has many considerations. This talk is focused only on safety and security. Obviously, consideration of reuse must include functionality, use of standards in that domain, and certification concerns. All these considerations have undercurrents of safety as well as security. Let us focus further on three topics:

- **Derivation of risk:** Derivation of risk depends on the target domain and the human/system use of the product. Also, the acceptable level of risk tolerance is inherently different in different domains. Aviation is one of the few domains where safety risk tolerance is codified. As stewards of safety in this society, we need to be aware of the real idea behind certification, and promulgate a safety culture to take responsibility for safe cross-domain use of the product throughout the product life.
- **Appropriate use of evidence:** While acceptability for certification is important, the knowledge and evidence for why a product is acceptable is even more important. Evidence may have been produced in a previous domain that appears to be usable in a target domain. Only the basis for that evidence may have a different interpretation and implication in the target domain because the terminology for even simple terms such as “reviews” may not have the same meaning in different domains. Further, the same functionality may be used in diverse ways in the two domains.
- **Importance of systems engineering:** There are certainly considerations that may be codified and delegated to checklists. But blind use of checklists makes a poor substitute for domain knowledge and engineering. Cross-domain use does not just mean that one could deploy a product. Continued safe use of the product in the target domain has specific implications for maintenance of the product as well as maintenance of the system of which the product is just one component. For example, an electro-mechanical system may need adjustments

to maintenance cycles depending on the characteristics of the component commanding the mechanical actions. In general, we must make sure that component engineering is within the context of system safety and security.

Opportunities of cross-domain reuse indeed come with responsibilities to understand, analyze, and engineer the product. Appropriate reuse considered in the system context can be a powerful tool to introduce newer technologies to solve complex problems.

Experiences from the Industry, Design and Application of a Control System Platform for Safety of Machinery

Richard Hendeberg

Epiroc Rock Drills AB, Örebro, Sweden
richard.hendeberg@epiroc.com

Abstract. Epiroc Rock Drills AB is a global manufacturer of mining and construction machinery. These highly automated machines operates in an incredibly harsh environment where reliability and availability is paramount. In this talk, the focus is on Epiroc's control systems platform and work with safety of machinery. How a modular design, componentization of software and standardization on hardware modules has led to an efficient reuse of engineering efforts and an automation platform, which is used throughout Epiroc's entire range of machinery. In this talk, it is also given an overview of Epiroc's journey with safety of control systems, leading up to the integration of safety functions into the existing control system platform. The challenges of designing safety functions for a harsh environment and why availability of the machine might be as important for the safety of the operator as the reliability of the safety function.

Keywords: Mining machinery · Construction machinery · Safety of machinery
Hardware component reuse

Contents

Automotive Safety Standards and Cross-Domain Reuse Potential

Practical Experience Report: Automotive Safety Practices vs. Accepted Principles	3
<i>Philip Koopman</i>	
A Generic Method for a Bottom-Up ASIL Decomposition	12
<i>Alessandro Frigerio, Bart Vermeulen, and Kees Goossens</i>	
Assurance Benefits of ISO 26262 Compliant Microcontrollers for Safety-Critical Avionics	27
<i>Andreas Schwierz and Håkan Forsberg</i>	

Autonomous Driving and Safety Analysis

Structuring Validation Targets of a Machine Learning Function Applied to Automated Driving	45
<i>Lydia Gauerhof, Peter Munk, and Simon Burton</i>	
Multi-aspect Safety Engineering for Highly Automated Driving: Looking Beyond Functional Safety and Established Standards and Methodologies	59
<i>Patrik Feth, Rasmus Adler, Takeshi Fukuda, Tasuku Ishigooka, Satoshi Otsuka, Daniel Schneider, Denis Uecker, and Kentaro Yoshimura</i>	
A Model-Based Safety Analysis of Dependencies Across Abstraction Layers	73
<i>Christoph Dropmann, Eike Thaden, Mario Trapp, Denis Uecker, Rakshith Amarnath, Leandro Avila da Silva, Peter Munk, Markus Schweizer, Matthias Jung, and Rasmus Adler</i>	

Verification

Formal Verification of Signalling Programs with SafeCap	91
<i>Alexei Iliasov, Dominic Taylor, Linas Laibinis, and Alexander Romanovsky</i>	
Deriving and Formalising Safety and Security Requirements for Control Systems.	107
<i>Elena Troubitsyna and Inna Vistbakka</i>	

Optimal Test Suite Generation for Modified Condition Decision Coverage Using SAT Solving 123
Takashi Kitamura, Quentin Maissonneuve, Eun-Hye Choi, Cyrille Artho, and Angelo Gargantini

Efficient Splitting of Test and Simulation Cases for the Verification of Highly Automated Driving Functions 139
Eckard Böde, Matthias Büker, Ulrich Eberle, Martin Fränzle, Sebastian Gerwinn, and Birte Kramer

Multi-Concern Assurance

Roadblocks on the Highway to Secure Cars: An Exploratory Survey on the Current Safety and Security Practice of the Automotive Industry 157
Michael Huber, Michael Brunner, Clemens Sauerwein, Carmen Carlan, and Ruth Breu

Safe and Secure Automotive Over-the-Air Updates 172
Thomas Chowdhury, Eric Lesiuta, Kerianne Rikley, Chung-Wei Lin, Eunsuk Kang, BaekGyu Kim, Shinichi Shiraishi, Mark Lawford, and Alan Wasssyng

Dependability Analysis of the AFDX Frame Management Design 188
Venesa Watson and Mahlet Bejiga

Fault Tolerance

Efficient On-Line Error Detection and Mitigation for Deep Neural Network Accelerators 205
Christoph Schorn, Andre Guntoro, and Gerd Ascheid

Random Additive Control Flow Error Detection 220
Jens Vankeirsbilck, Niels Penneman, Hans Hallez, and Jeroen Boydens

Fault-Tolerant Clock Synchronization with Only Two Redundant Paths 235
Zoha Moztarzadeh

MORE: MOdel-based REdundancy for Simulink. 250
Kai Ding, Andrey Morozov, and Klaus Janschek

Safety and Security Risk

Diversity in Open Source Intrusion Detection Systems. 267
Hafizul Asad and Ilir Gashi

Inter-device Sensor-Fusion for Action Authorization on Industrial Mobile Robots	282
<i>Sarah Haas, Andrea Höller, Thomas Ulz, and Christian Steger</i>	
Towards a Common Ontology of Safety Risk Concepts for Railway Vehicles and Signaling	297
<i>Bernhard Hulin, Hermann Kaindl, Roland Beckert, Thomas Rathfux, and Roman Popp</i>	
Author Index	311