

*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, Zürich, 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, 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>

Amund Skavhaug · Jérémie Guiochet  
Friedemann Bitsch (Eds.)

# Computer Safety, Reliability, and Security

35th International Conference, SAFECOMP 2016  
Trondheim, Norway, September 21–23, 2016  
Proceedings

*Editors*

Amund Skavhaug  
Norwegian University of Science and  
Technology  
Trondheim  
Norway

Friedemann Bitsch  
Thales Transportation Systems GmbH  
Ditzingen  
Germany

J r mie Guiochet  
University of Toulouse  
Toulouse  
France

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-319-45476-4            ISBN 978-3-319-45477-1 (eBook)  
DOI 10.1007/978-3-319-45477-1

Library of Congress Control Number: 2015948709

LNCS Sublibrary: SL2 – Programming and Software Engineering

  Springer International Publishing Switzerland 2016

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.

Printed on acid-free paper

This Springer imprint is published by Springer Nature  
The registered company is Springer International Publishing AG Switzerland

# Preface

It is our pleasure to present the proceedings of the 35th International Conference on Computer Safety, Reliability, and Security (SAFECOMP 2016), held in Trondheim, Norway, in September 2016. 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 the 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 ever increasing. Currently, we are witnessing the beginning of the era of truly autonomous systems, driverless cars being the most well-known phenomenon to the non-specialist, where the safety and correctness of their computer systems are already being discussed in the main-stream media. In this context, it is clear that the relevance of the SAFECOMP conference series is increasing.

The international Program Committee, consisting of 57 members from 16 countries, received 71 papers from 21 nations. Of these, 24 papers were selected to be presented at the conference.

The review process was thorough with at least 3 reviewers with ensured independency, and 20 of these reviewers met in person in Toulouse, France in April 2016 for the final discussion and selection. Our warm thanks go to the reviewers, who offered their time and competence in the Program Committee work. We are grateful for the support we received from LAAS-CNRS, who in its generosity hosted the PC meeting.

As has been the tradition for many years, the day before the main-track of the conference was dedicated to 6 workshops: DECSoS, ASSURE, SASSUR, CPSELabs, SAFADAPT, and TIPS. Papers from these are published in a separate LNCS volume.

We would like to express our gratitude to the many who have helped with the preparations and running of the conference, especially Friedemann Bitsch as publication chair, Elena Troubitsyna as publicity chair, Erwin Schoitsch as workshop chair, and not to be forgotten the local organization and support staff, Knut Reklef, Sverre Hendseth, and Adam L. Kleppe.

For its support, we would like to thank the Norwegian University of Science and Technology, represented by both the Department of Engineering Cybernetics and the Department for Production and Quality engineering.

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 also in the future.

Finally, the most important persons to whom we would like 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 generally had a memorable time in Trondheim.

September 2016

Amund Skavhaug  
Jérémie Guiochet

# Organization

## EWICS TC7 Chair

Francesca Saglietti      University of Erlangen-Nuremberg, Germany

## General Chair

Amund Skavhaug      The Norwegian University of Science and Technology,  
Norway

## Program Co-chairs

J r mie Guiochet      LAAS-CNRS, University of Toulouse, France  
Amund Skavhaug      The Norwegian University of Science and Technology,  
Norway

## Publication Chair

Friedemann Bitsch      Thales Transportation Systems GmbH, Germany

## Local Organizing Committee

Sverre Hendseth      The Norwegian University of Science and Technology,  
Norway

Knut Reklev      The Norwegian University of Science and Technology,  
Norway

Adam L. Kleppe      The Norwegian University of Science and Technology,  
Norway

## Workshop Chair

Erwin Schoitsch      AIT Austrian Institute of Technology, Austria

## Publicity Chair

Elena Troubitsyna      Åbo Akademi University, Finland

## International Program Committee

Eric Alata      LAAS-CNRS, France  
Friedemann Bitsch      Thales Transportation Systems GmbH, Germany

|                          |  |
|--------------------------|--|
| 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   |
| Nick Chozos              | ADELARD, London, UK  |
| Domenico Cotroneo        | Federico II University of Naples, Italy                                |
| Peter Daniel             | EWICS TC7, UK  |
| Ewen Denney              | SGT/NASA Ames Research Center, USA                                     |
| Felicita Di Giandomenico | ISTI-CNR, Italy  |
| Wolfgang Ehrenberger     | Hochschule Fulda – University of Applied Science, Germany              |
| Francesco Flammini       | Ansaldo STS Italy, Federico II University of Naples, Italy             |
| Barbara Gallina          | Mälardalen University, Sweden  |
| Iilir Gashi              | CSR, City University London, UK  |
| Janusz Górski            | Gdansk University of Technology, Poland                                |
| Lars Grunске             | University of Stuttgart, Germany                                       |
| J r mie Guiochet         | LAAS-CNRS, France  |
| Wolfgang Halang          | Fernuniversit t Hagen, Germany   |
| Poul Heegaard            | The Norwegian University of Science and Technology, Norway             |
| Maritta Heisel           | University of Duisburg-Essen, Germany                                  |
| Bjarne E. Helvik         | The Norwegian University of Science and Technology, Norway             |
| Chris Johnson            | University of Glasgow, UK  |
| Erland Jonsson           | Chalmers University, Stockholm, Sweden                                 |
| Mohamed Ka nische        | LAAS-CNRS, France  |
| Karama Kanoun            | LAAS-CNRS, France  |
| Tim Kelly                | University of York, UK   |
| John Knight              | University of Virginia, USA  |
| Phil Koopman             | Carnegie-Mellon University, USA  |
| Floor Koornneef          | Delft University of Technology, The Netherlands                        |
| Youssef Laarouchi        | Electricit  de France (EDF), France                                    |
| Bev Littlewood           | City University London, UK   |
| Regina Moraes            | Universidade Estadual de Campinas, Brazil                              |
| Takashi Nanya            | Canon Inc., Japan  |
| Odd Nordland             | SINTEF ICT, Trondheim, Norway  |
| Frank Ortmeier           | Otto-von-Guericke Universit t Magdeburg, Germany                       |
| Philippe Palanque        | University of Toulouse, IRIT, France                                   |
| Karthik Pattabiraman     | The University of British Columbia, Canada                             |
| Michael Paulitsch        | Thales Austria GmbH, Austria   |
| Holger Pfeifer           | fortiss GmbH, Germany  |
| 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                          |
| Walter Schön         | Heudiasyc, Université de Technologie de Compiègne,<br>France           |
| Christel Seguin      | Office National d'Etudes et Recherches Aérospatiales,<br>France        |
| Amund Skavhaug       | The Norwegian University of Science and Technology,<br>Norway          |
| 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<br>Engineering, Germany |
| Elena Troubitsyna    | Åbo Akademi University, Finland  |
| Meine van der Meulen | DNV GL, Norway   |
| Coen van Gulijk      | University of Huddersfield, UK   |
| Marcel Verhoef       | European Space Agency, The Netherlands                                 |
| Helene Waeselynck    | LAAS-CNRS, France  |

### **Sub-reviewers**

|                        |  |
|------------------------|--|
| Karin Bernsmed         | SINTEF ICT, Trondheim, Norway                        |
| John Filleau           | Carnegie Mellon University, USA                      |
| Denis Hatebur          | University of Duisburg-Essen, Germany                |
| Alexei Iliasov         | Newcastle University, UK                             |
| Viacheslav Izosimov    | KTH Royal Institute of Technology, Stockholm, Sweden |
| Linus Laibinis         | Åbo Akademi University, Finland                      |
| Paolo Lollini          | University of Florence, Italy                        |
| Mathilde Machin        | APSYS - Airbus, France                               |
| Naveen Mohan           | KTH Royal Institute of Technology, Stockholm, Sweden |
| André Luiz de Oliveira | Universidade Estadual do Norte do Paraná, Brazil     |
| Roberto Natella        | Federico II University of Naples, Italy              |
| Antonio Pecchia        | Federico II University of Naples, Italy              |
| José Rufino            | University of Lisbon, Portugal                       |
| Inna Pereverzeva       | Åbo Akademi University, Finland                      |
| Thomas Santen          | Technische Universität Berlin, Germany               |
| Christoph Schmittner   | AIT Austrian Institute of Technology, Austria        |
| Thierry Sotiropoulos   | LAAS-CNRS, France                                    |
| Milda Zizyte           | Carnegie Mellon University, USA                      |
| Tommaso Zoppi          | University of Florence, Italy                        |

## Sponsoring Institutions

European Workshop on Industrial Computer Systems Reliability, Safety and Security



Norwegian University of Science and Technology



**NTNU – Trondheim**  
Norwegian University of Science and Technology

Laboratory for Analysis and Architecture of Systems, Carnot Institute



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



**Springer**

International Federation for Information Processing



Austrian Institute of Technology



**AUSTRIAN INSTITUTE OF TECHNOLOGY**

Thales Transportation Systems GmbH



Austrian Association for Research in IT



Electronic Components and Systems for European Leadership - Austria



**ECSEL**  
Austria

ARTEMIS Industry Association



European Research Consortium for Informatics  
and Mathematics



Informationstechnische Gesellschaft



German Computer Society



Austrian Computer Society



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



Verband österreichischer Software Industrie



# Contents

## Fault Injection

- FISSC: A Fault Injection and Simulation Secure Collection . . . . . 3  
*Louis Dureuil, Guillaume Petiot, Marie-Laure Potet, Thanh-Ha Le,  
Aude Crohen, and Philippe de Choudens*
- FIDL: A Fault Injection Description Language for Compiler-Based  
SFI Tools. . . . . 12  
*Maryam Raiyat Aliabadi and Karthik Pattabiraman*

## Safety Assurance

- Using Process Models in System Assurance . . . . . 27  
*Richard Hawkins, Thomas Richardson, and Tim Kelly*
- The Indispensable Role of Rationale in Safety Standards . . . . . 39  
*John C. Knight and Jonathan Rowanhill*
- Composition of Safety Argument Patterns . . . . . 51  
*Ewen Denney and Ganesh Pai*

## Formal Verification

- Formal Analysis of Security Properties on the OPC-UA SCADA Protocol . . . 67  
*Maxime Puys, Marie-Laure Potet, and Pascal Lafourcade*
- A Dedicated Algorithm for Verification of Interlocking Systems . . . . . 76  
*Quentin Cappart and Pierre Schaus*
- Catalogue of System and Software Properties . . . . . 88  
*Victor Bos, Harold Bruintjes, and Stefano Tonetta*
- A High-Assurance, High-Performance Hardware-Based  
Cross-Domain System . . . . . 102  
*David Hardin, Konrad Slind, Mark Bortz, James Potts, and Scott Owens*

## Automotive

- Using STPA in an ISO 26262 Compliant Process . . . . . 117  
*Archana Mallya, Vera Pantelic, Morayo Adedjouma, Mark Lawford,  
and Alan Wassyn*

A Review of Threat Analysis and Risk Assessment Methods  
in the Automotive Context . . . . . 130  
*Georg Macher, Eric Armengaud, Eugen Brenner, and Christian Kreiner*

**Anomaly Detection and Resilience**

Context-Awareness to Improve Anomaly Detection in Dynamic Service  
Oriented Architectures . . . . . 145  
*Tommaso Zoppi, Andrea Ceccarelli, and Andrea Bondavalli*

Towards Modelling Adaptive Fault Tolerance for Resilient  
Computing Analysis . . . . . 159  
*William Excoffon, Jean-Charles Fabre, and Michael Lauer*

Automatic Invariant Selection for Online Anomaly Detection . . . . . 172  
*Leonardo Aniello, Claudio Ciccotelli, Marcello Cinque, Flavio Frattini,  
Leonardo Querzoni, and Stefano Russo*

**Cyber Security**

Modelling Cost-Effectiveness of Defenses in Industrial Control Systems . . . . 187  
*Andrew Fielder, Tingting Li, and Chris Hankin*

Your Industrial Facility and Its IP Address: A First Approach  
for Cyber-Physical Attack Modeling . . . . . 201  
*Robert Clausing, Robert Fischer, Jana Dittmann, and Yongjian Ding*

Towards Security-Explicit Formal Modelling of Safety-Critical Systems. . . . . 213  
*Elena Troubitsyna, Linas Laibinis, Inna Pereverzeva, Tuomas Kuismin,  
Dubravka Ilic, and Timo Latvala*

A New SVM-Based Fraud Detection Model for AMI . . . . . 226  
*Marcelo Zanetti, Edgard Jamhour, Marcelo Pellenz, and Manoel Penna*

Exploiting Trust in Deterministic Builds . . . . . 238  
*Christopher Jämthagen, Patrik Lantz, and Martin Hell*

**Fault Trees**

Advancing Dynamic Fault Tree Analysis - Get Succinct State Spaces Fast  
and Synthesise Failure Rates . . . . . 253  
*Matthias Volk, Sebastian Junges, and Joost-Pieter Katoen*

Effective Static and Dynamic Fault Tree Analysis . . . . . 266  
*Ola Bäckström, Yuliya Butkova, Holger Hermanns, Jan Krčál,  
and Pavel Krčál*

**Safety Analysis**

SAFER-HRC: Safety Analysis Through Formal vERification  
in Human-Robot Collaboration . . . . . 283  
*Mehrnoosh Askarpour, Dino Mandrioli, Matteo Rossi,  
and Federico Vicentini*

Adapting the Orthogonal Defect Classification Taxonomy  
to the Space Domain . . . . . 296  
*Nuno Silva and Marco Vieira*

Towards Cloud-Based Enactment of Safety-Related Processes . . . . . 309  
*Sami Alajrami, Barbara Gallina, Irfan Sljivo, Alexander Romanovsky,  
and Petter Isberg*

**Author Index** . . . . . 323