

Communications in Computer and Information Science

1008

Commenced Publication in 2007

Founding and Former Series Editors:

Phoebe Chen, Alfredo Cuzzocrea, Xiaoyong Du, Orhun Kara, Ting Liu,
Dominik Ślęzak, and Xiaokang Yang

Editorial Board

Simone Diniz Junqueira Barbosa

*Pontifical Catholic University of Rio de Janeiro (PUC-Rio),
Rio de Janeiro, Brazil*

Joaquim Filipe

Polytechnic Institute of Setúbal, Setúbal, Portugal

Ashish Ghosh

Indian Statistical Institute, Kolkata, India

Igor Kotenko

*St. Petersburg Institute for Informatics and Automation of the Russian
Academy of Sciences, St. Petersburg, Russia*

Krishna M. Sivalingam

Indian Institute of Technology Madras, Chennai, India

Takashi Washio

Osaka University, Osaka, Japan

Junsong Yuan

University at Buffalo, The State University of New York, Buffalo, USA

Lizhu Zhou

Tsinghua University, Beijing, China

More information about this series at <http://www.springer.com/series/7899>


Cyrille Artho · Peter Csaba Ölveczky (Eds.)

Formal Techniques for Safety-Critical Systems

6th International Workshop, FTSCS 2018
Gold Coast, Australia, November 16, 2018
Revised Selected Papers

Editors

Cyrille Artho
KTH Royal Institute of Technology
Stockholm, Sweden

Peter Csaba Ölveczky 
University of Oslo
Oslo, Norway

ISSN 1865-0929 ISSN 1865-0937 (electronic)
Communications in Computer and Information Science
ISBN 978-3-030-12987-3 ISBN 978-3-030-12988-0 (eBook)
<https://doi.org/10.1007/978-3-030-12988-0>

Library of Congress Control Number: 2019930853

© Springer Nature Switzerland AG 2019

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 6th International Workshop on Formal Techniques for Safety-Critical Systems (FTSCS 2018), held in Gold Coast on November 16, 2018, as a satellite event of the ICFEM conference.

The aim of this workshop is to bring together researchers and engineers who are interested in the application of formal and semi-formal methods to improve the quality of safety-critical computer systems. FTSCS strives to promote research and development of formal methods and tools for industrial applications, and is particularly interested in industrial applications of formal methods. Specific topics include, but are not limited to:

- case studies and experience reports on the use of formal methods for analyzing safety-critical systems, including avionics, automotive, railway, medical, and other kinds of safety-critical and QoS-critical systems;
- methods, techniques, and tools to support automated analysis, certification, debugging, etc., of complex safety/QoS-critical systems;
- analysis methods that address the limitations of formal methods in industry (usability, scalability, etc.);
- formal analysis support for modeling languages used in industry, such as AADL, Ptolemy, SysML, SCADE, Modelica, etc.; and
- code generation from validated models.

The workshop received 22 regular paper submissions. Each submission was reviewed by at least three referees. Based on the reviews and extensive discussions, the program committee selected ten papers for presentation at the workshop and inclusion in this volume. Another highlight of the workshop was an invited talk by César Muñoz on the use of formal methods at NASA during the development of highly assured software for unmanned aircraft systems.

Many colleagues and friends contributed to FTSCS 2018. We thank César Muñoz for accepting our invitation to give an invited talk and the authors who submitted their work to FTSCS 2018 and who, through their contributions, made this workshop an interesting event. We are particularly grateful to the members of the program committee, who provided timely, insightful, and detailed reviews. We also thank the editors of *Communications in Computer and Information Science* for agreeing to publish the proceedings of FTSCS 2018 as a volume in their series, and Jin Song Dong for his help with the local arrangements.

January 2019

Cyrille Artho
Peter Csaba Ölveczky

Organization

Program Chairs

Cyrille Artho
Peter Csaba Ölveczky

KTH Royal Institute of Technology, Sweden
University of Oslo, Norway

Program Committee

Étienne André
Toshiaki Aoki
Cyrille Artho
Kyungmin Bae
Daniel Fava
Sabine Glesner
Osman Hasan

Université Paris 13, France
JAIST, Japan
KTH Royal Institute of Technology, Sweden
Pohang University of Science and Technology, Korea
University of Oslo, Norway
TU Berlin, Germany
National University of Sciences and Technology,
Pakistan

Klaus Havelund
Jérôme Hugues
Marieke Huisman
Ralf Huuck
Fuyuki Ishikawa
Takashi Kitamura

Jet Propulsion Laboratory, USA
ISAE, France
University of Twente, The Netherlands
UNSW/SYNOPSIS, Australia
National Institute of Informatics, Japan
National Institute of Advanced Industrial Science
and Technology (AIST), Japan

Thierry Lecomte
Yang Liu
Robi Malik
Frédéric Mallet
Roberto Nardone
Thomas Noll
Peter Csaba Ölveczky
David Pearce
Markus Roggenbach
Ralf Sasse
Martina Seidl
Graeme Smith
Sofiene Tahar
Carolyn Talcott
Tatsuhiko Tsuchiya

ClearSy, France
Nanyang Technological University, Singapore
University of Waikato, New Zealand
Université Nice Sophia-Antipolis, France
Mediterranean University of Reggio Calabria, Italy
RWTH Aachen University, Germany
University of Oslo, Norway
Victoria University of Wellington, New Zealand
Swansea University, UK
ETH Zürich, Switzerland
Johannes Kepler University Linz, Austria
The University of Queensland, Australia
Concordia University, Canada
SRI International, USA
Osaka University, Japan

| | |
|----------------|---|
| Mark Utting | University of the Sunshine Coast, Australia |
| András Vörös | Budapest University of Technology and Economics, Hungary |
| Michael Whalen | University of Minnesota, USA |
| Huibiao Zhu | East China Normal University, China |

Additional Reviewers

Elderhalli, Yassmeen
Siddique, Umair

Formal Methods in the Development of Highly Assured Software for Unmanned Aircraft Systems (Invited Paper)

César Muñoz

NASA Langley Research Center, Hampton, USA

Abstract. Operational requirements of safety-critical systems are often written in restricted specification logics. These restricted logics are amenable to automated analysis techniques such as model-checking, but are not rich enough to express complex requirements of unmanned systems that involve, for example, the physical environment. This talk advocates the use of expressive logics, such as higher-order logic, to specify the complex operational requirements and safety properties of unmanned systems. These rich logics are less amenable to automation and, hence, require the use of interactive theorem proving techniques. However, they enable the formal verification of complex numerically intensive algorithms and the rigorous validation of their implementations. The proposed approach is illustrated with two cases studies from NASA's research on Unmanned Aircraft Systems (UAS): Detect and Avoid Alerting Logic for Unmanned Systems (DAIDALUS) and Independent Configurable Architecture for Reliable Operations of Unmanned Systems (ICAROUS). DAIDALUS is the reference implementation of detect and avoid for UAS in FAA DO-365. ICAROUS is a software architecture built on top of DAIDALUS that enables the development of autonomous UAS applications.

Contents

Analysis and Verification of Safety-Critical Systems

| | |
|---|----|
| Formal Stability Analysis of Control Systems | 3 |
| <i>Asad Ahmed, Osman Hasan, and Falah Awwad</i> | |
| Modular Verification of Vehicle Platooning with Respect to Decisions, Space and Time | 18 |
| <i>Maryam Kamali, Sven Linker, and Michael Fisher</i> | |
| Synthesizing and Optimizing FDIR Recovery Strategies from Fault Trees . . . | 37 |
| <i>Liana Mikaelyan, Sascha Müller, Andreas Gerndt, and Thomas Noll</i> | |
| Formal Verification of Random Forests in Safety-Critical Applications | 55 |
| <i>John Törnblom and Simin Nadjm-Tehrani</i> | |

Analysis of Timed Systems

| | |
|--|-----|
| A Benchmark Library for Parametric Timed Model Checking. | 75 |
| <i>Étienne André</i> | |
| Formal Timing Analysis of Digital Circuits | 84 |
| <i>Qurat Ul Ain and Osman Hasan</i> | |
| Embedding CCSL into Dynamic Logic: A Logical Approach for the Verification of CCSL Specifications | 101 |
| <i>Yuanrui Zhang, Hengyang Wu, Yixiang Chen, and Frédéric Mallet</i> | |

Semantics and Analysis Methods

| | |
|---|-----|
| Refinement of Statecharts with Run-to-Completion Semantics. | 121 |
| <i>Karla Morris, Colin Snook, Thai Son Hoang, Robert Armstrong, and Michael Butler</i> | |
| Abstraction Refinement with Path Constraints for 3-Valued Bounded Model Checking | 139 |
| <i>Nils Timm and Stefan Gruner</i> | |

Model Transformation

Model Transformation with Triple Graph Grammars
and Non-terminal Symbols 161
*William da Silva, Max Bureck, Ina Schieferdecker,
and Christian Hein*

Author Index 179