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

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

Springer

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

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	KTH Royal Institute of Technology, Sweden
Peter Csaba Ölveczky	University of Oslo, Norway

Program Committee

Étienne André	Université Paris 13, France
Toshiaki Aoki	JAIST, Japan
Cyrille Artho	KTH Royal Institute of Technology, Sweden
Kyungmin Bae	Pohang University of Science and Technology, Korea
Daniel Fava	University of Oslo, Norway
Sabine Glesner	TU Berlin, Germany
Osman Hasan	National University of Sciences and Technology, Pakistan
Klaus Havelund	Jet Propulsion Laboratory, USA
Jérôme Hugues	ISAE, France
Marieke Huisman	University of Twente, The Netherlands
Ralf Huuck	UNSW/SYNOPSYS, Australia
Fuyuki Ishikawa	National Institute of Informatics, Japan
Takashi Kitamura	National Institute of Advanced Industrial Science and Technology (AIST), Japan
Thierry Lecomte	ClearSy, France
Yang Liu	Nanyang Technological University, Singapore
Robi Malik	University of Waikato, New Zealand
Frédéric Mallet	Université Nice Sophia-Antipolis, France
Roberto Nardone	Mediterranean University of Reggio Calabria, Italy
Thomas Noll	RWTH Aachen University, Germany
Peter Csaba Ölveczky	University of Oslo, Norway
David Pearce	Victoria University of Wellington, New Zealand
Markus Roggenbach	Swansea University, UK
Ralf Sasse	ETH Zürich, Switzerland
Martina Seidl	Johannes Kepler University Linz, Austria
Graeme Smith	The University of Queensland, Australia
Sofiene Tahar	Concordia University, Canada
Carolyn Talcott	SRI International, USA
Tatsuhiro Tsuchiya	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

Analysis of Timed Systems

Semantics and Analysis Methods

Model Transformation