

Founding Editors

Gerhard Goos

Karlsruhe Institute of Technology, Karlsruhe, Germany

Juris Hartmanis

Cornell University, Ithaca, NY, USA

Editorial Board Members

Elisa Bertino

Purdue University, West Lafayette, IN, USA

Wen Gao

Peking University, Beijing, China

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Gerhard Woeginger 

RWTH Aachen, Aachen, Germany

Moti Yung

Columbia University, New York, NY, USA


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

Yiannis Papadopoulos · Koorosh Aslansefat ·
Panagiotis Katsaros · Marco Bozzano (Eds.)

Model-Based Safety and Assessment


6th International Symposium, IMBSA 2019
Thessaloniki, Greece, October 16–18, 2019
Proceedings

Editors

Yiannis Papadopoulos 
University of Hull
Hull, UK

Panagiotis Katsaros
Aristotle University of Thessaloniki
Thessaloniki, Greece

Koorosh Aslansefat 
University of Hull
Hull, UK

Marco Bozzano 
Fondazione Bruno Kessler
Trento, Trento, Italy

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-030-32871-9

ISBN 978-3-030-32872-6 (eBook)

<https://doi.org/10.1007/978-3-030-32872-6>

LNCS Sublibrary: SL2 – Programming and Software Engineering

© 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, expressed 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 papers presented at IMBSA 2019: the International Symposium on Model-Based Safety and Assessment, held during October 16–18, 2019, in Thessaloniki, Greece.

IMBSA focuses on model-based and automated ways of assessing safety and other attributes of dependability of complex computer systems. Since the first edition in Toulouse (2011), the workshop has evolved to a forum where brand new ideas from academia, leading-edge technology, and industrial experiences are brought together. The objectives are to present experiences and tools, to share ideas, and to federate the community.

This year a particular space was given to the assessment of open systems, autonomous systems, and systems that employ artificial intelligence (AI). There are specific challenges in the assessment of such systems which include unboundness, the infinity of possible configurations, uncertainty, and particularities related to the reasoning and operation of AI components.

To foster academic and industrial collaboration, in addition to more traditional talks reporting on novel advances on hot research topics, the program featured a poster and tutorial sessions, where speakers had the opportunity to present ongoing research and industrial experiences, and demonstrate their tool interactively.

We believe that a mixture of conventional talks about the newest achievements, the presentation of practical experiences, and interactive learning facilitates fruitful discussions, the exchange of information, as well as future cooperation. Therefore, following the previous edition of IMBSA in Trento (2017), an important focus of this year's edition in Thessaloniki was placed on tool tutorials and demonstrations. Nevertheless, the main scientific and industrial contributions were presented in traditional talks and are collected in this volume of LNCS.

For IMBSA 2019, we received 46 regular submissions from authors of 17 countries. Following rigorous review, the best 24 of these papers were selected by an international Program Committee to be published in this volume. As organizers, we want to extend a very warm thank you to all 50 members of the international Program Committee. Each submission was reviewed by at least three Program Committee members. The comprehensive review guaranteed the high quality of the accepted papers. We also want to thank the local organization team in Thessaloniki, and our fellow members of the Steering Committee: Leila Kloul, Frank Ortmeier, Antoine Rauzy, and Christel Seguin.

Finally, we wish you a pleasant reading of the articles in this volume. On behalf of everyone involved in this year's International Symposium on Model-Based Safety and Assessment, we hope you will be joining us at the next edition of IMBSA.

September 2019

Yiannis Papadopoulos
Koorosh Aslansefat
Panagiotis Katsaros
Marco Bozzano

Organization

General Chairs

Panagiotis Katsaros	Aristotle University of Thessaloniki, Greece
Yiannis Papadopoulos	University of Hull, UK

Program Committee Chairs

Marco Bozzano	FBK, Italy
Antoine Rauzy	Norwegian University of Science and Technology, Norway

Tools and Tutorials Chairs

Leila Kloul	Université de Versailles, France
Frank Ortmeier	Otto-von-Guericke University of Magdeburg, Germany

Industrial Chairs

Jean-Paul Blanquart	Airbus Defence and Space, France
Christel Seguin	ONERA, France

Organizing Committee

Yiannis Papadopoulos	University of Hull, UK
Koorosh Aslansefat	University of Hull, UK
David Parker	University of Hull, UK
Panagiotis Katsaros	Aristotle University of Thessaloniki, Greece

Program Committee

Ezio Bartocci	Technische Universität Wien, Austria
Stylianios Basagiannis	United Technologies Research Centre, Ireland
Saddek Bensalem	Universirsité Grenoble Alpes, France
Jean-Paul Blanquart	Airbus Defence and Space, France
Simon Bliudze	Inria Lille, France
Marc Bouissou	EDF, France
Marco Bozzano	FBK, Italy
Jean-Charles Chaudemar	ISAE, France
Lorenzo Bitetti	Thales Alenia Space, France
Jana Dittmann	Otto-von-Guericke University of Magdeburg, Germany
Marielle Doche-Petit	Systerel, France

Nicholas Matragkas	University of York, UK
Joxe Aizpurua Unanue	Mondragon University, Spain
Francesco Flammini	University of Naples, Italy
Lars Fücke	Diehl Aviation, Germany
Lars Grunske	Humboldt University Berlin, Germany
Matthias Güdemann	Input-Output Hong-Kong, China
Brendan Hall	Honeywell, USA
Kai Höfig	Siemens, Germany
Michaela Huhn	Ostfalia, Germany
Panagiotis Katsaros	Aristotle University of Thessaloniki, Greece
Tim Kelly	University of York, UK
Leila Kloul	Universite de Versailles, France
Agnes Lanusse	CEA LIST, France
Timo Latvala	Space Systems Finland, Finland
Till Mossakowski	Otto-von-Guericke University of Magdeburg, Germany
Jürgen Mottok	University of Regensburg, Germany
Thomas Noll	RWTH Aachen University, Germany
Frank Ortmeier	Otto-von-Guericke University of Magdeburg, Germany
Yiannis Papadopoulos	University of Hull, UK
Antoine Rauzy	Norwegian University of Science and Technology, Norway
Wolfgang Reif	Augsburg University, Germany
Jean-Marc Roussel	LURPA, ENS Cachan, France
Christel Seguin	ONERA, France
Ramin Tavakoli Kolagari	Technische Hochschule Nürnberg, Germany
Pascal Traverse	Airbus, France
Elena A. Troubitsyna	KTH, Sweden
Marcel Verhoef	European Space Agency, The Netherlands
Lijun Zhang	Chinese Academy of Sciences, China
Marc Zeller	Siemens, Germany

Steering Committee

Marco Bozzano	FBK, Italy
Leila Kloul	Universite de Versailles, France
Frank Ortmeier	Otto-von-Guericke University of Magdeburg, Germany
Yiannis Papadopoulos	University of Hull, UK
Antoine Rauzy	Norwegian University of Science and Technology, Norway
Christel Seguin	ONERA, France

Additional Reviewers

Sohag Kabir	University of Hull, UK
Youcef Gheraibia	University of York, UK
Alexander Knapp	University of London, UK
Viorel Preoteasa	Aalto University, Finland

Contents

Safety Models and Languages

Modeling Functional Allocation in AltaRica to Support MBSE/MBSA Consistency	3
<i>Mathilde Machin, Estelle Saez, Pierre Virelizier, and Xavier de Bossoreille</i>	
Model Based Approach for RAMS Analyses in the Space Domain with Capella Open-Source Tool	18
<i>Lorenzo Bitetti, Régis De Ferluc, David Mailland, Guy Gregoris, and Fulvio Capogna</i>	
Modeling Patterns for the Assessment of Maintenance Policies with AltaRica 3.0	32
<i>Michel Batteux, Tatiana Prosvirnova, and Antoine Rauzy</i>	
A Domain Specific Language to Support HAZOP Studies of SysML Models	47
<i>Arut Prakash Kaleeswaran, Peter Munk, Samir Sarkic, Thomas Vogel, and Arne Nordmann</i>	
Integrating Existing Safety Analyses into SysML	63
<i>Kester Clegg, Mole Li, David Stamp, Alan Grigg, and John McDermid</i>	
FDS-ML: A New Modeling Formalism for Probabilistic Risk and Safety Analyses	78
<i>Liu Yang and Antoine Rauzy</i>	
Integrating Safety Design Artifacts into System Development Models Using SafeDeML	93
<i>Tim Gonschorek, Philipp Bergt, Marco Filax, and Frank Ortmeier</i>	

Dependability Analysis Processes

A Conceptual Framework to Incorporate Complex Basic Events in HiP-HOPS	109
<i>Sohag Kabir, Koorosh Aslansefat, Ioannis Sorokos, Yiannis Papadopoulos, and Youcef Gheraibia</i>	
Compositionality of Component Fault Trees	125
<i>Simon Greiner, Peter Munk, and Arne Nordmann</i>	

Tiered Model-Based Safety Assessment	141
<i>Kevin Delmas, Christel Seguin, and Pierre Bieber</i>	
Model Synchronization: A Formal Framework for the Management of Heterogeneous Models.	157
<i>Michel Batteux, Tatiana Prosvirnova, and Antoine Rauzy</i>	
DPN – Dependability Priority Numbers	173
<i>Zhensheng Guo and Marc Zeller</i>	
Towards Dependability and Energy Aware Asset Management Framework for Maintenance Planning in Smart Grids.	188
<i>Jose Ignacio Aizpurua, Unai Garro, Eñaut Muxika, Mikel Mendicute, and Ian Paul Gilbert</i>	
Formal Verification of Network Interlocking Control by Distributed Signal Boxes	204
<i>Stylianios Basagiannis and Panagiotis Katsaros</i>	
SQUADfps: Integrated Model-Based Machine Safety and Product Quality for Flexible Production Systems	222
<i>Chee Hung Koo, Stefan Rothbauer, Marian Vorderer, Kai Höfig, and Marc Zeller</i>	
Security Assessment	
A Serverless Architecture for Wireless Body Area Network Applications. . . .	239
<i>Pangkaj Chandra Paul, John Loane, Fergal McCaffery, and Gilbert Regan</i>	
Automated Model-Based Attack Tree Analysis Using HiP-HOPS	255
<i>Declan Whiting, Ioannis Sorokos, Yiannis Papadopoulos, Gilbert Regan, and Eoin O’Carroll</i>	
What Today’s Serious Cyber Attacks on Cars Tell Us: Consequences for Automotive Security and Dependability	270
<i>Markus Zoppelt and Ramin Tavakoli Kolagari</i>	
Safety and Security Aspects of Fail-Operational Urban Surround perceptiON (FUSION).	286
<i>Georg Macher, Norbert Druml, Omar Veledar, and Jakob Reckenzaun</i>	
Safety Assessment in Automotive Industry	
An Approach for Validating Safety of Perception Software in Autonomous Driving Systems	303
<i>Deepak Rao, Plato Pathrose, Felix Huening, and Jithin Sid</i>	

Stochastic Modelling of Autonomous Vehicles Driving Scenarios Using PEPA	317
<i>Wei Chen and Leïla Kloul</i>	
A Runtime Safety Analysis Concept for Open Adaptive Systems	332
<i>Sohag Kabir, Ioannis Sorokos, Koorosh Aslansefat, Yiannis Papadopoulos, Youcef Gheraibia, Jan Reich, Merve Saimler, and Ran Wei</i>	
AI in Safety Assessment	
Clustering Environmental Conditions of Historical Accident Data to Efficiently Generate Testing Sceneries for Maritime Systems	349
<i>Tim Wuellner, Sebastian Feuerstack, and Axel Hahn</i>	
Pattern-Based Formal Approach to Analyse Security and Safety of Control Systems	363
<i>Inna Vistbakka and Elena Troubitsyna</i>	
Author Index	379