

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Alfred Kobsa

University of California, Irvine, CA, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, 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, Saarbruecken, Germany

Frank Ortmeier Antoine Rauzy (Eds.)

Model-Based Safety and Assessment

4th International Symposium, IMBSA 2014
Munich, Germany, October 27-29, 2014
Proceedings



Springer

Preface

The International Symposium on Model-Based Safety and Assessment (IMBSA) has now been held for the fourth time. 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. To foster academic and industrial collaboration, the program is split into three main parts: an academic part presenting new research, a tools and tutorials part presenting leading-edge development support, and an industrial part reporting on experiences and challenges in industrial practice.

The last conferences in Bordeaux (2012) and Versailles (2013) showed an increasing interest in practical demonstrations of model-based safety analysis techniques and tools. As a consequence, tool and tutorial demonstrations are now an important part in the event's program. We believe that a mixture of conventional talks about the newest achievements, presentation of practical experiences, and interactive learning allows for fruitful discussions, exchange of information, as well as future cooperation. Therefore, the focus of this year's edition in Munich, Germany, was placed on the tools and tutorials session, which, as a premiere, was given a full-day time slot.

Nevertheless, the main scientific and industrial contributions were presented in traditional talks and are published in this special volume of LNCS. For IMBSA 2014, we received 31 submission from authors of 12 countries. The best 15 of these papers were selected by an international Program Committee to be published in this volume. In addition to this LNCS volume, IMBSA 2014 also published separate tutorial and tool proceedings. These are aimed at an industrial audience and focus on recapitulating the practical demonstrations.

As program chairs, we want to extend a very warm thank you to all 24 members of the international Program Committee. The comprehensive review guaranteed the high quality of the accepted papers. We also want to thank the local organization team at the Otto von Guericke University of Magdeburg (OvGU), the chairs Martin Bott, Jürgen Mottok, and Christel Seguin, the Zühle Engineering Group, and the Gesellschaft für Informatik (GI).

Finally, we wish you pleasant reading of the articles in this volume. On behalf of everyone involved in this year's International Symposium on Model-Based Safety Assessment, we hope you will be joining us at the 2015 IMBSA edition.

August 2014

Frank Ortmeier
Antoine Rauzy

Organization

Program Committee

Jean-Paul Blanquart	Astrium Satellites, France
Martin Bott	Züelke Engineering, Germany
Marco Bozzano	FBK-irst, Italy
Jean-Charles Chaudemar	ISAE, France
Jana Dittmann	Otto von Guericke University Magdeburg, Germany
Marielle Doche-Petit	Systemel, France
Lars Grunске	University of Stuttgart, Germany
Matthias Güdemann	Systemel, France
Michaela Huhn	Technical University of Clausthal, Germany
Kai Höfig	Siemens AG, Germany
Tim Kelly	University of York, UK
Leila Kloul	Université de Versailles, France
Agnes Lanusse	CEA LIST, France
Till Mossakowski	Otto von Guericke University of Magdeburg, Germany
Juergen Mottok	LaS, OTH Regensburg
Frank Ortmeier	Otto von Guericke University of Magdeburg, Germany
Yiannis Papadopoulos	University of Hull, UK
Antoine Rauzy	École Polytechnique, France
Wolfgang Reif	Augsburg University, Germany
Jean-Marc Roussel	LURPA, ENS Cachan, France
Christel Seguin	ONERA, France
Pascal Traverse	Airbus, France

Table of Contents

Modeling Paradigms

A Practicable MBSA Modeling Process Using Altarica	1
<i>Shaojun Li and Su Duo</i>	
On Efficiently Specifying Models for Model Checking	14
<i>Mykhaylo Nykolaychuk, Michael Lipaczewski, Tino Liebusch, and Frank Ortmeier</i>	
A Model-Based Methodology to Formalize Specifications of Railway Systems	28
<i>Melissa Issad, Leïla Kloul, and Antoine Rauzy</i>	

Validation and Testing

A Systematic Approach to Requirements Driven Test Generation for Safety Critical Systems	43
<i>Toby Wilkinson, Michael Butler, and John Colley</i>	
Model-Based Safety Approach for Early Validation of Integrated and Modular Avionics Architectures	57
<i>Marion Morel</i>	
Exploring the Impact of Different Cost Heuristics in the Allocation of Safety Integrity Levels	70
<i>Luís Silva Azevedo, David Parker, Yiannis Papadopoulos, Martin Walker, Ioannis Sorokos, and Rui Esteves Araújo</i>	

Fault Detection and Handling

An Integrated Process for FDIR Design in Aerospace	82
<i>Benjamin Bittner, Marco Bozzano, Alessandro Cimatti, Regis De Ferluc, Marco Gario, Andrea Guiotto, and Yuri Yushtein</i>	
Reliability Analysis of Dynamic Systems by Translating Temporal Fault Trees into Bayesian Networks	96
<i>Sohag Kabir, Martin Walker, and Yiannis Papadopoulos</i>	
metaFMEA-A Framework for Reusable FMEAs	110
<i>Kai Höfig, Marc Zeller, and Lars Grunske</i>	

Safety Assessment in the Automotive Domain

AltaRica 3 Based Models for ISO 26262 Automotive Safety Mechanisms	123
<i>Abraham Cherfi, Antoine Rauzy, and Michel Leeman</i>	
A Pattern-Based Approach towards the Guided Reuse of Safety Mechanisms in the Automotive Domain	137
<i>Maged Khalil, Alejandro Prieto, and Florian Hölzl</i>	
Towards the Derivation of Guidelines for the Deployment of Real-Time Tasks on a Multicore Processor	152
<i>Stefan Schmidhuber, Michael Deubzer, Ralph Mader, Michael Niemetz, and Jürgen Mottok</i>	

Case Studies

Adaptive Error and Sensor Management for Autonomous Vehicles: Model-Based Approach and Run-Time System	166
<i>Jelena Frtunikj, Vladimir Rupanov, Michael Armbruster, and Alois Knoll</i>	
Safety Assessment of an Electrical System with AltaRica 3.0	181
<i>Hala Mortada, Tatiana Prosvirnova, and Antoine Rauzy</i>	
Applying Formal Methods into Safety-Critical Health Applications	195
<i>Mohammad-Reza Gholami and Hanifa Boucheneb</i>	
Author Index	209