

Lecture Notes in Computer Science

14010


Founding Editors


Gerhard Goos
Juris Hartmanis

Editorial Board Members

Elisa Bertino, *Purdue University, West Lafayette, IN, USA*

Wen Gao, *Peking University, Beijing, China*

Bernhard Steffen , *TU Dortmund University, Dortmund, Germany*

Moti Yung , *Columbia University, New York, NY, USA*

The series Lecture Notes in Computer Science (LNCS), including its subseries Lecture Notes in Artificial Intelligence (LNAI) and Lecture Notes in Bioinformatics (LNBI), has established itself as a medium for the publication of new developments in computer science and information technology research, teaching, and education.

LNCS enjoys close cooperation with the computer science R & D community, the series counts many renowned academics among its volume editors and paper authors, and collaborates with prestigious societies. Its mission is to serve this international community by providing an invaluable service, mainly focused on the publication of conference and workshop proceedings and postproceedings. LNCS commenced publication in 1973.

Uwe Glässer · Jose Creissac Campos ·
Dominique Méry · Philippe Palanque
Editors

Rigorous State-Based Methods


9th International Conference, ABZ 2023
Nancy, France, May 30 – June 2, 2023
Proceedings

Editors

Uwe Glässer
Simon Fraser University
Burnaby, BC, Canada

Jose Creissac Campos
University of Minho
Braga, Portugal

Dominique Méry 
Université de Lorraine
Vandoeuvre-lès-Nancy, France

Philippe Palanque 
University of Toulouse
Toulouse, France

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-031-33162-6

ISBN 978-3-031-33163-3 (eBook)

<https://doi.org/10.1007/978-3-031-33163-3>

© The Editor(s) (if applicable) and The Author(s), under exclusive license
to Springer Nature Switzerland AG 2023

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

The International Conference on Rigorous State-Based Methods (ABZ 2023) was an international forum for the cross-fertilization of related state-based and machine-based formal methods, mainly Abstract StateMachines (ASM), Alloy, B, TLA +, VDM and Z. Rigorous state-based methods share common conceptual foundations and are widely used in both academia and industry for the design and analysis of hardware and software systems. The acronym ABZ was invented at the first conference, held in London in 2008, where the ASM, B and Z conference series merged into a single event. The second ABZ 2010 conference was held in Orford (Canada), where the Alloy community joined the event; ABZ 2012 was held in Pisa (Italy), which saw the inclusion of the VDM community (but not in the title); ABZ 2014 was held in Toulouse (France), which brought the inclusion of the TLA + community into the ABZ conference series. Lastly, the ABZ 2016 conference was held in Linz, Austria and ABZ 2018 in Southampton, UK. In 2018 the steering committee decided to retain the (well-known) acronym ABZ and add the subtitle ‘International Conference on Rigorous State-Based Methods’ to make more explicit the intention to include all state-based formal methods. Two successive ABZ events have been organized in Ulm (Germany) and these were the two first virtual ABZ events.

Since 2014 in Toulouse, each ABZ asked for the application of formal specifications on industrial case studies. This year, we extend the previous areas (aerospace, medical equipment, rails, automotive) with the HMI domain. The ABZ 2023 case study introduces a safety critical interactive system called AMAN (Arrival MANager), which is a partly autonomous scheduler of landing sequences of aircraft in airports. This interactive system interleaves Air Traffic Controller’s activities with automation in AMAN. While some AMAN systems are currently deployed in airports, we consider here only a subset of functions which represent a challenge in modelling and verification. The ABZ 2023 case study is provided by José C. Campos and Philippe Palanque, who have interacted with authors of submissions for the case study and did a great job while managing the review process of the five submissions in five different modelling languages, namely B, Event-B, ASM, Alloy and Statecharts. They accepted four of those submissions for presentation at ABZ 2023 and inclusion in the proceedings. As usual, a special issue will be organized in a Springer journal for a larger audience and inviting other replies to the ABZ 2023 case study. José and Phil answered almost a hundred questions and gave clarifying explanations, for which we would like to thank them. The objective of these case studies is to provide an opportunity to demonstrate the applicability of the ABZ methods to real examples and also to allow a better comparison of them. You should visit the link <https://abz-conf.org/case-studies/> which collects the past case studies with solutions. ABZ 2023 received 47 submissions from 22 countries around the world. The selection process was rigorous, where each paper received at least four reviews. The program committee, after careful discussions, decided to accept 8 full research papers, 3 journal-first papers, 5 short research papers and 2 industry papers. The acceptance ratio

of those papers was 18 accepted out of 38 which is 46%. Four case study papers were accepted and selected by a separate sub-committee; the acceptance rate was 80%. One research paper of one of the four keynote speakers is also included in the proceedings. All accepted papers cover broad research areas in both theoretical systems and practical aspects of state-based methods. A doctoral symposium was organized and PhD students had to submit a short paper presenting their PhD topics; those 4 submissions were evaluated by a separate PC committee including the two chairs of ABZ; the review of the four submitted PhD contributions was conducted by Silvia Bonfanti and Guillaume Dupont. Thanks Silvia and Guillaume for your contribution to the programme of ABZ 2023! The conference was held on May 30 – June 2, 2023 in Nancy, France and the venue was the LORIA laboratory, a joint structure of CNRS, Inria and the University of Lorraine.

We are honored that all four distinguished guests as keynote speakers have agreed to give their keynotes this year. Marieke Huisman, University of Twente, The Netherlands, gave a talk entitled ‘VerCors & Alpinist: verification of optimised GPU programs’; Véronique Cortier, LORIA CNRS, Inria and Université de Lorraine, France, gave a talk entitled ‘Formal verification of electronic voting systems’; André Platzer, Karlsruhe Institute of Technology, Germany and Carnegie Mellon University, USA, gave a talk entitled ‘Refinements in Hybrid Dynamical Systems Logic’; finally, Burkhart Wolff, University Paris Saclay and Laboratoire des Méthodes Formelles (LMF), France, gave a talk entitled ‘Using Deep Ontologies in Formal Software Engineering’.

The EasyChair conference management system was set up for ABZ 2023, supporting submission, review and volume editing processes. We acknowledge it is an outstanding tool for the academic community. We would like to thank all the authors who submitted their work to ABZ 2023. We are grateful to the program committee members and external reviewers for their high-quality reviews and discussions. Finally, we wish to thank the Organizing Committee members for their continuous support. When writing the preface, we have also to mention the continuous support and assistance of Springer and the publishing team managed by Ronan Nugent. Finally, we would like to thank our sponsors:

- the LORIA laboratory for contributing to the budget and for providing a strong administrative support for the organisation.
- l’Université de Lorraine and la Métropole du Grand Nancy for financial support.
- the GDR CNRS GPL for supporting PhD students participation.
- the ANR projects DISCONT (<https://anr.fr/Projet-ANR-17-CE25-0005>) and EBRP Plus (<https://anr.fr/Projet-ANR-19-CE25-0010>) for financial contribution.

For readers of these proceedings, we hope these papers are interesting and they inspire ideas for future research.

April 2023

José C. Campos
Uwe Glässer
Dominique Méry
Philippe Palanque

José Creissac Campos	University of Minho & HASLab/INESC TEC, Portugal
David Deharbe	ClearSy System Engineering, France
Juergen Dingel	Queen's University, Canada
Catherine Dubois	ENSIIE-Samovar, France
Guillaume Dupont	IRIT/INPT-ENSEEIH, France
Marie Farrell	University of Manchester, UK
Flavio Ferrarotti	Software Competence Centre Hagenberg, Austria
Simon Foster	University of York, UK
Marc Frappier	Université de Sherbrooke, Canada
Angelo Gargantini	University of Bergamo, Italy
Vincenzo Gervasi	University of Pisa, Italy
Uwe Glässer	Simon Fraser University, Canada
Gudmund Grov	Norwegian Defence Research Establishment (FFI), Norway
Stefan Hallerstede	Aarhus University, Denmark
Klaus Havelund	Jet Propulsion Laboratory, USA
Ian J. Hayes	The University of Queensland, Australia
Thai Son Hoang	University of Southampton, UK
Frank Houdek	Mercedes-Benz AG, Austria
Alexei Iliasov	The Formal Route, UK
Fuyuki Ishikawa	National Institute of Informatics, Japan
Igor Konnov	Informal Systems Austria, Austria
Olga Kouchnarenko	University of Franche-Comté, France
Markus Alexander Kuppe	Microsoft, USA
Regine Laleau	Paris-Est Creteil University, France
Thierry Lecomte	ClearSy System Engineering, France
Martin Leucker	University of Lübeck, Germany
Michael Leuschel	University of Düsseldorf, Germany
Alexei Lisitsa	University of Liverpool, UK
Nuno Macedo	University of Porto & INESC TEC, Portugal
Frederic Mallet	Universite Nice Sophia-Antipolis, France
Tiziana Margaria	Lero and University of Limerick, Ireland
Paolo Masci	National Institute of Aerospace (NIA), USA
Atif Mashkoor	Johannes Kepler University Linz, Austria
Jackson Mayo	Sandia National Laboratories, USA
Dominique Mery	Université de Lorraine, LORIA, France
Stephan Merz	Inria, LORIA, France
Stefan Mitsch	Carnegie Mellon University, USA
Rosemary Monahan	Maynooth University, Ireland
Mohamed Mosbah	University of Bordeaux, France
Shin Nakajima	National Institute of Informatics, Japan

Uwe Nestmann	TU Berlin, Germany
Jose Oliveira	University of Minho & HASLab/INESC TEC, Portugal
Philippe Palanque	ICS-IRIT, Paul Sabatier University, France
Luigia Petre	Åbo Akademi University, Finland
Andreas Prinz	University of Agder, Norway
Philippe Queinnec	IRIT - Université de Toulouse, France
Alexander Raschke	Ulm University, Germany
Elvinia Riccobene	University of Milan, Italy
Markus Roggenbach	Swansea University, UK
Patrizia Scandurra	University of Bergamo, Italy
Gerhard Schellhorn	Universität Augsburg, Germany
Klaus-Dieter Schewe	Zhejiang University, China
Steve Schneider	University of Surrey, UK
Neeraj Singh	INPT-ENSEEIH/IRIT, University of Toulouse, France
Maurice ter Beek	ISTI-CNR, Pisa, Italy
Elena Troubitsyna	KTH, Sweden
Laurent Voisin	Systemel, France
Alan Wassyng	McMaster University, Canada
Virginie Wiels	ONERA/DTIS, France
Naijun Zhan	Institute of Software, Chinese Academy of Sciences, China
Huibiao Zhu	East China Normal University, China
Wolf Zimmermann	Martin Luther University Halle-Wittenberg, Germany

Additional Reviewers

Chen, Ningning	Mendil, Ismail
Cheng, Zheng	Monahan, Rosemary
Fakhfakh, Faten	Poorhadi, Ehsan
Farrell, Marie	Safina, Larisa
Feliu Gabaldon, Marco Antonio	Singh, Neeraj
Filali-Amine, Mamoun	Titolo, Laura
Kobayashi, Tsutomu	Tounsi, Mohamed
Küster Filipe Bowles, Juliana	Völlinger, Kim
Laleau, Regine	Wu, Hao
Leuschel, Michael	Xu, Xiong
MacConville, Dara	Yang, Tengshun
Mallet, Frederic	

Contents

Invited Papers

Refinements of Hybrid Dynamical Systems Logic	3
<i>André Platzer</i>	
Using Deep Ontologies in Formal Software Engineering	15
<i>Achim D. Brucker, Idir Ait-Sadoune, Nicolas Méric, and Burkhart Wolff</i>	

Selected Papers for Presentation and Publication

Pattern-Based Refinement Generation Through Domain Specific Languages	35
<i>Elie Fares, Paul Jean Bodeveix, and Mamoun Filali</i>	
Introducing Inductive Construction in B with the Theory Plugin	43
<i>Julien Cervelle and Frédéric Gervais</i>	
Validation of Formal Models by Interactive Simulation	59
<i>Fabian Vu and Michael Leuschel</i>	
Thread-Local, Step-Local Proof Obligations for Refinement of State-Based Concurrent Systems	70
<i>Gerhard Schellhorn, Stefan Bodenmüller, and Wolfgang Reif</i>	
Encoding TLA ⁺ Proof Obligations Safely for SMT	88
<i>Rosalie Defourné</i>	
Modeling the MVM-Adapt System by Compositional I/O Abstract State Machines	107
<i>Silvia Bonfanti, Elvinia Riccobene, Davide Santandrea, and Patrizia Scandurra</i>	
Crucible Tools for Test Generation and Animation of Alloy Models	116
<i>Thomas Wilson and Stuart Matthews</i>	
Modelling an Automotive Software System with TASTD	124
<i>Diego de Azevedo Oliveira and Marc Frappier</i>	
TASTD: A Real-Time Extension for ASTD	142
<i>Diego de Azevedo Oliveira and Marc Frappier</i>	

Validation by Abstraction and Refinement	160
<i>Sebastian Stock, Fabian Vu, David Geleßus, Michael Leuschel, Atif Mashkoor, and Alexander Egyed</i>	
Verifying Event-B Hybrid Models Using Cyclone	179
<i>Hao Wu and Zheng Cheng</i>	
Exploration of Reflective ASMs for Security	185
<i>Linjie Tong, Ke Xu, Jiarun Hu, Flavio Ferrarotti, and Klaus-Dieter Schewe</i>	
Standalone Event-B Models Analysis Relying on the EB4EB Meta-theory	193
<i>P. Rivière, N. K. Singh, Y. Ait-Ameur, and G. Dupont</i>	
Adding Records to Alloy	212
<i>Julien Brunel, David Chemouil, Alcino Cunha, and Nuno Macedo</i>	
Designing Critical Systems Using Hierarchical STPA and Event-B	220
<i>Asieh Salehi Fathabadi, Colin Snook, Dana Dghaym, Thai Son Hoang, Fahad Alotaibi, and Michael Butler</i>	
Behavioural Theory of Reflective Algorithms	238
<i>Flavio Ferrarotti and Klaus-Dieter Schewe</i>	
Building Specifications in the Event-B Institution: A Summary	245
<i>Marie Farrell, Rosemary Monahan, and James F. Power</i>	
Verifying Temporal Relational Models with Pardinus	254
<i>Nuno Macedo, Julien Brunel, David Chemouil, and Alcino Cunha</i>	
The ABZ 2023 Case Study	
AMAN Case Study	265
<i>Philippe Palanque and José Creissac Campos</i>	
Modeling and Analysis of a Safety-Critical Interactive System Through Validation Obligations	284
<i>David Geleßus, Sebastian Stock, Fabian Vu, Michael Leuschel, and Atif Mashkoor</i>	
Task Model Design and Analysis with Alloy	303
<i>Alcino Cunha, Nuno Macedo, and Eunsuk Kang</i>	
Modeling and Verifying an Arrival Manager Using EVENT- B	321
<i>Amel Mammar and Michael Leuschel</i>	

*formal MVC: A Pattern for the Integration of ASM Specifications in UI
Development* 340
Andrea Bombarda, Silvia Bonfanti, and Angelo Gargantini

Doctoral Symposium

Exploring a Methodology for Formal Verification of Safety-Critical
Systems 361
Oisín Sheridan

Extending Modelchecking with ProB to Floating-Point Numbers
and Hybrid Systems 366
Kristin Rutenkolk

A Framework for Formal Verification and Validation of Railway Systems 371
Yannis Benabbi

Reconstruction of TLAPS Proofs Solved by VeriT in Lambdapi 375
Coltellacci Alessio

Author Index 379