

## 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 subseries at <http://www.springer.com/series/7407>

Alexander Raschke · Dominique Méry (Eds.)

# Rigorous State-Based Methods

8th International Conference, ABZ 2021  
Ulm, Germany, June 9–11, 2021  
Proceedings

*Editors*

Alexander Raschke   
Ulm University  
Ulm, Germany

Dominique Méry   
University of Lorraine  
Vandœuvre-lès-Nancy, France

ISSN 0302-9743 ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-030-77542-1 ISBN 978-3-030-77543-8 (eBook)  
<https://doi.org/10.1007/978-3-030-77543-8>

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

© Springer Nature Switzerland AG 2021

Chapter “Formalizing the Institution for Event-B in the Coq Proof Assistant” is licensed under the terms of the Creative Commons Attribution 4.0 International License (<http://creativecommons.org/licenses/by/4.0/>). For further details see license information in the chapter.

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 2021) is an international forum for the cross-fertilization of related state-based and machine-based formal methods, mainly Abstract State Machines (ASM), Alloy, B, TLA+, VDM, and Z. Rigorous state-based methods share a common conceptual foundation and are widely used in both academia and industry for the design and analysis of hardware and software systems.

The name 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 conference, ABZ 2010, 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 in the conference series (but not in the title); and ABZ 2014 was held in Toulouse, France, which brought the inclusion of the TLA+ community. Lastly, ABZ 2016 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.

In 2020, the ABZ conference should have been held in Ulm, Germany. Unfortunately, the conference had to be cancelled at short notice due to the worldwide rampant COVID-19 virus and was postponed to this year, with the hope of welcoming all participants personally in Ulm. Unfortunately this hope did not come true, so we had to organize the conference as a virtual event after all. Since the proceedings were ready before the cancellation of the 2020 conference, we decided to publish them immediately. We also launched a new call for papers for ABZ 2021 so that researchers had the opportunity to publish new results in a timely manner.

Because the ABZ conference is normally hosted every two years we had not defined a new case study, and with the restrictions of the pandemic and the associated increased efforts, for example for teaching, being felt in the research community, significantly fewer papers were submitted to ABZ 2021. There were 15 papers submitted from authors in 8 countries spread over Europe, Asia, and America. Fortunately, the submitted papers were of very high quality, so that the four reviews per paper were consistently positive and only one paper had to be rejected. A total of 6 full research papers and 8 short research papers were accepted. All accepted papers cover broad research areas on theoretical, systems, or practical aspects of state-based methods.

The doctoral symposium, which was organized for the first time in 2020, also took place in 2021. Three PhD students submitted a four-page abstract describing their research projects and received constructive feedback from the senior researchers of the ABZ community. Each of the submitted abstracts was also evaluated by a separate Program Committee.

The conference was due to be held during June 9–11, 2021, in Ulm, Germany, but unfortunately the successes of the COVID-19 vaccination program will probably not be seen for several months, so the conference was held virtually. In addition to the new submissions, the authors of ABZ 2020 were also invited to present their papers, which fortunately many took advantage of and thus a comprehensive program could be put together.

Unfortunately, due to consequences of the COVID-19 crisis in the personal environment, one of the keynote speakers understandably had to cancel at short notice. However, we were all the more pleased to listen to the keynotes of Ana Cavalcanti, University of York, UK, on “RoStar technology — a roboticist’s toolbox for combined proof and sound simulation” and Gilles Dowek, Inria/ENS Paris-Saclay, France, on “Sharing proofs across logics and systems: a boost for formal methods?”

The EasyChair conference management system was set up for ABZ 2021, supporting submissions and the review process.

We would like to thank all the authors who submitted their work to ABZ 2021. We are grateful to the Program Committee members for their high-quality reviews and discussions. Finally, we wish to thank the Organizing Committee members for their continuous support.

We hope the vaccination program will also reach poor countries as fast as possible such that the COVID-19 crisis will decrease within the next two years and we can meet together in person at ABZ 2023 in France.

For readers of these proceedings, we hope these papers are interesting and they inspire ideas for future research that can be presented at the next ABZ!

April 2021

Alexander Raschke  
Dominique Méry

# Organization

## General Chairs

Alexander Raschke  
Dominique Méry

Ulm University, Germany  
Université de Lorraine, LORIA, France

## Program Committee

Yamine Ait Ameur  
Paolo Arcaini  
Richard Banach  
Egon Boerger  
Eerke Boiten  
Michael Butler  
Andrew Butterfield  
David Deharbe  
Juergen Dingel  
Flavio Ferrarotti  
Mamoun Filali-Amine  
Marc Frappier  
Angelo Gargantini  
Vincenzo Gervasi  
Gudmund Grov

IRIT/INPT-ENSEEIHT, France  
National Institute of Informatics, Japan  
University of Manchester, UK  
Università di Pisa, Italy  
De Montfort University, UK  
University of Southampton, UK  
Trinity College Dublin, Ireland  
ClearSy System Engineering, France  
Queen's University, Canada  
Software Competence Centre Hagenberg, Austria  
IRIT, France  
Université de Sherbrooke, Canada  
University of Bergamo, Italy  
University of Pisa, Italy  
Norwegian Defence Research Establishment (FFI),  
Norway

Stefan Hallerstedt  
Klaus Havelund  
Ian J. Hayes  
Thai Son Hoang  
Frank Houdek  
Alexei Iliasov  
Felix Kossak  
Regine Laleau  
Thierry Lecomte  
Michael Leuschel  
Alexei Lisitsa  
Atif Mashkoor  
Jackson Mayo  
Stephan Merz  
Stefan Mitsch  
Rosemary Monahan  
Mohamed Mosbah  
Cesar Munoz

Aarhus University, Denmark  
Jet Propulsion Laboratory, USA  
The University of Queensland, Australia  
University of Southampton, UK  
Daimler AG, Germany  
Newcastle University, UK  
Software Competence Center Hagenberg, Austria  
Paris-Est Créteil University, France  
ClearSy, France  
University of Düsseldorf, Germany  
University of Liverpool, UK  
Johannes Kepler University, Austria  
Sandia National Laboratories, USA  
Inria Nancy, France  
Carnegie Mellon University, USA  
Maynooth University, Ireland  
University of Bordeaux, France  
NASA, USA

Shin Nakajima	National Institute of Informatics, Japan
Uwe Nestmann	TU Berlin, Germany
Jose Oliveira	University of Minho, Portugal
Philipp Paulweber	Vienna University of Technology, Austria
Luigia Petre	Åbo Akademi University, Finland
Andreas Prinz	University of Agder, Norway
Shengchao Qin	Teesside University, UK
Philippe Queinnec	Université de Toulouse, France
Elvinia Riccobene	University of Milan, Italy
Victor Rivera	Australian National University, Australia
Thomas Santen	TU Berlin, Germany
Patrizia Scandurra	University of Bergamo, Italy
Gerhard Schellhorn	Universitaet Augsburg, Germany
Klaus-Dieter Schewe	Zhejiang University, China
Steve Schneider	University of Surrey, UK
Jun Sun	Singapore Management University, Singapore
Maurice H. ter Beek	ISTI-CNR, Italy
Laurent Voisin	Systerel, France
Virginie Wiels	ONERA/DTIM, France
Uwe Zdun	University of Vienna, Austria
Wolf Zimmermann	Martin Luther University Halle-Wittenberg, Germany



# Contents

## Regular Research Articles

Unbounded Barrier-Synchronized Concurrent ASMs for Effective MapReduce Processing on Streams . . . . .	3
<i>Zilinghan Li, Shilan He, Yiqing Du, Senén González, and Klaus-Dieter Schewe</i>	
Towards ASM-Based Automated Formal Verification of Security Protocols . . . . .	17
<i>Chiara Braghin, Mario Lilli, and Elvinia Riccobene</i>	
Verifying System-Level Security of a Smart Ballot Box. . . . .	34
<i>Dana Dghaym, Thai Son Hoang, Michael Butler, Runshan Hu, Leonardo Aniello, and Vladimiro Sassone</i>	
Proving the Safety of a Sliding Window Protocol with Event-B . . . . .	50
<i>Sophie Coudert</i>	
Event-B Formalization of Event-B Contexts . . . . .	66
<i>Jean-Paul Bodeveix and Mamoun Filali</i>	
Validation of Formal Models by Timed Probabilistic Simulation. . . . .	81
<i>Fabian Vu, Michael Leuschel, and Atif Mashkoor</i>	

## Short Articles

Sterling: A Web-Based Visualizer for Relational Modeling Languages. . . . .	99
<i>Tristan Dyer and John Baugh</i>	
Extending ASMETA with Time Features . . . . .	105
<i>Andrea Bombarda, Silvia Bonfanti, Angelo Gargantini, and Elvinia Riccobene</i>	
About the Concolic Execution and Symbolic ASM Function Promotion in CASM. . . . .	112
<i>Philipp Paulweber, Jakob Moosbrugger, and Uwe Zdun</i>	
Towards Refinement of Unbounded Parallelism in ASMs Using Concurrency and Reflection . . . . .	118
<i>Fengqing Jiang, Neng Xiong, Xinyu Lian, Senén González, and Klaus-Dieter Schewe</i>	

<b>The CamilleX Framework for the Rodin Platform . . . . .</b>	<b>124</b>
<i>Thai Son Hoang, Colin Snook, Dana Dghaym, Asieh Salehi Fathabadi, and Michael Butler</i>	
<b>Extensible Record Structures in Event-B . . . . .</b>	<b>130</b>
<i>Asieh Salehi Fathabadi, Colin Snook, Thai Son Hoang, Dana Dghaym, and Michael Butler</i>	
<b>Formalizing and Analyzing System Requirements of Automatic Train Operation over ETCS Using Event-B . . . . .</b>	<b>137</b>
<i>Robert Eschbach</i>	
<b>Automatic Transformation of SysML Model to Event-B Model for Railway CCS Application. . . . .</b>	<b>143</b>
<i>Shubhangi Salunkhe, Randolph Berglehner, and Abdul Rasheeq</i>	
<b>Short Articles of the PhD-Symposium (Work in Progress)</b>	
<b>Formal Meta Engineering Event-B: Extension and Reasoning The EB4EB Framework . . . . .</b>	<b>153</b>
<i>Peter Riviere</i>	
<b>A Modeling and Verification Framework for Security Protocols . . . . .</b>	<b>158</b>
<i>Mario Lilli</i>	
<b>Formalizing the Institution for Event-B in the Coq Proof Assistant . . . . .</b>	<b>162</b>
<i>Conor Reynolds</i>	
<b>Author Index . . . . .</b>	<b>167</b>