More information about this series at http://www.springer.com/series/7407
Abstract State Machines, Alloy, B, TLA, VDM, and Z
6th International Conference, ABZ 2018
Southampton, UK, June 5–8, 2018
Proceedings
Preface

This volume contains the papers presented at ABZ 2018 (6th International ABZ Conference on ASM, Alloy, B, TLA, VDM, and Z) held during June 5–8, 2018, in Southampton, UK. This conference records the latest research developments in state-based formal methods, abstract state machines, Alloy, B, Circus, Event-B, TLS+, VDM, and Z. The 2018 edition followed the success of the previous ABZ conferences in London, UK (2008), Orford, Canada (2010), Pisa, Italy (2012), Toulouse, France (2014), and Linz, Austria (2016).

Four keynotes were presented at ABZ 2018. Janet Barnes and Angela Wallenburg from Altran, UK, jointly gave a talk on making the use of formal methods mainstream within industrial practice and outlined some of the successes and challenges for Altran in using formal methods. Klaus-Dieter Schewe from the Software Competence Centre Hagenberg, Austria, gave a talk on a formal characterization of adaptive distributed systems based on concurrent reflective abstract state machines. Daniel Jackson from MIT gave a talk that argued for the importance of good design in software development. Jean-Raymond Abrial gave a talk that reflected on principles, successes, and challenges around the development and deployment of B and Event-B. We are grateful to the invited speakers for contributing to the success of ABZ 2018.

ABZ 2018 coincided with the 25th anniversary of the first major industrial use of the B Method on METEOR, a railway project for the Paris Metro Line 14, which commenced in 1993. In recognition of this, we organized a panel session at ABZ 2018, with assistance from Laurent Voisin of Systerel, to discuss the evolution of the industrial use of the B Method since 1993.

As successfully practiced at ABZ 2014 and ABZ 2016, the 6th edition of ABZ included special sessions dedicated to a shared real-life case study. The objective of this is to provide points of comparison between ABZ methods and to enrich the set of case studies developed with the methods using a practical and real-life system. This time the case study organizers, Thai Son Hoang and Klaus Reichl, defined a case study from the railway domain with challenging safety requirements. The ABZ 2018 case study is based on the Hybrid ERTMS/ETCS Level 3 standard. These proceedings include an overview of the case study as well as several accepted papers outlining solutions to the case study.

ABZ 2018 received 60 submissions covering a range of formal methods within the scope of the conference. These papers ranged from fundamental contributions, applications in practical contexts, tool developments, and contributions to the case study. Each paper was reviewed by four reviewers and the Program Committee accepted 13 regular research papers, seven papers on the Hybrid ERTMS case study, and 11 short papers presenting work in progress.

We would like to thank the Program Committee members and the external reviewers who carefully reviewed all submissions and selected the best contributions. This event would not exist if authors did not submit their papers. We extend our thanks to all the
people who contributed to the success of ABZ 2018 – reviewers, authors, invited speakers, panelists, Program Committee members, and local organizers. We also thank EasyChair for providing a powerful platform for managing the submissions, reviews, decisions, and proceedings production.

April 2018

Michael Butler
Alexander Raschke
Thai Son Hoang
Klaus Reichl
Organization

Program Committee

Yamine Ait Ameur  IRIT/INPT-ENSEEIHT, Toulouse, France
Paolo Arcaini  National Institute of Informatics, Japan
Richard Banach  The University of Manchester, UK
Egon Boerger  Università di Pisa, Italy
Eerke Boiten  De Montfort University, Leicester, UK
Michael Butler  University of Southampton, UK
Marcel Dausend  e.solutions GmbH, Germany
David Deharbe  Clearsy, France
John Derrick  University of Sheffield, UK
Juergen Dingel  Queen’s University, Canada
Roozbeh Farahbod  Huawei Technologies, Germany
Flavio Ferrarotti  Software Competence Centre Hagenberg, Austria
Mamoun Filali-Amine  IRIT, Toulouse, France
Marc Frappier  Université de Sherbrooke, Canada
Leo Freitas  Newcastle University, UK
Angelo Gargantini  University of Bergamo, Italy
Vincenzo Gervasi  University of Pisa, Italy
Uwe Glässer  Simon Fraser University, Canada
Gudmund Grov  Norwegian Defence Research Establishment, Norway
Lindsay Groves  Victoria University of Wellington, New Zealand
Stefan Hallerstede  Aarhus University, Denmark
Klaus Havelund  Jet Propulsion Laboratory, USA
Ian J. Hayes  The University of Queensland, Australia
Rob Hierons  Brunel University, UK
Thai Son Hoang  University of Southampton, UK
Jeremy Jacob  University of York, UK
Regine Laleau  Paris Est Creteil University, France
Peter Gorm Larsen  Aarhus University, Denmark
Thierry Lecomte  ClearSy, France
Michael Leuschel  University of Düsseldorf, Germany
Zhiming Liu  Southwest University, China
Tiziana Margaria  Lero, University of Limerick, Ireland
Atif Mashkoor  Software Competence Centre Hagenberg, Austria
Jackson Mayo  Sandia National Laboratories, USA
Dominique Mery  Université de Lorraine, LORIA, France
Stephan Merz  Inria Nancy, France
Mohamed Mosbah  LaBRI - University of Bordeaux, France
Cesar Munoz  NASA, USA
Uwe Nestmann | TU Berlin, Germany
Jose Oliveira | University of Minho, Portugal
Luigia Petre | Åbo Akademi University, Finland
Andreas Prinz | University of Agder, Norway
Philippe Queinnec | IRIT - Université de Toulouse, France
Alexander Raschke | University of Ulm, Germany
Klaus Reichl | Thales Austria GmbH, Austria
Elvinia Riccobene | University of Milan, Italy
Thomas Rodeheffer | Google, USA
Alexander Romanovsky | Newcastle University, UK
Thomas Santen | TU Berlin, Germany
Patrizia Scandurra | DIIMM - University of Bergamo, Italy
Gerhard Schellhorn | Universitaet Augsburg, Germany
Klaus-Dieter Schewe | Software Competence Center Hagenberg, Austria
Steve Schneider | University of Surrey, UK
Colin Snook | University of Southampton, UK
Michael Stegmaier | University of Ulm, Germany
Jing Sun | The University of Auckland, New Zealand
Loredana Tec | Software Competence Centre Hagenberg, Austria
Laurent Voisin | Systerel, France
Qing Wang | ANU, Australia
Virginie Wiels | ONERA/DTIM, France
Kirsten Winter | The University of Queensland, Australia
Frank Zeyda | University of York, UK

Additional Reviewers

Bacis, Enrico | Knapp, Alexander
Bodenmüller, Stefan | Krings, Sebastian
Bonfanti, Silvia | Mammar, Amel
Boussabbeh, Maha | Pei, Yu
Cunha, Alcino | Stankaitis, Paulius
González, Senén | Tayebi, Mohammad
Götz, Stefan | Thirioux, Xavier
Hallerstede, Stefan | Tounsi, Mohamed
Haneberg, Dominik | Tueno Fotso, Steve Jeffrey
Hansen, Dominik | Wildman, Luke
Iliasov, Alexei | Yaghoubi Shahir, Amir
Kanakis, Georgios | Zohrevand, Zahra
How Bugs Led Us Astray
(Abstract of Invited Talk)

Daniel Jackson
MIT

Abstract. When the field of formal methods began, it had broad and noble goals. But somehow, over time, these goals were eclipsed by a more reductionist view. Nowadays, quality is measured by defect counts, and eliminating bugs has become the central focus of our field. In this talk, I’ll explain how I think this came about, why it’s insidious, and what we can do about it.

My key observation will be that bugs are not the causes of problems but are instead symptoms. To improve our software—to make it more secure, safe and usable—we need to move from symptoms to diagnosis, to determine the underlying causes of poor software and fix those. I will argue that design is essential to achieving this, and that we need to reinvigorate design as a central activity in formal methods research and practice. I will give examples of designs, good and bad, drawn from my ongoing work on conceptual design of software.
Contents

Invited Talks

ABZ Languages and Tools in Industrial-Scale Application . . . . . . . . . . . . . . 3
Janet Barnes, Jonathan Hammond, Angela Wallenburg,
and Thomas Wilson

Distributed Adaptive Systems: Theory, Specification, Reasoning . . . . . . . . . . . 16
Klaus-Dieter Schewe, Flavio Ferrarotti, Loredana Tec,
and Qing Wang

On B and Event-B: Principles, Success and Challenges . . . . . . . . . . . . . . . . 31
Jean-Raymond Abrial

Translation and Transformation

CASM-IR: Uniform ASM-Based Intermediate Representation
for Model Specification, Execution, and Transformation. . . . . . . . . . . . . . . . 39
Philipp Paulweber, Emmanuel Pescosta, and Uwe Zdun

Event-B Expression and Verification of Translation Rules Between
SysML/KAOS Domain Models and B System Specifications . . . . . . . . . . . . . 55
Steve Jeffrey Tueno Fotso, Amel Mammar, Régine Laleau,
and Marc Frappier

A Translation from Alloy to B . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 71
Sebastian Krings, Joshua Schmidt, Carola Brings, Marc Frappier,
and Michael Leuschel

Analysis and Tests

Extracting Symbolic Transitions from TLA⁺ Specifications . . . . . . . . . . . . . . 89
Jure Kukovec, Thanh-Hai Tran, and Igor Konnov

Systematic Generation of Non-equivalent Expressions
for Relational Algebra . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 105
Kaiyuan Wang, Allison Sullivan, Manos Kourkoutos, Darko Marinov,
and Sarfraz Khurshid

Solver-Based Sketching of Alloy Models Using Test Valuations . . . . . . . . . . . 121
Kaiyuan Wang, Allison Sullivan, Darko Marinov, and Sarfraz Khurshid
## Contents

### Reals and Hybrid Systems

- Abstract State Machines with Exact Real Arithmetic .................................................. 139
  - Christoph Beierle and Klaus-Dieter Schewe
- Proof-Based Approach to Hybrid Systems Development: Dynamic Logic and Event-B .................................................. 155
  - Guillaume Dupont, Yamine Aït-Ameur, Marc Pantel, and Neeraj Kumar Singh
- Issues in Automated Urban Train Control: ‘Tackling’ the Rugby Club Problem .................. 171
  - Richard Banach

### Refinement

- Clarification of Ambiguity for the Simple Authentication and Security Layer .................................................. 189
  - Farah Al-Shareefi, Alexei Lisitsa, and Clare Dixon
- Systematic Refinement of Abstract State Machines with Higher-Order Logic .................................................. 204
  - Flavio Ferrarotti, Senén González, Klaus-Dieter Schewe, and José María Turull-Torres
- Refinement of Timing Constraints for Concurrent Tasks with Scheduling .......................... 219
  - Chenyang Zhu, Michael Butler, and Corina Cirstea
- Verifiable Code Generation from Scheduled Event-B Models .................................................. 234
  - Mohammadsadegh Dalvandi, Michael Butler, Abdolbaghi Reza Zadeh, and Asieh Salehi Fathabadi

### Hybrid ERTMS Case Study

- The Hybrid ERTMS/ETCS Level 3 Case Study .................................................. 251
  - Thai Son Hoang, Michael Butler, and Klaus Reichl
- Modeling the Hybrid ERTMS/ETCS Level 3 Standard Using a Formal Requirements Engineering Approach .................................................. 262
  - Steve Jeffrey Tueno Fotso, Marc Frappier, Régine Laleau, and Amel Mammar
- Modelling the Hybrid ERTMS/ETCS Level 3 Case Study in SPIN .................................................. 277
  - Paolo Arcaini, Pavel Ježek, and Jan Kofířoň
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using a Formal B Model at Runtime in a Demonstration of the ETCS</td>
<td>292</td>
</tr>
<tr>
<td>Hybrid Level 3 Concept with Real Trains</td>
<td></td>
</tr>
<tr>
<td>Dominik Hansen, Michael Leuschel, David Schneider, Sebastian Krings,</td>
<td></td>
</tr>
<tr>
<td>Philipp Körner, Thomas Naulin, Nader Nayeri, and Frank Skowron</td>
<td></td>
</tr>
<tr>
<td>Validating the Hybrid ERTMS/ETCS Level 3 Concept with Electrum</td>
<td>307</td>
</tr>
<tr>
<td>Alcino Cunha and Nuno Macedo</td>
<td></td>
</tr>
<tr>
<td>The ABZ-2018 Case Study with Event-B</td>
<td>322</td>
</tr>
<tr>
<td>Jean-Raymond Abrial</td>
<td></td>
</tr>
<tr>
<td>Diagram-Led Formal Modelling Using iUML-B for Hybrid ERTMS Level 3</td>
<td>338</td>
</tr>
<tr>
<td>Dana Dghaym, Michael Poppleton, and Colin Snook</td>
<td></td>
</tr>
<tr>
<td>An EVENT-B Model of the Hybrid ERTMS/ETCS Level 3 Standard</td>
<td>353</td>
</tr>
<tr>
<td>Amel Mammar, Marc Frappier, Steve Jeffrey Tueno Fotso, and Réjane Laleau</td>
<td></td>
</tr>
<tr>
<td>Short Papers</td>
<td></td>
</tr>
<tr>
<td>AsmetaA: Animator for Abstract State Machines</td>
<td>369</td>
</tr>
<tr>
<td>Silvia Bonfanti, Angelo Gargantini, and Atif Mashkoor</td>
<td></td>
</tr>
<tr>
<td>Formal Specification of the Semantics of Control State Diagrams</td>
<td>374</td>
</tr>
<tr>
<td>Markus Leitz and Alexander Raschke</td>
<td></td>
</tr>
<tr>
<td>Capturing Membrane Computing by ASMs</td>
<td>380</td>
</tr>
<tr>
<td>Klaus-Dieter Schewe, Loredana Tec, and Qing Wang</td>
<td></td>
</tr>
<tr>
<td>Towards Creating a DSL Facilitating Modelling of Dynamic Access</td>
<td>386</td>
</tr>
<tr>
<td>Control in Event-B</td>
<td></td>
</tr>
<tr>
<td>Inna Vistbakka, Mikhail Barash, and Elena Troubitsyna</td>
<td></td>
</tr>
<tr>
<td>State-Based Formal Methods in Scientific Computation</td>
<td>392</td>
</tr>
<tr>
<td>John Baugh and Tristan Dyer</td>
<td></td>
</tr>
<tr>
<td>Proposition of an Action Layer for Electrum</td>
<td>397</td>
</tr>
<tr>
<td>Julien Brunel, David Chemouil, Alcino Cunha, Thomas Hujsa, Nuno Macedo, and Jeanne Tawa</td>
<td></td>
</tr>
<tr>
<td>Insulin Pump: Modular Modeling of Hybrid Systems Using Event-B</td>
<td></td>
</tr>
<tr>
<td>Wen Su, Jinxin Chen, and Shehroz Khan</td>
<td></td>
</tr>
<tr>
<td>An Automation-Friendly Set Theory for the B Method</td>
<td>409</td>
</tr>
<tr>
<td>Guillaume Bury, Simon Cruanes, David Delahaye, and Pierre-Louis Euvrard</td>
<td></td>
</tr>
</tbody>
</table>
Teaching an Old Dog New Tricks: The Drudges of the Interactive Prover in Atelier B ......................................................... 415
   Lilian Burdy and David Deharbe

Modelling Dynamic Data Structures with the B Method. ................. 420
   Frédéric Badeau, Vincent Lacroix, Vincent Monfort, Laurent Voisin,
   and Christophe Métayer

On the Importance of Explicit Domain Modelling in Refinement-Based Modelling Design. Experiments with Event-B. .................. 425
   Yamine Aït-Ameur, Idir Ait-Sadoune, P. Casteran, Paul Gibson,
   K. Hacid, S. Kherroubi, Dominique Méry, L. Mohand-Oussaid,
   Neeraj K. Singh, and Laurent Voisin

Author Index ........................................................................ 431