Industrial Deployment of System Engineering Methods
Alexander Romanovsky • Martyn Thomas
Editors

Industrial Deployment of System Engineering Methods
Foreword

This book is a splendid condensed record of the DEPLOY project, epitomising a reflective and informed approach to the industrial use of formal methods in software development. The project plan was to introduce a formal method—Event-B—into a handful of industrial organisations working in different application domains; its larger aim was to learn lessons from the experience. There would be technical and managerial lessons: lessons for the industrial partners, for the academic and research partners, and for the builders of tools to support the selected method. In this larger aim the project succeeded brilliantly, and the book contains an honest and insightful account of what has been learned.

For the academic and research partners and the tool vendors, necessary improvements in the formal method and its supporting tools were identified; some have already been implemented in the course of the project. For the industrial partners, much has been learned about the value of formal methods in general and of Event-B in particular, and the match—or mismatch—with specific complexities of the systems they build and with their established development techniques. All the participants have acquired a stronger understanding of the roles of formal methods in developing dependable systems.

The industrial applications included automotive, space, railway and business systems, and even the development of an instruction set architecture for an industrial microprocessor. The varied complexities of their system functionalities, and the heterogeneous nature of their problem worlds demanded a rich variety of development processes and of concepts and techniques to be used at each development stage. A formal method cannot be the main engine of the development process. It must be applied more locally within an essentially non-formal structure. Its vital contribution is to improve system dependability by motivating formalisation where it is useful, and then by mathematically rigorous analysis and proof. Many development artifacts, formalised in a sufficiently expressive language, can be analysed to detect inconsistency, failure to satisfy known formal specifications, and other errors. Other development artifacts, most conspicuously those closely associated with the discovery, design and expression of system requirements, spring from inherently non-formal investigations and decisions, and may not admit of useful formalisation.
Their importance lies in the conceptual infrastructure they provide for other more formal artifacts.

The contributors to the book have provided an impressive wealth of detail. They report efforts on pilot projects, the results obtained, and their considered judgement of their experiences. They describe their difficulties and failures with honesty, and offer sober evaluations of their successes. The tool builders give a careful account of their responses to requests for new and improved features. Deficiencies in the method and its supporting tools are frankly discussed, as is the work that was put in hand to remedy them. Quantitative evaluations are given where appropriate, and qualitative evaluation is not spurned where it is more suitable. Managerial and organisational challenges are discussed. The software tools supporting Event-B are described, along with enhancements and extensions motivated by the needs of the industrial partners. There is a concise introduction to Event-B and its conceptual basis.

In short, this book describes a project that has made a major contribution towards bridging the gap between formalists and practitioners in software development for dependable systems. The detailed substance of the contribution lies in the specifics of what has been done; but the full value lies even more in the cooperative way in which the project has been carried out and the open-minded acknowledgement of challenges. This book will amply repay a careful and thoughtful reading by researchers and practitioners alike.

London, UK

June 2012

Michael Jackson
Preface

This book is about experience gained and lessons learnt in the course of a major European project on industrial deployment of formal methods. The DEPLOY Integrated Project ran for 4 years and involved 15 partners from academia and industry. The editors came to the project from different backgrounds and with different motivations. Sascha (Alexander) Romanovsky has been working on system dependability and fault tolerance for many years and has always stressed the importance of reasoning about faults and fault tolerance at the earlier phases of system development. He coordinated the RODIN project, preceding DEPLOY, and became involved in writing the DEPLOY proposal and coordination of DEPLOY to see the tools and methods originated in RODIN further advanced and applied in wide industrial settings. Martyn Thomas is an industrialist who has been concerned with safety-critical and other high-dependence computer systems since the 1980s, and who came to DEPLOY eager to understand the barriers to greater use of science-based software engineering in industry. The reader will see in Chapter 15 what we have learnt through DEPLOY and through editing this book, and where we believe the field now stands. It is enough to say here that we have both learnt a lot, and to acknowledge that the success of DEPLOY and the insight that this book contains are the result of the talents, good-humoured collaboration and very hard work of the whole project. We therefore thank Zoe Andrews (Newcastle University), Frédéric Badeau (Systerel), Iulia Banu, Tudor Balanescu (University of Pitesti), David Basin (ETH Zurich), Nicolas Beauger (Systerel), Jens Bendiposto (University of Düsseldorf), Karim Berkani (Siemens), Emmanuel Billaud (Systerel), Pontus Bostrom (Åbo Akademi University), Jeremy Bryans (Newcastle University), Lilian Burdy (Inria), Michael Butler (University of Southampton), Mathieu Clabaut (Systerel), Kriangsak Damchoom (University of Southampton), Renaud De Landtsheer (CETIC), Fredrik Degerlund (Åbo Akademi University), Jean-Christophe Deprez (CETIC), Denisa Diaconescu, Ionut Dinca (University of Pitesti), Nicolas Dubois, Andy Edmunds (University of Southampton), Nadine Elbeshhausen, Jérôme Falampa (Siemens), Yoann Fages-Tafanelli (Systerel), John Fitzgerald (Newcastle University), Fabian Fritz (University of Düsseldorf), Andreas Fuerst (ETH Zurich), Aurélien Gilles (Consultant), Rainer Gmehlich (Bosch), Radu Gramatovici (Uni-
iversity of Bucharest), Katrin Grau (Bosch), Stefan Hallerstede (Aarhus University), Natasha Hebdige (Newcastle University), Thai Son Hoang (ETH Zurich), Jodi Hossbach (Newcastle University), Alexei Iliasov (Newcastle University), Florentin Ipate (University of Pitești), Michael Jackson (Consultant), Michael Jastram (University of Düsseldorf), Cliff Jones (Newcastle University), Minh-Thang Khuu, Linas Laibinis (Åbo Akademi University), Gwenaël Le Cointre (ClearSy), Hung Le Dang (Siemens), Raluca Lefticaru (University of Pitești), Thierry Lecomte (ClearSy), Eric Lelay (Siemens), Michael Leuschel (University of Düsseldorf), Ioana Leustean (University of Bucharest), Christophe Logerot, Ilya Lopatkin (Newcastle University), Felix Lösch (Bosch), Li Luo, Benoît Lucet (Systerel), Manuel Mazzara (Newcastle University), Larissa Meinicke, Christophe Métayer (Systerel), Arnaud Michot (CETIC), Mikael Mokrani (Siemens), Thomas Muller (Systerel), Louis Mussat (ClearSy), Mats Neovius (Åbo Akademi University), Carine Pascal (Systerel), Luigia Petre (Åbo Akademi University), Daniel Plagge (University of Düsseldorf), Marta Plaska (Åbo Akademi University), Christophe Ponsard (CETIC), Mike Poppleton (University of Southampton), Antoine Requet (ClearSy), Abdolbaghi Rezazadeh (University of Southampton), Sanae Saadaoui (CETIC), Denis Sabatier (ClearSy), Yah Said Mar (University of Southampton), Peter Sandvik, Kaisa Sere (Åbo Akademi University), Matthias Schmalz (ETH Zurich), Renato Silva (University of Southampton), Colin Snook (University of Southampton), Corinna Spermann (University of Düsseldorf), Alin Stefanescu (University of Bucharest), Anton Tarasyuk (Åbo Akademi University), Monica Tataram (University of Bucharest), Elena Troubitsyna (Åbo Akademi University), Cristina Tudose (University of Pitești), Adrian Turcanu, Laurent Voisin (Systerel), Marina Walden (Åbo Akademi University), Jon Warwick (Newcastle University), Ingo Weigelt (University of Düsseldorf) and Sebastian Wieczorek (SAP).

Newcastle upon Tyne, UK
London, UK
May 2012

Alexander Romanovsky
Martyn Thomas
## Contents

1. **Introduction** ................................ 1  
   Alexander Romanovsky and Martyn Thomas

2. **Integrated Project DEPLOY** .......................... 5  
   Alexander Romanovsky

3. **Experience of Deployment in the Automotive Industry**  .......... 13  
   Rainer Gmehl and Cliff Jones

4. **Improving Railway Data Validation with ProB** .............. 27  
   Jérôme Falampin, Hung Le-Dang, Michael Leuschel, Mikael Mokrani,  
   and Daniel Plagge

5. **Deployment in the Space Sector** .......................... 45  
   Dubravka Ilić, Linas Laibinis, Timo Latvala, Elena Troubitsyna, and  
   Kimmo Varpaaniemi

6. **Business Information Sector** ............................. 63  
   Sebastian Wieczorek, Vitaly Kozyura, Wei Wei, Andreas Roth, and  
   Alin Stefanescu

7. **Formal Methods as an Improvement Tool** ................. 81  
   Aryldo G. Russo Jr.

8. **Critical Software Technologies’ Experience with Formal Methods** ...... 97  
   Alex Hill, Jose Reis, and Paulo Carvalho

9. **Experience of Deploying Event-B in Industrial Microprocessor Development** ............. 107  
   Stephen Wright and Kerstin Eder

10. **Industrial Deployment of Formal Methods: Trends and Challenges** .... 123  
    John Fitzgerald, Juan Bicarregui, Peter Gorm Larsen, and Jim Woodcock

11. **Introducing Formal Methods into Existing Industrial Practices** ........ 145  
    Martyn Thomas and Alexander Romanovsky
12 Tooling ........................................ 157
   Michael Butler, Laurent Voisin, and Thomas Muller

13 Technology Transfer ........................................ 187
   David Basin and Thai Son Hoang

14 After and Outside DEPLOY: The DEPLOY Ecosystem ........ 197
   Alexander Romanovsky

15 Industrial Software Engineering and Formal Methods ........ 203
   Martyn Thomas and Alexander Romanovsky

Appendix A An Introduction to the Event-B Modelling Method ........ 211
   Thai Son Hoang

Appendix B Evidence-Based Assistance for the Adoption of Formal
   Methods in Industry ........................................ 237
   Jean-Christophe Deprez, Christophe Ponsard, and Renaud De Landtsheer