Shengchao Qin  Zongyan Qiu (Eds.)

Formal Methods and Software Engineering

13th International Conference on Formal Engineering Methods, ICFEM 2011
Durham, UK, October 26-28, 2011
Proceedings
Preface

Formal engineering methods have been extensively studied over decades. Various theories, techniques, and tools have been proposed, developed, and applied in the specification, design, verification, and validation of software systems or in the construction of such systems. The challenge now is how to integrate them to effectively deal with large-scale and complex systems, e.g., cyber-physical systems, for their sound and efficient construction and maintenance. This requires us to improve the state of the art by researching effective approaches and techniques for integration of formal methods into industrial engineering practice.

The now long-established series of International Conferences on Formal Engineering Methods has provided a forum for those interested in the application of formal methods to computer systems. This volume contains the papers presented at ICFEM 2011, the 13th International Conference on Formal Engineering Methods, held during October 26–28, 2011 in Durham, UK.

There were 103 submissions from 28 countries. Each paper was reviewed by at least three Program Committee members. After extensive discussion, the Program Committee decided to accept 40 papers. The program also included three invited talks by Jifeng He, from East China Normal University, Peter O’Hearn, from Queen Mary, University of London, and Shaz Qadeer, from Microsoft Research. One invited paper and two abstracts are also included here.

ICFEM 2011 was organized mainly by the School of Computing, Teesside University. We acknowledge the financial support from our main sponsors, including Teesside University, Microsoft Research, and Formal Methods Europe. We thank our honorary chairs Cliff Hardcastle and Marc Cavazza for their support and our conference chairs Cliff Jones and Phil Brooke for their hard work during the organization of ICFEM 2011. Special thanks should be given to Angela Ackerley and Mandie Hall for their help on logistics including finance and registration.

We are grateful to all members of the Program Committee and external reviewers for their hard work. We would also like to thank all the authors of the invited and submitted papers, and all the participants of the conference. They are the main focus of the whole event. The EasyChair system was used to manage the submissions, reviewing, and proceedings production. We would like to thank the EasyChair team for a very useful tool.

August 2011

Shengchao Qin
Zongyan Qiu
Organization

Honorary Chairs
Marc Cavazza  Teesside University
Cliff Hardcastle  Teesside University

General Chairs
Phil Brooke  Teesside University
Cliff Jones  Newcastle University

Program Chairs
Shengchao Qin  Teesside University
Zongyan Qiu  Peking University

Program Committee
Bernhard K. Aichernig  TU Graz
Keijiro Araki  Kyushu University
Farhad Arbab  CWI and Leiden University
Richard Banach  University of Manchester
Nikolaj Bjorner  Microsoft Research
Jonathan P. Bowen  Museophile Limited
Michael Butler  University of Southampton
Andrew Butterfield  University of Dublin
Ana Cavalcanti  University of York
Aziem Chawdhary  University of Edinburgh
Wei-Ngan Chin  National University of Singapore
Florin Craciun  National University of Singapore
Thao Dang  VERIMAG
Jim Davies  University of Oxford
Dino Distefano  Queen Mary, University of London
Jin-Song Dong  National University of Singapore
Zhenhua Duan  Xidian University
Colin Fidge  Queensland University of Technology
J.S. Fitzgerald  Newcastle University
Leo Freitas  Newcastle University
Joaquim Gabarro  Universitat Politecnica de Catalunya
Stefania Gnesi  ISTI-CNR
Anthony Hall  Independent Consultant
Ian J. Hayes  
Mike Hinchey  
Zhenjiang Hu  
Michael Jackson  
Thierry Jéron  
Gerwin Klein  
Laura Kovacs  
Kim G. Larsen  
Peter Gorm Larsen  
Michael Leuschel  
Xuandong Li  
Shaoying Liu  
Zhiming Liu  
Tiziana Margaria  
Dominique Mery  
Stephan Merz  
Huaikou Miao  
Peter Müller  
Jun Pang  
Matthew Parkinson  
Geguang Pu  
Shengchao Qin  
Zongyan Qiu  
Augusto Sampaio  
Thomas Santen  
Wuwei Shen  
Marjan Sirjani  
Bill Stoddart  
Jing Sun  
Jun Sun  
Meng Sun  
Kenji Taguchi  
Tetsuo Tamai  
Yih-Kuen Tsay  
T.H. Tse  
Viktor Vafeiadis  
Miroslav Velev  
Laurent Voisin  
Hai H. Wang  
Ji Wang  
Linzhang Wang  
Heike Wehrheim  
Jim Woodcock  
Hongli Yang  
Wang Yi  

University of Queensland  
Lero  
NII  
Independent Consultant  
Inria Rennes - Bretagne Atlantique  
NICTA and UNSW  
TU Vienna  
Aalborg University  
Aarhus School of Engineering  
University of Düsseldorf  
Nanjing University  
Hosei University  
UNU/IIST  
University of Potsdam  
Université Henri Poincaré Nancy 1 and LORIA  
INRIA Lorraine  
Shanghai University  
ETH Zurich  
University of Luxembourg  
Microsoft Research  
East China Normal University  
Teesside University  
Peking University  
Federal University of Pernambuco  
European Microsoft Innovation Center  
Western Michigan University  
Reykjavik University  
Teesside University  
The University of Auckland  
Singapore University of Technology and Design  
Peking University  
AIST  
University of Tokyo  
National Taiwan University  
The University of Hong Kong  
MPI-SWS  
Aries Design Automation  
Systerel  
University of Aston  
NUTD  
Nanjing University  
University of Paderborn  
University of York  
Beijing University of Technology  
Uppsala University
<table>
<thead>
<tr>
<th>Name</th>
<th>Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Naijun Zhan</td>
<td>Institute of Software, Chinese Academy of Sciences</td>
</tr>
<tr>
<td>Jian Zhang</td>
<td>Institute of Software, Chinese Academy of Sciences</td>
</tr>
<tr>
<td>Hong Zhu</td>
<td>Oxford Brookes University</td>
</tr>
<tr>
<td>Huibiao Zhu</td>
<td>East China Normal University</td>
</tr>
</tbody>
</table>

**Publicity Chairs**

<table>
<thead>
<tr>
<th>Name</th>
<th>Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jonathan P. Bowen</td>
<td>Museophile Limited</td>
</tr>
<tr>
<td>Jun Sun</td>
<td>Singapore University of Technology and Design</td>
</tr>
<tr>
<td>Huibiao Zhu</td>
<td>East China Normal University</td>
</tr>
</tbody>
</table>

**Local Organization Committee**

<table>
<thead>
<tr>
<th>Name</th>
<th>Institution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Angela Ackerley</td>
<td>Teesside University</td>
</tr>
<tr>
<td>Phil Brooke</td>
<td>Teesside University</td>
</tr>
<tr>
<td>Steve Dunne</td>
<td>Teesside University</td>
</tr>
<tr>
<td>Mandie Hall</td>
<td>Teesside University</td>
</tr>
<tr>
<td>Shengchao Qin</td>
<td>Teesside University</td>
</tr>
</tbody>
</table>

**Steering Committee**

- Keijiro Araki, Japan
- Jin Song Dong, Singapore
- Chris George, Canada
- Jifeng He, China
- Mike Hinchey, Ireland
- Shaoying Liu (Chair), Japan
- John McDermid, UK
- Tetsuo Tamai, Japan
- Jim Woodcock, UK

**Sponsors**

- Formal Methods Europe (FME)
- Microsoft Research Limited
- Teesside University
Additional Reviewers
Aboulsamh, Mohammed
Andriamiarina, Manamiary Bruno
Andronick, June
Anh Tuan, Luu
Bauer, Sebastian
Bertolini, Cristiano
Bertrand, Nathalie
Besova, Galina
Blanchette, Jasmin Christian
Bodeveix, Jean-Paul
Bu, Lei
Carmona, Josep
Chen, Chunqing
Chen, Liqian
Chen, Xin
Chen, Zhenbang
Colley, John
Cong-Vinh, Phan
Cos, Andreea Costea
Costea, Andreea
Daum, Matthias
Dongol, Brijesh
Du, Yuyue
Edmunds, Andrew
Falcone, Ylies
Ferrari, Alessio
Ferreira, Joao F.
Gao, Ping
Gherghina, Cristian
Gotsman, Alexey
Greenaway, David
Hallerstedt, Stefan
Hallestede, Stefan
Hayes, Ian
Hayman, Jonathan
He, Guanhua
Heisel, Maritta
Jaghoori, Mohammad Mahdi
Khakpour, Narges
Khamespanah, Ehsan
Kong, Weiqiang
Kreitz, Christoph
Kumazawa, Tsutomu
Kusakabe, Shigeru
Le, Quang Loc
Legay, Axel
Li, Yuan Fang
Liu, Yang
Mazzanti, Franco
Mcneile, Ashley
Meinicke, Larissa
Mochio, Hiroshi
Morisset, Charles
Moscato, Mariano
Nakajima, Shin
Nogueira, Sidney
Nyman, Ulrik
Olsen, Petur
Omori, Yoichi
Orejas, Fernando
Petersen, Rasmus Lerchedahl
Plagge, Daniel
Sabouri, Hamideh
Sewell, Thomas
Singh, Neeraj
Snook, Colin
Song, Songzheng
Stainer, Amelie
Stewart, Alan
Struth, Georg
Tiezzi, Francesco
Timm, Nils
Tounsi, Mohamed
Tsai, Ming-Hsien
Walther, Sven
Wang, Jackie
Wang, Shuling
Wang, Zheng
Welch, James
Wijs, Anton
Wu, Bin
Yamagata, Yoriyuki
Yatsu, Hirokazu
Zhang, Chenyi
Zhang, Pengcheng
Zhao, Yongxin
Zheng, Man Chun
Zheng, Manchun
Zhu, Jiaqi
# Table of Contents

## Invited Talks

Towards a Signal Calculus for Event-Based Synchronous Languages .......................... 1  
   *Yongxin Zhao and He Jifeng*

Reasoning about Programs Using a Scientific Method .................................. 14  
   *Peter W. O’Hearn*

Poirot—A Concurrency Sleuth ......................................................... 15  
   *Shaz Qadeer*

## Formal Models

Context-Based Behavioral Equivalence of Components in Self-Adaptive Systems .......................................................... 16  
   *Narges Khakpour, Marjan Sirjani, and Ursula Goltz*

Towards a Practical Approach to Check UML/fUML Models Consistency Using CSP ....................................................... 33  
   *Islam Abdelhalim, Steve Schneider, and Helen Treharne*

The Safety-Critical Java Mission Model: A Formal Account ......................... 49  
   *Frank Zeyda, Ana Cavalcanti, and Andy Wellings*

Is There Evolution Before Birth? Deterioration Effects of Formal Z Specifications ......................................................... 66  
   *Andreas Bollin*

Asynchronous Communication in MSVL ............................................. 82  
   *Dapeng Mo, Xiaobing Wang, and Zhenhua Duan*

## Model Checking and Probability

Verification of Orchestration Systems Using Compositional Partial Order Reduction ......................................................... 98  
   *Tian Huat Tan, Yang Liu, Jun Sun, and Jin Song Dong*

Domain-Driven Probabilistic Analysis of Programmable Logic Controllers ................................................................. 115  
   *Hehua Zhang, Yu Jiang, William N.N. Hung, Xiaoyu Song, and Ming Gu*
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Statistical Model Checking for Distributed Probabilistic-Control Hybrid Automata with Smart Grid Applications</td>
<td>131</td>
</tr>
<tr>
<td>João G. Martins, André Platzer, and João Leite</td>
<td></td>
</tr>
<tr>
<td>PRTS: An Approach for Model Checking Probabilistic Real-Time Hierarchical Systems</td>
<td>147</td>
</tr>
<tr>
<td>Jun Sun, Yang Liu, Songzheng Song, Jin Song Dong, and Xiaohong Li</td>
<td></td>
</tr>
<tr>
<td>Specification and Development</td>
<td></td>
</tr>
<tr>
<td>Integrating Prototyping into the SOFL Three-Step Modeling Approach</td>
<td>163</td>
</tr>
<tr>
<td>Fauziah binti Zainuddin and Shaoying Liu</td>
<td></td>
</tr>
<tr>
<td>A Deterministic Interpreter Simulating a Distributed Real Time System Using VDM</td>
<td>179</td>
</tr>
<tr>
<td>Kenneth Lausdahl, Peter Gorm Larsen, and Nick Battle</td>
<td></td>
</tr>
<tr>
<td>On Fitting a Formal Method Into Practice</td>
<td>195</td>
</tr>
<tr>
<td>Rainer Gmehlich, Katrin Grau, Stefan Hallerstede, Michael Leuschel, Felix Lösch, and Daniel Plagge</td>
<td></td>
</tr>
<tr>
<td>A Formal Engineering Approach to High-Level Design of Situation Analysis Decision Support Systems</td>
<td>211</td>
</tr>
<tr>
<td>Roozbeh Farahbod, Vladimir Avram, Uwe Glässer, and Adel Guittouni</td>
<td></td>
</tr>
<tr>
<td>Security</td>
<td></td>
</tr>
<tr>
<td>Conformance Checking of Dynamic Access Control Policies</td>
<td>227</td>
</tr>
<tr>
<td>David Power, Mark Slaymaker, and Andrew Simpson</td>
<td></td>
</tr>
<tr>
<td>A Knowledge-Based Verification Method for Dynamic Access Control Policies</td>
<td>243</td>
</tr>
<tr>
<td>Masoud Koleini and Mark Ryan</td>
<td></td>
</tr>
<tr>
<td>Validation of Security-Design Models Using Z</td>
<td>259</td>
</tr>
<tr>
<td>Nafees Qamar, Yves Ledru, and Akram Idani</td>
<td></td>
</tr>
<tr>
<td>Formal Verification</td>
<td></td>
</tr>
<tr>
<td>Mutation in Linked Data Structures</td>
<td>275</td>
</tr>
<tr>
<td>Ewen Maclean and Andrew Ireland</td>
<td></td>
</tr>
<tr>
<td>Contract-Based Verification of Simulink Models</td>
<td>291</td>
</tr>
<tr>
<td>Pontus Boström</td>
<td></td>
</tr>
<tr>
<td>Exploiting Abstraction for Efficient Formal Verification of DSPs with Arrays of Reconfigurable Functional Units</td>
<td>307</td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td></td>
</tr>
<tr>
<td>Miroslav N. Velev and Ping Gao</td>
<td></td>
</tr>
</tbody>
</table>

| Architectural Verification of Control Systems Using CSP        | 323 |
|----------------------------------------------------------------|
| Joabe Jesus, Alexandre Mota, Augusto Sampaio, and Luiz Grijo   |

| Symbolic Execution of Alloy Models                            | 340 |
|----------------------------------------------------------------|
| Junaid Haroon Siddiqui and Sarfraz Khurshid                    |

**Cyber Physical Systems**

| Distributed Theorem Proving for Distributed Hybrid Systems   | 356 |
|--------------------------------------------------------------|
| David W. Renshaw, Sarah M. Loos, and André Platzer           |

| Towards a Model Checker for NesC and Wireless Sensor Networks | 372 |
|----------------------------------------------------------------|
| Manchun Zheng, Jun Sun, Yang Liu, Jin Song Dong, and Yu Gu    |

| Formal Analysis of a Scheduling Algorithm for Wireless Sensor Networks | 388 |
|-----------------------------------------------------------------------|
| Maissa Elleuch, Osman Hasan, Sofiène Tahar, and Mohamed Abid          |

| An Abstract Model for Proving Safety of Multi-lane Traffic Manoeuvres | 404 |
|---------------------------------------------------------------------|
| Martin Hilscher, Sven Linker, Ernst-Rüdiger Olderog, and Anders P. Ravn |

**Event-B**

| Formal Derivation of a Distributed Program in Event B            | 420 |
|------------------------------------------------------------------|
| Alexei Iliasov, Linas Laibinis, Elena Troubitsyna, and Alexander Romanovsky |

| From Requirements to Development: Methodology and Example         | 437 |
|------------------------------------------------------------------|
| Wen Su, Jean-Raymond Abrial, Runlei Huang, and Huibiao Zhu       |

| Reasoning about Liveness Properties in Event-B                   | 456 |
|------------------------------------------------------------------|
| Thai Son Hoang and Jean-Raymond Abrial                           |

**Verification, Analysis and Testing**

| Extracting Significant Specifications from Mining through Mutation Testing | 472 |
|----------------------------------------------------------------------------|
| Anh Cuong Nguyen and Siau-Cheng Khoo                                     |

| Developer-Oriented Correctness Proofs: A Case Study of Cheneys Algorithm | 489 |
|-------------------------------------------------------------------------|
| Holger Gast                                                             |
Static Analysis of String Values ........................................... 505
Giulia Costantini, Pietro Ferrara, and Agostino Cortesi

A Theory of Classes from the Theoretical Foundations of LePUS3 ...... 522
Jonathan Nicholson

Differencing Labeled Transition Systems ................................. 537
Zhenchang Xing, Jun Sun, Yang Liu, and Jin Song Dong

Refinement

Developing a Consensus Algorithm Using Stepwise Refinement........ 553
Jeremy W. Bryans

Refining Nodes and Edges of State Machines .......................... 569
Stefan Hallerstede and Colin Snook

Managing Complexity through Abstraction: A Refinement-Based
Approach to Formalize Instruction Set Architectures .................. 585
Fangfang Yuan, Stephen Wright, Kerstin Eder, and David May

A Language for Test Case Refinement in the Test Template
Framework ............................................................................... 601
Maximiliano Cristiá, Diego Hollmann, Pablo Albertengo,
Claudia Frydman and Pablo Rodríguez Monetti

Theorem Proving and Rewriting

Automating Algebraic Methods in Isabelle ......................... 617
Walter Guttmann, Georg Struth, and Tjark Weber

Term Rewriting in Logics of Partial Functions ...................... 633
Matthias Schmalz

Synchronous AADL and Its Formal Analysis in Real-Time Maude.... 651
Kyungmin Bae, Peter Csaba Ölveczky, Abdullah Al-Nayeem, and
José Meseguer

Author Index ........................................................................... 669