Editorial Board

David Hutchison  
*Lancaster University, UK*

Takeo Kanade  
*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler  
*University of Surrey, Guildford, UK*

Jon M. Kleinberg  
*Cornell University, Ithaca, NY, USA*

Alfred Kobsa  
*University of California, Irvine, CA, USA*

Friedemann Mattern  
*ETH Zurich, Switzerland*

John C. Mitchell  
*Stanford University, CA, USA*

Moni Naor  
*Weizmann Institute of Science, Rehovot, Israel*

Oscar Nierstrasz  
*University of Bern, Switzerland*

C. Pandu Rangan  
*Indian Institute of Technology, Madras, India*

Bernhard Steffen  
*TU Dortmund University, Germany*

Demetri Terzopoulos  
*University of California, Los Angeles, CA, USA*

Doug Tygar  
*University of California, Berkeley, CA, USA*

Gerhard Weikum  
*Max Planck Institute for Informatics, Saarbruecken, Germany*
FM 2014:
Formal Methods

19th International Symposium
Singapore, May 12-16, 2014
Proceedings
Preface

Message from the Organising Committee

Welcome to FM-2014! Welcome to Singapore! This is the nineteenth in a series of symposia organized by Formal Methods Europe, this is its first time in Asia! The conference is jointly organized by three Singapore universities NUS, NTU, SUTD and a French-Singapore joint research lab IPAL. FM week is May 12–16, 2014 at the NUS, with a strong core technical program. Additionally six workshops and five tutorials focusing on specific formal methods for various application areas will be held early in FM week. I would like to express my heart-felt thanks to Programme Committee Cliff Jones, Pekka Pihlajasaari and Jun Sun; Doc Symposium Chair: Annabelle McIver; Workshop Chair: Shengchao Qin; Publicity Chairs: Jonathan Bowen, Kenji Taguchi; Tutorial Chair: Richard Paige; and Financial/Local Chair: Yang Liu; local organising committee members: Guangdong Bai, Manman Chen, Jianqi Shi, Ling Shi, Yan Liu as well as the workshop organisers, tutorial presenters and many student helpers, for their hard work to make FM-2014 successful.

February 2014

Jin Song Dong
Message from Programme Committee Chairs

FM-2014 is the 19th symposium in a series that began life as “VDM Europe” in 1987 and, in 1993, became “Formal Methods Europe”. The nod to Europe in these names marked the initial funding support from the European Union but is now purely historical with “FME” being today an international organisation and the renowned FM symposia attracting papers from across the globe. For the Programme Committee (PC) chairs of the Singapore event, it has been a privilege to play a part in continuing the success of a series that has consistently focussed on applicable formal methods.

This Singapore event is only the second to take place outside of Europe (the first was in 2006 at McMaster University in Canada). Placing a conference in a completely new geographical location poses some risks so the PC was delighted to receive a strong set of over 150 submitted papers; for the Main Stream 38 papers were selected and seven for the Industry Stream. In both cases, we felt that we were able to set the very highest standard. The overall acceptance rate is 29%.

We were extremely happy to gain ready acceptance to our invitation from three excellent invited speakers:

- Zhenjiang Hu from Japan’s National Institute of Informatics is one of the leading researchers in the new field of bidirectional model transformations.
- Gerwin Klein has led NICTA’s formal verification part of the Trustworthy Embedded Systems project and was the leader of the L4.verified and L4pilot projects.
- Jim Woodcock has made numerous contributions to the application of industrial-scale software engineering and formal methods.

Dines Bjørner was one of the co-founders of this series of symposia and has done an enormous amount to promote formal methods in general and to help FME in particular (anyone who attended FM-99 in Toulouse will never forget the experience!). We decided therefore to create a special role for his “Distinguished Lecture”.

John Fitzgerald was chair of FME for the gestation period and birth of FM-2014 and we should like to express our thanks both to the committee and to John in particular for his many years of unstinting service to our community. Nor has he forgotten one of the most important roles of any leader – that of finding (and persuading) a worthy successor – and we Ana Cavalcanti the very best for her period as Chair of FME.

The volume in your hands provides a scientific guarantee of a successful symposium. The vibrant city-state of the Lion and its famous hospitality will, we believe, do the rest to ensure that FM-2014 in Singapore will provide its own memorable experience to participants.

Our warm thanks go to the members of the PC and their reviewers. Without them, the selection of papers would have been overwhelming and sterile. The enormous breadth of background in their comments resulted in the discovery of
a number of gems that could otherwise have been overlooked. Of course the PC would have nothing to work on but for the authors who submit interesting and relevant papers and it is to them we express our final thanks.

February 2014

Cliff Jones
Pekka Pihlajasaari
Jun Sun
Organisation

We are grateful to Formal Methods Europe (FME), National University of Singapore (NUS), Nanyang Technological University (NTU), Singapore University of Technology and Design (SUTD) and the French-Singapore joint research lab IPAL for organizing FM 2014. Our special thanks to the faculty, students, and staff, who volunteered their time in the Organizing Committee.

General Chair

Jin Song Dong National University of Singapore, Singapore

Program Committee Chairs

Cliff B. Jones Newcastle University, UK
Pekka Pihlajasaari Data Abstraction (Pty) Ltd, South Africa
Jun Sun Singapore University of Technology and Design, Singapore

Doctoral Symposium Chair

Annabelle McIver Macquarie University, Australia

Workshop Chair

Shengchao Qin University of Teesside, UK

Publicity Chairs

Jonathan Bowen London South Bank University, UK
Kenji Taguchi AIST, Japan

Tutorial Chair

Richard Paige University of York, UK
Financial/Local Chair

Yang Liu
Nanyang Technological University, Singapore

Program Committee

Bernhard Aichernig
Graz University of Technology, Austria

Richard Banach
University of Manchester, UK

Juan Bicarregui
Rutherford Appleton Laboratory, UK

Jon Burton
Praxis, UK

Andrew Butterfield
Trinity College Dublin, Ireland

Ana Cavalcanti
York University, UK

Marsha Chechik
University of Toronto, Canada

Yu-Fang Chen
Academia Sinica, Taiwan

Wei-Ngan Chin
National University of Singapore, Singapore

Cristina Cifuentes
Oracle, USA

Jim Davies
University of Oxford, UK

Frank De Boer
CWI, The Netherlands

Ewen Denney
SGT/NASA Ames, USA

Dino Distefano
Facebook and University of London, UK

José Luiz Fiadeiro
Royal Holloway, University of London, UK

John Fitzgerald
Newcastle University, UK

Marie-Claude Gaudel
LRI, Université Paris-Sud and CNRS, France

Jaco Geldenhuys
Stellenbosch University, South Africa

Dimitra Giannakopoulou
NASA Ames, USA

Stefania Gnesi
ISTI-CNR, Italy

Wolfgang Grieskamp
Google, USA

Lindsay Groves
Victoria University of Wellington, New Zealand

Jim Grundy
Intel Corporation, USA

Stefan Gruner
University of Pretoria, South Africa

Anne E. Haxthausen
Technical University of Denmark, Denmark

Ian J. Hayes
University of Queensland, Australia

Constance Heitmeyer
Naval Research Laboratory, USA

Jane Hillston
University of Edinburgh, UK

Michael Holloway
NASA, USA

Shinichi Honiden
National Institute of Informatics, Japan

Ralf Huuck
NICTA, Australia

Daniel Jackson
MIT, USA

Cliff Jones
Newcastle University, UK

Rajeev Joshi
Laboratory for Reliable Software, Jet Propulsion Laboratory, USA

Peter Gorm Larsen
Aarhus School of Engineering, Denmark

Gary T. Leavens
University of Central Florida, USA
Yves Ledru
Michael Leuschel
Brendan Mahony
Tom Maibaum
Annabelle McIver
Dominique Mery
Peter Müller
Tobias Nipkow
Colin O’Halloran
Jose Oliveira
Pekka Pihlajasaari
André Platzer
Zongyan Qiu
Ken Robinson
Andreas Roth
Abhik Roychoudhury
Augusto Sampaio
Steve Schneider
Emil Sekerkinski
Xiaoyu Song
Ketil Stoelen
Jing Sun
Jun Sun
Axel Van Lamsweerde
Marcel Verhoef
Willem Visser
Chao Wang
Alan Wassung
Pamela Zave
Lijun Zhang
Hongjun Zheng

Laboratoire d’Informatique de Grenoble -
Université Joseph Fourier, France
University of Düsseldorf, Germany
DSTO, Australia
McMaster University, Canada
Macquarie University, Australia
Université de Lorraine, LORIA, France
ETH Zürich, Switzerland
TU München, Germany
QinetiQ Ltd., UK
Universidade do Minho, Portugal
Data Abstraction (Pty) Ltd, South Africa
Carnegie Mellon University, USA
Peking University, China
The University of New South Wales, Australia
SAP Research, Germany
National University of Singapore, Singapore
Federal University of Pernambuco, Brazil
University of Surrey, UK
McMaster University, Canada
Portland State University, USA
SINTEF, Norway
The University of Auckland, New Zealand
Singapore University of Technology and Design
Université Catholique de Louvain, Belgium
Chess, The Netherlands
Stellenbosch University, South Africa
Virginia Tech, USA
McMaster University, Canada
AT&T Laboratories–Research, USA
Technical University of Denmark, DK
MathWorks, USA

Additional Reviewers

Abal, Iago
Ait Ameur, Yamine
Albarghouthi, Aws
Aliakbary, Sadegh
Almeida, Jose Bacelar
Andrews, Zoe
Atanasiu, Radu-Florian
Banach, Richard
Bezirgiannis, Nikolaos
Bicarregui, Juan
Blanchette, Jasmin Christian
Bobot, François
Bodeveix, Jean-Paul
Bonakdarpour, Borzoo
Brekling, Aske
Bryans, Jeremy W.
Buccharone, Antonio
Carvalho, Gustavo
Castro, Pablo
Ciancia, Vincenzo
Clark, Allan
Coleman, Joey
Costea, Andreea
Couto, Luis
Davies, Jim
Demasi, Ramiro
Dobrikov, Ivaylo
Dunne, Steve
Durán, Francisco
Eldib, Hassan
Fantechi, Alessandro
Galpin, Vashti
Gherghina, Cristian
Gheyi, Rohit
Ghorbal, Khalil
Gilmore, Stephen
Gretz, Friedrich
Gurfinkel, Arie
Hague, Matthew
Hahn, Moritz
Hallerstedt, Stefan
Hansen, Dominik
Henriques, David
Holik, Lukas
Ishikawa, Fuyuki
Isobe, Yoshinao
Janicki, Ryszard
Jansen, David N.
Jeannin, Jean-Baptiste
Joeblt, Elisabeth
Joshi, Rajeev
Jorgensen, Peter
K.R., Raghavendra
Kassios, Ioannis
Kiniry, Joseph
Krautsevich, Leanid
Krenn, Willibald
Kings, Sebastian
Krishnan, Paddy
Kusano, Markus
Le, Duy Khanh
Le, Quang Loc
Le, Ton Chanh
Lepri, Daniela
Li, Guangyuan
Li, Qin
Li, Yi
Liu, Yang
Lluch Lafuente, Alberto
Loos, Sarah
Lorber, Florian
Loreti, Michele
Lovengreen, Hans Henrik
Martins, João G.
Meinicke, Larissa
Merz, Stephan
Miyazawa, Alvaro
Monahan, Rosemary
Moreira, Nelma
Morgan, Carrol
Morgan, Carroll
Murray, Toby
Müller, Andreas
Nickovic, Dejan
Olivier, Martin
Payne, Richard
Pereira, David
Pierce, Ken
Quesel, Jan-David
Refsdal, Atle
Robinson, Peter
Rogalewicz, Adam
Runde, Ragnhild Kobro
Safilian, Aliakbar
Sakamoto, Kazunori
Santosa, Andrew Edward
Schewe, Sven
Schulze, Uwe
Seehusen, Fredrik
Seidl, Helmut
Serbanescu, Vlad
Sharma, Asankhaya
Sighiream, Mihaela
Simmonds, William
Singh, Neeraj
Solhaug, Bjørnar
Solms, Fritz
Song, Lei
<table>
<thead>
<tr>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sousa Pinto, Jorge</td>
</tr>
<tr>
<td>Steggles, Jason</td>
</tr>
<tr>
<td>Tanabe, Yoshinori</td>
</tr>
<tr>
<td>Tarasyuk, Anton</td>
</tr>
<tr>
<td>Ter Beek, Maurice H.</td>
</tr>
<tr>
<td>Timm, Nils</td>
</tr>
<tr>
<td>Tiran, Stefan</td>
</tr>
<tr>
<td>Treharne, Helen</td>
</tr>
<tr>
<td>Trung, Ta Quang</td>
</tr>
<tr>
<td>Turrini, Andrea</td>
</tr>
<tr>
<td>Vakili, Sasan</td>
</tr>
<tr>
<td>van der Storm, Tijs</td>
</tr>
<tr>
<td>Vu, Linh H.</td>
</tr>
<tr>
<td>Wang, Chen-Wei</td>
</tr>
<tr>
<td>Wang, Hao</td>
</tr>
<tr>
<td>Wasowski, Andrzej</td>
</tr>
<tr>
<td>Watson, Bruce</td>
</tr>
<tr>
<td>Wei, Wei</td>
</tr>
<tr>
<td>Yang, Zijiang</td>
</tr>
<tr>
<td>Yi, Jooyong</td>
</tr>
<tr>
<td>Yoshioka, Nobukazu</td>
</tr>
<tr>
<td>Zeyda, Frank</td>
</tr>
<tr>
<td>Zhang, Chenyi</td>
</tr>
<tr>
<td>Zhang, Lu</td>
</tr>
</tbody>
</table>
# Table of Contents

Validity Checking of Putback Transformations in Bidirectional Programming .................................................... 1  
   *Zhenjiang Hu, Hugo Pacheco, and Sebastian Fischer*

Proof Engineering Considered Essential ........................................ 16  
   *Gerwin Klein*

Engineering UToPiA: Formal Semantics for *CML* ............................... 22  
   *Jim Woodcock*

40 Years of Formal Methods: Some Obstacles and Some Possibilities? ... 42  
   *Dines Bjørner and Klaus Havelund*

A Refinement Based Strategy for Local Deadlock Analysis of Networks of CSP Processes .............................................. 62  
   *Pedro Antonino, Augusto Sampaio, and Jim Woodcock*

Algebraic Principles for Rely-Guarantee Style Concurrency Verification Tools .......................................................... 78  
   *Alasdair Armstrong, Victor B.F. Gomes, and Georg Struth*

Definition, Semantics, and Analysis of Multirate Synchronous AADL ... 94  
   *Kyungmin Bae, Peter Csaba Ołveczky, and José Meseguer*

TRUSTFOUND: Towards a Formal Foundation for Model Checking Trusted Computing Platforms .......................................... 110  
   *Guangdong Bai, Jianan Hao, Jianliang Wu, Yang Liu, Zhenkai Liang, and Andrew Martin*

The VerCors Tool for Verification of Concurrent Programs ............ 127  
   *Stefan Blom and Marieke Huisman*

Knowledge-Based Automated Repair of Authentication Protocols ...... 132  
   *Borzoo Bonakdarpour, Reza Hajisheykhi, and Sandeep S. Kulkarni*

A Simplified Z Semantics for Presentation Interaction Models .......... 148  
   *Judy Bowen and Steve Reeves*

Log Analysis for Data Protection Accountability .......................... 163  
   *Denis Butin and Daniel Le Métayer*

Automatic Compositional Synthesis of Distributed Systems .......... 179  
   *Werner Damm and Bernd Finkbeiner*
Automated Real Proving in PVS via MetiTarski ......................... 194
William Denman and César Muñoz

Quiescent Consistency: Defining and Verifying Relaxed Linearity ................. 200
John Derrick, Brijesh Dongol, Gerhard Schellhorn, Bogdan Tofan, Oleg Travkin, and Heike Wehrheim

Temporal Precedence Checking for Switched Models and Its Application to a Parallel Landing Protocol ....................... 215
Parasara Sridhar Duggirala, Le Wang, Sayan Mitra, Mahesh Viswanathan, and César Muñoz

Contracts in Practice ........................................ 230
H.-Christian Estler, Carlo A. Furia, Martin Nordio, Marco Piccioni, and Bertrand Meyer

When Equivalence and Bisimulation Join Forces in Probabilistic Automata .......... 247
Yuan Feng and Lijun Zhang

Precise Predictive Analysis for Discovering Communication Deadlocks in MPI Programs ........................................ 263
Vojtěch Forejt, Daniel Kroening, Ganesh Narayanaswamy, and Subodh Sharma

Proof Patterns for Formal Methods ................................ 279
Leo Freitas and Iain Whiteside

Efficient Runtime Monitoring with Metric Temporal Logic: A Case Study in the Android Operating System .................. 296
Hendra Gunadi and Alwen Tiu

ISCASMc: A Web-Based Probabilistic Model Checker .................. 312
Ernst Moritz Hahn, Yi Li, Sven Schewe, Andrea Turrini, and Lijun Zhang

Invariants, Well-Founded Statements and Real-Time Program Algebra .... 318
Ian J. Hayes and Larissa Meinicke

Checking Liveness Properties of Presburger Counter Systems Using Reachability Analysis ......................................... 335
K. Vasanta Lakshmi, Aravind Acharya, and Raghavan Komondoor

A Symbolic Algorithm for the Analysis of Robust Timed Automata .... 351
Piotr Kordy, Rom Langerak, Sjouke Mauw, and Jan Willem Polderman
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Revisiting Compatibility of Input-Output Modal Transition Systems</td>
<td>367</td>
</tr>
<tr>
<td>Ivo Krka, Nicolás D’Ippolito, Nenad Medvidović, and</td>
<td></td>
</tr>
<tr>
<td>Sebastián Uchitel</td>
<td></td>
</tr>
<tr>
<td>Co-induction Simply: Automatic Co-inductive Proofs in a Program</td>
<td>382</td>
</tr>
<tr>
<td>K. Rustan M. Leino and Michal Moskal</td>
<td></td>
</tr>
<tr>
<td>Management of Time Requirements in Component-Based Systems</td>
<td>399</td>
</tr>
<tr>
<td>Yi Li, Tian Huat Tan, and Marsha Chechik</td>
<td></td>
</tr>
<tr>
<td>Compositional Synthesis of Concurrent Systems through Causal Model</td>
<td>416</td>
</tr>
<tr>
<td>Shang-Wei Lin and Pao-Ann Hsiung</td>
<td></td>
</tr>
<tr>
<td>Formal Verification of Operational Transformation</td>
<td>432</td>
</tr>
<tr>
<td>Yang Liu, Yi Xu, Shao Jie Zhang, and Chengzheng Sun</td>
<td></td>
</tr>
<tr>
<td>Verification of a Transactional Memory Manager under Hardware</td>
<td>449</td>
</tr>
<tr>
<td>Failures and Restarts</td>
<td></td>
</tr>
<tr>
<td>Ognjen Marić and Christoph Sprenger</td>
<td></td>
</tr>
<tr>
<td>SCJ: Memory-Safety Checking without Annotations</td>
<td>465</td>
</tr>
<tr>
<td>Chris Marriott and Ana Cavalcanti</td>
<td></td>
</tr>
<tr>
<td>Refactoring, Refinement, and Reasoning: A Logical Characterization</td>
<td>481</td>
</tr>
<tr>
<td>for Hybrid Systems</td>
<td></td>
</tr>
<tr>
<td>Stefan Mitsch, Jan-David Quesel, and André Platzer</td>
<td></td>
</tr>
<tr>
<td>Object Propositions</td>
<td>497</td>
</tr>
<tr>
<td>Lígia Nistor, Jonathan Aldrich, Stephanie Balzer, and Hannes Mehnert</td>
<td></td>
</tr>
<tr>
<td>Flexible Invariants through Semantic Collaboration</td>
<td>514</td>
</tr>
<tr>
<td>Nadia Polikarpova, Julian Tschanne, Carlo A. Furia, and</td>
<td></td>
</tr>
<tr>
<td>Bertrand Meyer</td>
<td></td>
</tr>
<tr>
<td>Efficient Tight Field Bounds Computation Based on Shape</td>
<td>531</td>
</tr>
<tr>
<td>Pablo Ponzio, Nicolás Rosner, Nazareno Aguirre, and Marcelo Frias</td>
<td></td>
</tr>
<tr>
<td>A Graph-Based Transformation Reduction to Reach UPPAAL States Faster</td>
<td>547</td>
</tr>
<tr>
<td>Jonas Rinast, Sibylle Schupp, and Dieter Gollmann</td>
<td></td>
</tr>
<tr>
<td>Computing Quadratic Invariants with Min- and Max-Policy Iterations:</td>
<td>563</td>
</tr>
<tr>
<td>A Practical Comparison</td>
<td></td>
</tr>
<tr>
<td>Pierre Roux and Pierre-Loïc Garoche</td>
<td></td>
</tr>
</tbody>
</table>
Efficient Self-composition for Weakest Precondition Calculi

Christoph Scheben and Peter H. Schmitt
579

Towards a Formal Analysis of Information Leakage for Signature
Attacks in Preferential Elections

Roland Wen, Annabelle McIver, and Carroll Morgan
595

Analyzing Clinical Practice Guidelines Using a Decidable Metric
Interval-Based Temporal Logic

Morteza Yousef Sanati, Wendy MacCaull, and
Thomas S.E. Maibaum
611

A Modular Theory of Object Orientation in Higher-Order UTP

Frank Zeyda, Thiago Santos, Ana Cavalcanti, and Augusto Sampaio
627

Formalizing and Verifying a Modern Build Language

Maria Christakis, K. Rustan M. Leino, and Wolfram Schulte
643

The Wireless Fire Alarm System: Ensuring Conformance to Industrial
Standards through Formal Verification

Sergio Feo-Arenis, Bernd Westphal, Daniel Dietsch,
Marco Muñiz, and Ahmad Siyar Andisha
658

Formally Verifying Graphics FPU: An Intel® Experience

Aarti Gupta, V. Achutha Kirankumar M., and Rajnish Ghughal
673

MDP-Based Reliability Analysis of an Ambient Assisted
Living System

Yan Liu, Lin Gui, and Yang Liu
688

Diagnosing Industrial Business Processes: Early Experiences

Suman Roy, A.S.M. Sajeev, and Srivibha Sripathy
703

Formal Verification of Lunar Rover Control Software Using UPPAAL

Lijun Shan, Yuying Wang, Ning Fu, Xingshe Zhou, Lei Zhao,
Lijing Wan, Lei Qiao, and Jianxin Chen
718

Formal Verification of a Descent Guidance Control Program of a Lunar
Lander

Hengjun Zhao, Mengfei Yang, Naijun Zhan, Bin Gu,
Liang Zou, and Yao Chen
733

Author Index
749