Preface

FME 2001 is the tenth in a series of meetings organized every eighteen months by Formal Methods Europe (FME), an independent association whose aim is to stimulate the use of, and research on, formal methods for software development. It follows four VDM Europe Symposia, four other Formal Methods Europe Symposia, and the 1999 World Congress on Formal Methods in the Development of Computing Systems. These meetings have been notably successful in bringing together a community of users, researchers, and developers of precise mathematical methods for software development.

FME 2001 took place in Berlin, Germany and was organized by the Computer Science Department of the Humboldt-Universität zu Berlin. The theme of the symposium was Formal Methods for Increasing Software Productivity. This theme recognizes that formal methods have the potential to do more for industrial software development than enhance software quality – they can also increase productivity at many different points in the software life-cycle.

The importance of the theme is borne out by the many contributed papers showing how formal methods can make software development more efficient. There is an emphasis on tools that find errors automatically, or with relatively little human effort. There is also an emphasis on the use of formal methods to assist with critical, labor-intensive tasks such as program design and test-case generation.

The many application areas addressed in the various parts of the symposium (tutorials, workshops, contributed papers, and invited papers) include smart cards, avionic and satellite computers, financial contracts, E-commerce, middleware, security, telecommunications, and the FireWire standard. Many contributions involve multi-disciplinary teams of researchers coming from both industry and academia. We are pleased to see this evidence of the spreading influence of formal methods.

In addition to the 32 papers selected for presentation by the program committee (out of 72 submissions involving authors from 25 countries), this volume contains the abstracts of three invited talks: Lightweight Formal Methods, by Daniel Jackson (Laboratory for Computer Science, MIT); A Programming Model for Wide-Area Computing, by Jayadev Misra (University of Texas at Austin); and Composing Contracts: An Adventure in Financial Engineering by Simon Peyton Jones (Microsoft Research Ltd).

January 2001

José Nuno Oliveira
Pamela Zave
Acknowledgements

We are very grateful to the members of the program committee and their referees for their care and diligence in reviewing the submitted papers. We are also grateful to the local organizers and the sponsoring institutions.

Program Committee

Eerke Boiten (UK)  
Rick Butler (USA)  
Lars-Henrik Eriksson (Sweden)  
John Fitzgerald (UK)  
Peter Gorm Larsen (Denmark)  
Yves Ledru (France)  
Dominique Méry (France)  
Jayadev Misra (USA)  
Richard Moore (Macau)  
Friederike Nickl (Germany)  

Tobias Nipkow (Germany)  
José N. Oliveira (co-chair, Portugal)  
Paritosh Pandya (India)  
Nico Plat (The Netherlands)  
Amir Pnueli (Israel)  
Augusto Sampaio (Brazil)  
Steve Schneider (UK)  
Jim Woodcock (UK)  
Pamela Zave (co-chair, USA)  

Organizing Committee

Birgit Heene  
Stefan Jähnichen (co-chair)  
Axel Martens  

Wolfgang Reisig (co-chair)  
Thomas Urban  
Tobias Vesper  

Sponsoring Institutions

The generous support of the following companies and institutions is gratefully acknowledged:

Humboldt-Universität zu Berlin  
GMD FIRST  
Formal Methods Europe  
Universidade do Minho  
DaimlerChrysler AG  
WIDIS GmbH Berlin  
WISTA Management GmbH  

External Referees

All submitted papers were reviewed by members of the program committee and a number of external referees, who produced extensive review reports and without whose work the quality of the symposium would have suffered. To the best of our knowledge the list below is accurate. We apologize for any omissions or inaccuracies.
<table>
<thead>
<tr>
<th>Name</th>
<th>Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Will Adams</td>
<td>Nora Koch</td>
</tr>
<tr>
<td>Carlos Bacelar Almeida</td>
<td>Izak van Langevelde</td>
</tr>
<tr>
<td>Rajeev Alur</td>
<td>Antónia Lopes</td>
</tr>
<tr>
<td>Tamarah Arons</td>
<td>Gavin Lowe</td>
</tr>
<tr>
<td>Roberto Souto Maior de Barros</td>
<td>Panagiotis Manolios</td>
</tr>
<tr>
<td>Pierre Berlioux</td>
<td>Andrew Martin</td>
</tr>
<tr>
<td>Didier Bert</td>
<td>Stephan Merz</td>
</tr>
<tr>
<td>Juan Bicarregui</td>
<td>Anna Mikhailova</td>
</tr>
<tr>
<td>Lynne Blair</td>
<td>Oliver Moeller</td>
</tr>
<tr>
<td>Roland Bol</td>
<td>Alexandre Mota</td>
</tr>
<tr>
<td>Paulo Borba</td>
<td>Paul Mukherjee</td>
</tr>
<tr>
<td>Lydie du Bousquet</td>
<td>Kedar S. Namjoshi</td>
</tr>
<tr>
<td>Max Breitling</td>
<td>David Naumann</td>
</tr>
<tr>
<td>Dominique Cansell</td>
<td>George Necula</td>
</tr>
<tr>
<td>Ana Cavalcanti</td>
<td>Gertjan van Oosten</td>
</tr>
<tr>
<td>Michel Chaudron</td>
<td>Stephen Paynter</td>
</tr>
<tr>
<td>David Cohen</td>
<td>Andrej Pietschker</td>
</tr>
<tr>
<td>Ernie Cohen</td>
<td>Nir Piterman</td>
</tr>
<tr>
<td>Jonathan Draper</td>
<td>Marie-Laure Potet</td>
</tr>
<tr>
<td>Sophie Dupuy-Chessa</td>
<td>Alexander Pretschner</td>
</tr>
<tr>
<td>Peter van Eijk</td>
<td>Kees Pronk</td>
</tr>
<tr>
<td>Loe Feijs</td>
<td>Antonio Ravara</td>
</tr>
<tr>
<td>Jean-Claude Fernandez</td>
<td>Jean-Luc Richier</td>
</tr>
<tr>
<td>Dana Fisman</td>
<td>Steve Riddle</td>
</tr>
<tr>
<td>D. Galmiche</td>
<td>Jan Rogier</td>
</tr>
<tr>
<td>Max Geerling</td>
<td>Nick Rossiter</td>
</tr>
<tr>
<td>Chris George</td>
<td>Stefan Römmer</td>
</tr>
<tr>
<td>P. Gibson</td>
<td>Thomas Santen</td>
</tr>
<tr>
<td>N. Goga</td>
<td>João Saraiva</td>
</tr>
<tr>
<td>Jan Friso Groote</td>
<td>Emil Sekerinski</td>
</tr>
<tr>
<td>Jan Haveman</td>
<td>Kaisa Sere</td>
</tr>
<tr>
<td>Ian Hayes</td>
<td>Elad Shahar</td>
</tr>
<tr>
<td>Maritta Heisel</td>
<td>Ofer Shtrichman</td>
</tr>
<tr>
<td>Rolf Hennicker</td>
<td>Kim Sunesen</td>
</tr>
<tr>
<td>Dang Van Hung</td>
<td>Hans Tonino</td>
</tr>
<tr>
<td>Tomasz Janowski</td>
<td>Richard Trefler</td>
</tr>
<tr>
<td>He Jifeng</td>
<td>Alexandre Vasconcelos</td>
</tr>
<tr>
<td>Adrian Johnstone</td>
<td>Marcel Verhoeft</td>
</tr>
<tr>
<td>Cliff B. Jones</td>
<td>Vladimir Zadorozhny</td>
</tr>
<tr>
<td>Rajeev Joshi</td>
<td>Irfan Zakiuuddin</td>
</tr>
<tr>
<td>Charanjit S. Jutla</td>
<td>Lenore Zuck</td>
</tr>
<tr>
<td>Alexander Knapp</td>
<td></td>
</tr>
</tbody>
</table>
Tutorials and Workshops

The following tutorials were scheduled for the two days preceding the research symposium:

**SDL 2001** — J. Fischer, Andreas Prinz, and Eckhardt Holz (Humboldt-Universität zu Berlin and DResearch Digital Media Systems GmbH)

**Modeling for Formal Methods** — Micheál Mac an Airchinnigh, Andrew Butterfield, and Arthur Hughes (University of Dublin)

**From UML to Z, Support for Requirements Engineering with RoZ** — Yves Ledru and Sophie Dupuy (LSR/IMAG)

**Beyond Model Checking: Formal Specification and Verification of Practical Mission-Critical Systems** — Ramesh Bharadwaj (Naval Research Laboratory, USA)

We are grateful to all those who kindly submitted tutorial proposals. In addition, two international workshops were co-located with the symposium tutorials:

**First International Workshop on Automated Verification of Infinite-State Systems (AVISS'01)** — organized by Ramesh Bharadwaj (Naval Research Laboratory, USA) and Steve Sims (Reactive-Systems, Inc.)

**Formal Approaches to the IEEE 1394 (FireWire) Identify Protocol** — organized by Carron Shankland, Savi Maharaj (University of Stirling), and Judi Romijn (University of Nijmegen).

We thank the organizers of these events for their interest in sharing the atmosphere of the symposium.
Table of Contents

Lightweight Formal Methods ...................................................... 1  
  Daniel Jackson

Reformulation: A Way to Combine Dynamic Properties and B Refinement 2  
  F. Bellegarde, C. Darlot, J. Julliand, O. Kouchnarenko

Mechanized Analysis of Behavioral Conformance in the Eiffel  
Base Libraries ................................................................. 20  
  Steffen Helke, Thomas Santen

Proofs of Correctness of Cache-Coherence Protocols .................... 43  
  Joseph Stoy, Xiaowei Shen, Arvind

Model-Checking Over Multi-valued Logics.................................. 72  
  Marsha Chechik, Steve Easterbrook, Victor Petrovykh

How to Make FDR Spin: LTL Model Checking of CSP by Refinement ...... 99  
  Michael Leuschel, Thierry Massart, Andrew Currie

Avoiding State Explosion for Distributed Systems with Timestamps ...... 119  
  Fabrice Derepas, Paul Gastin, David Plainfosé

Secrecy-Preserving Refinement................................................ 135  
  Jan Jürjens

Information Flow Control and Applications – Bridging a Gap – .......... 153  
  Heiko Mantel

A Rigorous Approach to Modeling and Analyzing  
E-Commerce Architectures ..................................................... 173  
  Vasu S. Alagar, Zheng Xi

A Formal Model for Reasoning about Adaptive QoS-Enabled Middleware . 197  
  Nalini Venkatasubramanian, Carolyn Talcott, Gul Agha

A Programming Model for Wide-Area Computing.......................... 222  
  Jayadev Misra

A Formal Model of Object-Oriented Design and GoF Design Patterns .... 223  
  Andres Flores, Richard Moore, Luis Reynoso

Validation of UML Models Thanks to Z and Lustre ....................... 242  
  Sophie Dupuy-Chessa, Lydie du Bousquet
Components, Contracts, and Connectors for the Unified Modelling Language UML .................................................. 259
\textit{Claus Pahl}

An Integrated Approach to Specification and Validation of Real-Time Systems .................................................. 278
\textit{Adnan Sherif, Augusto Sampaio, Sérgio Cavalcante}

Real-Time Logic Revisited ........................................... 300
\textit{Stephen E. Paynter}

Improvements in BDD-Based Reachability Analysis of Timed Automata .................................................. 318
\textit{Dirk Beyer}

Serialising Parallel Processes in a Hardware/Software Partitioning Context .................................................. 344
\textit{Leila Silva, Augusto Sampaio, Geraint Jones}

Verifying Implementation Relations ................................ 364
\textit{Jonathan Burton, Maciej Koutny, Giuseppe Pappalardo}

An Adequate Logic for Full LOTOS .................................. 384
\textit{Muffy Calder, Savi Maharaj, Carron Shankland}

Towards a Topos Theoretic Foundation for the Irish School of Constructive Mathematics (\(\mathcal{M}\mathcal{C}\)) ........................................... 396
\textit{Micheál Mac an Airchinnigh}

Faithful Translations among Models and Specifications ............. 419
\textit{Shmuel Katz}

Composing Contracts: An Adventure in Financial Engineering ..... 435
\textit{Simon Peyton Jones}

From Complex Specifications to a Working Prototype. A Protocol Engineering Case Study .................................. 436
\textit{Manuel J. Fernández Iglesias, Francisco J. González-Castaño, José M. Pousada Carballo, Martín Llamas Nistal, Alberto Romero Feijoo}

Coverage Directed Generation of System-Level Test Cases for the Validation of a DSP System .......................... 449
\textit{Laurent Arditi, Hédi Boufaïed, Arnaud Cavanié, Vincent Stehlé}

Using Formal Verification Techniques to Reduce Simulation and Test Effort ........................................ 465
\textit{O. Laurent, P. Michel, V. Wiels}

Transacted Memory for Smart Cards .................................. 478
\textit{Pieter H. Hartel, Michael J. Butler, Eduard de Jong, Mark Longley}
Houdini, an Annotation Assistant for ESC/Java ......................... 500
Cormac Flanagan, K. Rustan M. Leino

A Heuristic for Symmetry Reductions with Scalarsets .................. 518
Dragan Bošnački, Dennis Dams, Leszek Holenderski

View Updatability Based on the Models of a Formal Specification ...... 534
Michael Johnson, Robert Rosebrugh

Grammar Adaptation ................................................................. 550
Ralf Lämmel

Test-Case Calculation through Abstraction ................................. 571
Bernhard K. Aichernig

A Modular Approach to the Specification and Validation of an Electrical
Flight Control System ................................................................. 590
M. Doche, I. Vernier-Mounier, F. Kordon

A Combined Testing and Verification Approach for Software Reliability . 611
Natasha Sharygina, Doron Peled

Author Index ................................................................. 629