FME 2003: Formal Methods

International Symposium of Formal Methods Europe
Pisa, Italy, September 8-14, 2003
Proceedings
Preface

This volume contains the proceedings of FM 2003, the 12th International Formal Methods Europe Symposium which was held in Pisa, Italy on September 8–14, 2003. Formal Methods Europe (FME, www.fmeurope.org) is an independent association which aims to stimulate the use of and research on formal methods for system development. FME conferences began with a VDM Europe symposium in 1987. Since then, the meetings have grown and have been held about once every 18 months. Throughout the years the symposia have been notably successful in bringing together researchers, tool developers, vendors, and users, both from academia and from industry.

Unlike previous symposia in the series, FM 2003 was not given a specific theme. Rather, its main goal could be synthesized as “widening the scope.” Indeed, the organizers aimed at enlarging the audience and impact of the symposium along several directions. Dropping the suffix ‘E’ from the title of the conference reflects the wish to welcome participation and contribution from every country; also, contributions from outside the traditional Formal Methods community were solicited. The recent innovation of including an Industrial Day as an important part of the symposium shows the strong commitment to involve industrial people more and more within the Formal Methods community. Even the traditional and rather fuzzy borderline between “software engineering formal methods” and methods and formalisms exploited in different fields of engineering was somewhat challenged. This is in recognition of the increasing need to look at and to understand systems (often hybrid systems) in their entirety: something that should have a higher priority than focusing on the specific software issues that in most cases just relate to a component of the whole system.

All in all we can claim to have made significant steps towards our goal of widening our scope, although, certainly, many challenges are still open. In particular, we were very happy with the paper submissions: 144 papers were submitted from 27 countries of all continents. Submitted papers were of both theoretical and applicative nature, and were overall of high quality. Not only were the 44 accepted papers selected according to our traditional high standards, but the Program Committee board also recognized significant potential contributions in many papers that had to be rejected, mostly due to their fairly preliminary development stage. Four of the 44 accepted papers were selected for presentation during the Industry Day. Besides the refereed papers, these proceedings include contributions from the following invited speakers: Kouichi Kishida, Brian Randell, Gerard Holzmann, and Jean-Raymond Abrial. Finally, we emphasize the importance and quality of numerous satellite events: besides the Industry Day, eight tutorials, seven workshops, and a rich tool fair completed the program of the symposium. Enjoy reading!

September 2003 Keijiro Araki, Stefania Gnesi and Dino Mandrioli
Organization

FM 2003 was organized by Formal Methods Europe, the Institute for Informatics Science and Technology (ISTI) of the National Research Council of Italy, and CoLogNet.

Conference Chairs

General Chair
Stefania Gnesi (ISTI-CNR, I)

Program Co-chairs
Keijiro Araki (Kyushu University, J)
Dino Mandrioli (Politecnico di Milano, I)

Organizing Committee Chair
Alessandro Fantechi (Università di Firenze, I)

Publicity Chair
Vinícius Lami (ISTI-CNR, I)

Tool Exhibition Chair
Tiziana Margaria (Universität Dortmund, and Metaframe, D)

Tutorials Chair
Mieke Massink (ISTI-CNR, I)

Workshops Chair
Tommaso Bolognesi (ISTI-CNR, I)

Program Committee

Dominique Bolignano
Trusted Logic, France

Jonathan Bowen
South Bank Univ., London, UK

Lubos Brim
Masaryk Univ., Brno, Czech Republic

Han-Myung Chang
Nanzan Univ., Japan

Krzysztof Czarnecki
DaimlerChrysler Research Lab, Germany

Lars-Henrik Eriksson
Uppsala Univ., Sweden

Jose Fiadeiro
Leicester Univ., UK

John Fitzgerald
Transitive Technologies Ltd., UK

Kokichi Futatsugi
JAIST, Japan

Chris George
UNU/IIST, Macao

Connie Heitmeyer
NRL, USA

Shusaku Iida
Senshu Univ., Japan

Mehdi Jazayeri
Technical Univ., Vienna, Austria

Kyo-Chul Kang
POSTECH, Korea

Shmuel Katz
Technion, Israel

Shigeru Kusakabe
Kyushu Univ., Japan

Diego Latella
ISTI-CNR, Pisa, Italy

Yves Ledru
IMAG Grenoble, France

Raimondas Lencevicius
Nokia, USA

Peter Lindsay
Queensland Univ., Australia

Shaoying Liu
Hosei Univ., Japan

Peter Löhr
Freie Univ., Berlin, Germany
Tom Maibaum  
King’s College London, UK

Huaikou Miao  
Shanghai Univ., China

Nico Plat  
West Consulting, The Netherlands

Harald Ruess  
SRI, USA

Shin Sahara  
JFITS, Japan

Pierluigi San Pietro  
Politecnico di Milano, Italy

Jim Woodcock  
Kent Univ., Canterbury, UK

Pamela Zave  
AT&T Labs, USA

External Referees

The Program Committee members and the external referees listed below did an excellent job in managing an unexpectedly high number of submissions under the usual pressure of strict deadlines. All papers were refereed by at least three reviewers. Reports were thorough, detailed, and rich with constructive suggestions even when rejection was recommended. Both PC members and external referees further contributed to the active and intense “e-discussion” that led to the final decision. We are very happy to acknowledge such a superb contribution to the quality of these proceedings.

Referees

Nazareno Aguirre  
Antonio Cerone  
Roland Groz

Bernhard K. Aicherning  
Yihai Chen  
Orna Grumberg

Myla Archer  
Judy Crow  
Stefan Gruner

James M. Armstrong  
Giampaolo Cugola  
Gregoire Hamon

Jos Baeten  
Paul Curzon  
Ian Hayes

Luciano Baresi  
David Cyrluk  
Simon Helsen

Jiri Barnat  
Zhe Dang  
John Herbert

Maurice ter Beek  
Leonardo de Moura  
Michael G. Hinchey

Saddek Bensalem  
Lydie du Bousquet  
Zhu Huibiao

Neil Bergmann  
Sophie Dupuy  
Ralph D. Jeffords

Pierre Berlioux  
Adolfo Duran  
He Jifeng

Roxane Bernier  
Giorgio Faconti  
Cliff Jones

Didier Bert  
Alessandro Fantechi  
Joost-Pieter Katoen

Denis Besnard  
Loe Feijs  
Clemens Kerer

Gustavo Betarte  
Pascal Fenkm  
James Kirby

Ramesh Bharadwaj  
Jean-Claude Fernandez  
Manuel Koch

Jonathan Billington  
M.J. Fernández Iglesias  
Andre Koster

Tommaso Bolognesi  
Colin Fidge  
Vishnu Kotrajaras

Sylvain Boulmé  
Torsten Fink  
Pavel Krcal

Juan C. Burguillos Rial  
Leonardo Freitas  
Mojmir Kretinsky

Ana Cavalcanti  
Eduardo Gimenez  
G. Kwon

Ivana Cerna  
Jan Friso Groote  
Regine Laleau
Sponsoring Institutions

Formal Methods Europe
www.fmeurope.org

ISTI-CNR
www.isti.cnr.it

CoLogNET
www.eurice.de/colognet

Ercim
www.ercim.org

Microsoft
www.microsoft.com

TESS-COM Italia s.r.l.
www.tess-com.it

Telelogic
www.telelogic.com

EPSON
www.epson.com

Metaframe
www.metaframe.de

DataPort
www.dataport.it
Table of Contents

Invited Speakers

Looking Back to the Future ................................................. 1
  Kouichi Kishida

Past, Present, and Future of SRA Implementation of CafeOBJ (Annex) ... 7
  Toshimi Sawada, Kouichi Kishida, Kokichi Futatsugi

On Failures and Faults .................................................... 18
  Brian Randell

Trends in Software Verification ........................................... 40
  Gerard J. Holzmann

Event Based Sequential Program Development:
Application to Constructing a Pointer Program ....................... 51
  Jean-Raymond Abrial

I-Day

Proving the Shalls ....................................................... 75
  Steven P. Miller, Alan C. Tribble, Mats P.E. Heimdahl

Adaptable Translator of B Specifications to Embedded C Programs ...... 94
  Didier Bert, Sylvain Boulmé, Marie-Laure Potet,
  Antoine Requet, Laurent Voisin

Integrating Model-Checking Architectural Analysis and Validation
in a Real Software Life-Cycle ............................................ 114
  Daniele Compare, Paola Inverardi,
  Patrizio Pelliccione, Alessandra Sebastiani

Lessons Learned from a Successful Implementation of Formal Methods
in an Industrial Project .................................................. 133
  Alan Wassyng, Mark Lawford

Control Systems and Industrial Applications

Determining the Specification of a Control System
from That of Its Environment ........................................... 154
  Ian J. Hayes, Michael A. Jackson, Cliff B. Jones
Managerial Issues for the Consideration and Use of Formal Methods ...... 170
  Donna C. Stidolph, James Whitehead

Verifying Emulation of Legacy Mission Computer Systems ............... 187
  Colin J. Fidge

Improving Safety Assessment of Complex Systems:
  An Industrial Case Study .......................................................... 208
  Marco Bozzano, Antonella Cavallo, Massimo Cifaldi, Laura Valacca,
  Adolfo Villafiorita

Communications System Verification

  Compositional Verification of an ATM Protocol .......................... 223
    Vlad Rusu

  Proving the Correctness of Simpson’s 4-Slot ACM
  Using an Assertional Rely-Guarantee Proof Method ...................... 244
    Neil Henderson

  Synthesis and Verification of Constraints in the PGM Protocol ....... 264
    Marc Boyer, Mihaela Sighireanu

Co-specification and Compilers

  Mapping Statecharts to Verilog for Hardware/Software Co-specification . 282
    Shengchao Qin, Wei-Ngan Chin

  A Strategy for Compiling Classes, Inheritance, and Dynamic Binding ... 301
    Adolfo Duran, Ana Cavalcanti, Augusto Sampaio

Composition

  A Semantic Foundation for TCOZ in Unifying Theories of Programming . 321
    Shengchao Qin, Jin Song Dong, Wei-Ngan Chin

  Refinement and Verification of Synchronized Component-Based Systems . 341
    Olga Kouchnarenko, Arnaud Lanoix

  Certifying and Synthesizing Membership Equational Proofs ............. 359
    Grigore Roşu, Steven Eker, Patrick Lincoln, José Meseguer

  Team Automata Satisfying Compositionality .............................. 381
    Maurice H. ter Beek, Jetty Kleijn

  Composing Invariants ...................................................... 401
    Michel Charpentier
Java, Object Orientation and Modularity

Java Applet Correctness: A Developer-Oriented Approach ................. 422
   Lilian Burdy, Antoine Requet, Jean-Louis Lanet

Improving JML: For a Safer and More Effective Language ............... 440
   Patrice Chalin

Using Abstractions for Heuristic State Space Exploration
of Reactive Object-Oriented Systems ................................... 462
   Marc Lettrari

A Formal Framework for Modular Synchronous System Design .......... 482
   Maria-Cristina V. Marinescu, Martin C. Rinard

Model Checking

Generating Counterexamples for Multi-valued Model-Checking .......... 503
   Arie Gurfinkel, Marsha Chechik

Combining Real-Time Model-Checking and Fault Tree Analysis .......... 522
   Andreas Schäfer

Model-Checking TRIO Specifications in SPIN .......................... 542
   Angelo Morzenti, Matteo Pradella, Pierluigi San Pietro, Paola Spoletini

Computing Meta-transitions
for Linear Transition Systems with Polynomials ....................... 562
   Julien Musset, Michaël Rusinowitch

Translation-Based Compositional Reasoning for Software Systems ...... 582
   Fei Xie, James C. Browne, Robert P. Kurshan

Watchdog Transformations for Property-Oriented Model-Checking ...... 600
   Michael Goldsmith, Nick Moffat, Bill Roscoe,
   Tim Whitworth, Irfan Zakiuddin

Parallel Process

A Circus Semantics for Ravenscar Protected Objects .................... 617
   Diyaa-Addein Atiya, Steve King, Jim C.P. Woodcock

Constructing Deadlock Free Event-Based Applications:
A Rely/Guarantee Approach ............................................. 636
   Pascal Fenkam, Harald Gall, Mehdi Jazayeri
# Table of Contents

A General Approach to Deadlock Freedom Verification for Software Architectures ........................................... 658  
*Alessandro Aldini, Marco Bernardo*

Taking *Alloy* to the Movies ........................................ 678  
*Marcelo F. Frias, Carlos G. López Pombo, Gabriel A. Baum, Nazareno M. Aguirre, Tom Maibaum*

Interacting State Machines for Mobility ............................ 698  
*Thomas A. Kuhn, David von Oheimb*

Composing Temporal-Logic Specifications with Machine Assistance ........ 719  
*Jei-Wen Teng, Yih-Kuen Tsay*

## Program Checking and Testing

Model Checking FTA .................................................. 739  
*Andreas Thums, Gerhard Schellhorn*

Program Checking with Certificates: Separating Correctness-Critical Code 758  
*Sabine Glesner*

Reification of Executable Test Scripts in Formal Specification-Based Test Generation: The Java Card Transaction Mechanism Case Study ..... 778  
*Fabrice Bouquet, Bruno Legeard*

Checking and Reasoning about Semantic Web through *Alloy* ........... 796  
*Jin Song Dong, Jing Sun, Hai Wang*

## B Method

Structuring Retrenchments in B by Decomposition ................. 814  
*Michael Poppleton, Richard Banach*

Design of an Automatic Prover Dedicated to the Refinement of Database Applications ........................... 834  
*Amel Mammar, Régine Laleau*

ProB: A Model Checker for B ........................................ 855  
*Michael Leuschel, Michael Butler*

## Security

SAT-Based Model-Checking of Security Protocols Using Planning Graph Analysis ........................................ 875  
*Alessandro Armando, Luca Compagna, Pierre Ganty*
Correctness of Source-Level Safety Policies .............................. 894
   *Ewen Denney, Bernd Fischer*

A Topological Characterization of TCP/IP Security ....................... 914
   *Giovanni Vigna*

**Author Index** ................................................................. 941