

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

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*

Madhu Sudan

*Microsoft Research, Cambridge, MA, USA*

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*

John Derrick Stefania Gnesi  
Diego Latella Helen Treharne (Eds.)

# Integrated Formal Methods

9th International Conference, IFM 2012  
Pisa, Italy, June 18-21, 2012  
Proceedings

Volume Editors

John Derrick  
University of Sheffield  
Department of Computer Science  
Regent Court, 211 Portobello Street  
Sheffield S1 4DP, UK  
E-mail: j.derrick@dcs.shef.ac.uk

Stefania Gnesi  
Diego Latella  
Consiglio Nazionale delle Ricerche  
Istituto di Scienza e Tecnologie dell'Informazione "A. Faedo"  
Via Moruzzi 1  
56124 Pisa, Italy  
E-mail: {stefania.gnesi; diego.latella@isti.cnr.it}

Helen Treharne  
University of Surrey  
Department of Computing  
Surrey GU2 7XH, UK  
E-mail: h.treharne@surrey.ac.uk

ISSN 0302-9743  
ISBN 978-3-642-30728-7  
DOI 10.1007/978-3-642-30729-4  
Springer Heidelberg Dordrecht London New York

e-ISSN 1611-3349  
e-ISBN 978-3-642-30729-4

Library of Congress Control Number: 2012939244

CR Subject Classification (1998): D.2, F.3, D.3, D.2.4, F.4.1, D.1

LNCS Sublibrary: SL 2 – Programming and Software Engineering

© Springer-Verlag Berlin Heidelberg 2012

This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, re-use of illustrations, recitation, broadcasting, reproduction on microfilms or in any other way, and storage in data banks. Duplication of this publication or parts thereof is permitted only under the provisions of the German Copyright Law of September 9, 1965, in its current version, and permission for use must always be obtained from Springer. Violations are liable to prosecution under the German Copyright Law.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

*Typesetting:* Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

# Foreword

iFM 2012, the 9th International Conference on Integrated Formal Methods, and ABZ 2012, the 3rd International Conference on Abstract State Machines, Alloy, B, VDM, and Z, were joined in a single event, iFM&ABZ 2012, to celebrate Egon Börger's 65th birthday and his contribution to state-based formal methods.

This colocation of iFM&ABZ 2012 was hosted by the Institute of Scienza e Tecnologie dell'Informazione "A. Faedo" of the National Research Council (ISTI-CNR) of Italy and took place at the Area della Ricerca del CNR in Pisa, during June 18–21, 2012.

We would like to thank everyone in Pisa for making us feel very welcome during our time there. It was a pleasure to run an event to honor Egon.

Professor Egon Börger was born in Bad Laer, Lower Saxony, Germany. Between 1965 and 1971 he studied at the Sorbonne, Paris (France), Université Catholique de Louvain and Institut Supérieur de Philosophie de Louvain (in Louvain-la-Neuve, Belgium), and the University of Münster (Germany). Since 1985 he has held a Chair in computer science at the University of Pisa, Italy. In September 2010 he was elected as member of the Academia Europaea. Throughout his work he has been a pioneer of applying logical methods in computer science. Particularly notable is his contribution as one of the founders of the Abstract State Machine (ASM) method. Egon Börger has been cofounder and Managing Director of the Abstract State Machines Research Center (see [www.asmcenter.org](http://www.asmcenter.org)).

Building on his work on ASM, he was a cofounder of the series of international ASM workshops, which were part of this year's conference under the ABZ banner. He contributed to the theoretical foundations of the method and initiated its industrial applications in a variety of fields, in particular programming languages, system architecture, requirements and software (re-)engineering, control systems, protocols and Web services. In 2007, he received the Humboldt Research Award.

He has been coauthor of several books and over 150 research papers; he has organized over 30 international conferences, workshops, schools in logic and computer science.

As one can see, his influence has been broad as well as deep. It is an influence that ones finds in all of the notations covered in the ABZ conference, as well as in the iFM event and the various integrations and combinations of formal methods seen therein. Neither iFM or ABZ have been here before, and it is thus especially fitting that we held such an event in Pisa, where Egon has held a Chair for many years.

In addition to contributed papers, the conference programme included two tutorials and three keynote speakers. The tutorials were offered by: Eric C.R. Hehner on “Practical Predicative Programming Primer” and Joost-Pieter Katoen, Thomas Noll, Alessandro Cimatti and Marco Bozzano on “Safety, Dependability and Performance Analysis of Extended AADL Models.” We are grateful to Egon Börger, Muffy Calder and Ian J. Hayes for accepting our invitation to address the conference.

Each conference, ABZ and iFM, had its own Programme Committee Chairs and Programme Committees, and we leave it to them to describe their particular conference. We shared invited speakers, so all conference attendees had the opportunity to hear Egon, Muffy and Ian. We also shared some technical sessions so that all participants could see some of the best technical work from each conference.

We would like to thank the Programme Committee Chairs, Diego Latella, CNR/ ISTI, Italy and Helen Treharne, University of Surrey, UK for iFM 2012; Steve Reeves, University of Waikato, New Zealand and Elvinia Riccobene, University of Milan, Italy for ABZ 2012 for their efforts in setting up two high-quality conferences.

We also would like to thank the members of the Organizing Committee as well as several other people whose efforts contributed to making the conference a success and particular thanks go to the Organizing Committee Chair Maurice ter Beek.

June 2012

John Derrick  
Stefania Gnesi

# Preface

This volume contains the proceedings of iFM 2012, the 9th International Conference on Integrated Formal Methods, held during June 18–21, 2012, in Pisa, Italy, jointly with ABZ 2012, the 3rd International Conference on Abstract State Machines, Alloy, B, VDM, and Z, in honor of Egon Börger’s 65th birthday. The ABZ proceedings appear as a separate LNCS volume, number 7316. The invited talk of Egon Börger appears in both proceedings.

The iFM conference programme also included an invited talk by Muffy Calder and the ABZ conference programme included an invited talk by Ian Hayes.

Previous iFM conferences were held in York, Dagstuhl, Turku, Canterbury, Eindhoven, Oxford, Düsseldorf and Nancy. The iFM conference series seeks to further research into the combination of different formal methods for modelling and analysis. However, the work of iFM goes beyond that, covering all aspects from language design, verification techniques, tools and the integration of formal methods into software engineering practice.

iFM 2012 received 59 submissions, covering the spectrum of integrated formal methods, ranging across formal and semi-formal modelling notations, semantics, proof frameworks, refinement, verification, timed systems, tools and case studies. Each submission was reviewed by at least three Programme Committee members. The committee decided to accept 22 papers.

The conference was preceded by a day dedicated to tutorials on “Practical Predicative Programming Primer” by Eric C. R. Hehner and “Safety, Dependability and Performance Analysis of Extended AADL Models” by Joost-Pieter Katoen, Thomas Noll, Alessandro Cimatti and Marco Bozzano.

We are grateful to the members of the Programme Committee and the external reviewers for their diligence and thoroughness. We also appreciate the support of EasyChair for managing the reviewing process and the preparation of the proceedings. We thank all those involved in organizing the conference and an important note of thanks must be extended to the members of CNR who helped locally.

June 2012

Diego Latella  
Helen Treharne

# Organization

## General Chairs

John Derrick	University of Sheffield, UK
Stefania Gnesi	CNR/ISTI, Italy

## Conference Chairs

Diego Latella	CNR/ISTI, Italy
Helen Treharne	University of Surrey, UK

## Programme Committee

Marc Benveniste	STMICROELECTRONICS, France
Eerke Boiten	University of Kent, UK
Jonathan P. Bowen	MUSEOPHILE LIMITED, UK
Jim Davies	University of Oxford, UK
John Derrick	University of Sheffield, UK
Jin Song Dong	National University of Singapore, Singapore
Kerstin Eder	University of Bristol, UK
Alessandro Fantechi	University of Florence and CNR/ISTI, Italy
John Fitzgerald	Newcastle University, UK
Andy Galloway	University of York, UK
Einar Broch Johnsen	University of Oslo, Norway
Rajeev Joshi	NASA Jet Propulsion Laboratory (JPL), USA
Michael Leuschel	University of Düsseldorf, Germany
Michele Loreti	University of Florence, Italy
Silvia Mazzini	Intecs S.p.A, Italy
Dominique Mery	LORIA and Université de Lorraine, France
Stephan Merz	INRIA Nancy and LORIA, France
Alexandre Mota	Centre of Informatics (CIn-UFPE), Brazil
Flemming Nielson	Technical University of Denmark and MT-LAB, Denmark
Luigia Petre	Åbo Akademi University, Finland
David Pichardie	INRIA Rennes, France
Thomas Santen	European Microsoft Innovation Center, Germany
Steve Schneider	University of Surrey, UK
Kaisa Sere	Åbo Akademi University, Finland
Graeme Smith	University of Queensland, Australia
Kenji Taguchi	National Institute of Advanced Industrial Science and Technology, Japan

Mirco Tribastone  
Marina Waldén  
Heike Wehrheim  
Kirsten Winter

Ludwig-Maximilians-Universität, Germany  
Åbo Akademi University, Finland  
University of Paderborn, Germany  
University of Queensland, Australia

## Additional Reviewers

Islam Abdel Halim  
Étienne André  
Emilie Balland  
Sebastien Bardin  
Cristiano Bertolini  
Lorenzo Bettini  
Irene Bicchierai  
Jean-Paul Bodeviex  
Carl Friedrich Bolz  
Pontus Boström  
Jeremy W. Bryans  
Laura Carnevali  
Márcio Cornélio  
Fredrik Degerlund  
Delphine Demange  
Andre Didier  
Johan Dovland  
Neil Evans  
Marc Fontaine

Carl Gamble  
Juliano Iyoda  
Mohammad Mahdi  
Jaghoori  
Maryam Kamali  
Weiqiang Kong  
Linus Laibinis  
Shang-Wei Lin  
Alberto Lluch Lafuente  
Acciai Lucia  
Toby Murray  
Keishi Okamoto  
Richard Payne  
Stefano Pepi  
Ken Pierce  
Steve Riddle  
Petter Sandvik  
Rudolf Schlatte  
Alexander Schremmer

Ling Shi  
Mihaela Sighireanu  
Tarciana Silva  
Neeraj-Kumar Singh  
Songzheng Song  
Dominik Steenzen  
Volker Stolz  
Anton Tarasyuk  
Maurice ter Beek  
Francesco Tiezzi  
Max Tschaikowski  
Leonidas Tsiopoulos  
Sven Walther  
Daniel Wonisch  
Yoriyuki Yamagata  
Shaojie Zhang  
Manchun Zheng  
Steffen Ziegert

## Sponsoring Institutions

A final note of appreciation to our sponsors:



INTECS  
S.p.A.



Formal Methods  
Europe



**BNL**  
GRUPPO BNP PARIBAS

Banca Nazionale del Lavoro  
S.p.A.



European Association for  
Theoretical Computer Science  
Italian Chapter

EATCS  
Italian Chapter

We particularly would like to thank *Formal Methods Europe* (FME), since it is due to their generous support that were able to invite Muffy Calder for a keynote presentation.



# Table of Contents

Contribution to a Rigorous Analysis of Web Application Frameworks . . .	1
<i>Egon Börger, Antonio Cisternino, and Vincenzo Gervasi</i>	
Process Algebra for Event-Driven Runtime Verification: A Case Study of Wireless Network Management . . . . .	21
<i>Muffy Calder and Michele Sevegnani</i>	
Translating TLA <sup>+</sup> to B for Validation with PROB . . . . .	24
<i>Dominik Hansen and Michael Leuschel</i>	
Rely/Guarantee Reasoning for Teleo-reactive Programs over Multiple Time Bands . . . . .	39
<i>Brijesh Dongol and Ian J. Hayes</i>	
Safety and Line Capacity in Railways – An Approach in Timed CSP . . .	54
<i>Yoshinao Isobe, Faron Moller, Hoang Nga Nguyen, and Markus Roggenbach</i>	
Refinement-Based Development of Timed Systems . . . . .	69
<i>Jesper Berthing, Pontus Boström, Kaisa Sere, Leonidas Tsiopoulos, and Jüri Vain</i>	
Analysing and Closing Simulation Coverage by Automatic Generation and Verification of Formal Properties from Coverage Reports . . . . .	84
<i>Tim Blackmore, David Halliwell, Philip Barker, Kerstin Eder, and Naresh Ramaram</i>	
Model Checking as Static Analysis: Revisited . . . . .	99
<i>Fuyuan Zhang, Flemming Nielson, and Hanne Riis Nielson</i>	
Formal Verification of Compiler Transformations on Polychronous Equations . . . . .	113
<i>Van Chan Ngo, Jean-Pierre Talpin, Thierry Gautier, Paul Le Guernic, and Loïc Besnard</i>	
Understanding Programming Bugs in ANSI-C Software Using Bounded Model Checking Counter-Examples . . . . .	128
<i>Herbert Rocha, Raimundo Barreto, Lucas Cordeiro, and Arilo Dias Neto</i>	
MULE-Based Wireless Sensor Networks: Probabilistic Modeling and Quantitative Analysis . . . . .	143
<i>Fatemeh Kazemeyni, Einar Broch Johnsen, Olaf Owe, and Ilanko Balasingham</i>	

Mechanized Extraction of Topology Anti-patterns in Wireless Networks . . . . .	158
<i>Matthias Woehrle, Rena Bakhshi, and Mohammad Reza Mousavi</i>	
A Proof Framework for Concurrent Programs . . . . .	174
<i>Leonard Lensink, Sjaak Smetsers, and Marko van Eekelen</i>	
A UTP Semantics of pGCL as a Homogeneous Relation . . . . .	191
<i>Riccardo Bresciani and Andrew Butterfield</i>	
Behaviour-Based Cheat Detection in Multiplayer Games with Event-B . . . . .	206
<i>HaiYun Tian, Phillip J. Brooke, and Anne-Gwenn Bosser</i>	
Refinement-Preserving Translation from Event-B to Register-Voice Interactive Systems . . . . .	221
<i>Denisa Diaconescu, Ioana Leustean, Luigia Petre, Kaisa Sere, and Gheorghe Stefanescu</i>	
Formal Modelling and Verification of Service-Oriented Systems in Probabilistic Event-B . . . . .	237
<i>Anton Tarasyuk, Elena Troubitsyna, and Linas Laibinis</i>	
Partially-Supervised Plants: Embedding Control Requirements in Plant Components . . . . .	253
<i>Jasen Markovski, Dirk A. van Beek, and Jos Baeten</i>	
Early Fault Detection in Industry Using Models at Various Abstraction Levels . . . . .	268
<i>Jozef Hooman, Arjan J. Mooij, and Hans van Wezep</i>	
PE-KeY: A Partial Evaluator for Java Programs . . . . .	283
<i>Ran Ji and Richard Bubel</i>	
Specification-Driven Unit Test Generation for Java Generic Classes . . . . .	296
<i>Francisco Rebello de Andrade, João P. Faria, Antónia Lopes, and Ana C.R. Paiva</i>	
Specifying UML Protocol State Machines in Alloy . . . . .	312
<i>Ana Garis, Ana C.R. Paiva, Alcino Cunha, and Daniel Riesco</i>	
Patterns for a Log-Based Strengthening of Declarative Compliance Models . . . . .	327
<i>Dennis M.M. Schunselaar, Fabrizio Maria Maggi, and Natalia Sidorova</i>	
A Formal Interactive Verification Environment for the Plan Execution Interchange Language . . . . .	343
<i>Camilo Rocha, Héctor Cadavid, César Muñoz, and Radu Siminiceanu</i>	
<b>Author Index . . . . .</b>	<b>359</b>