Lecture Notes in Computer Science 2999

Edited by G. Goos, J. Hartmanis, and J. van Leeuwen

Springer
*Berlin*
*Heidelberg*
*New York*
*Hong Kong*
*London*
*Milan*
*Paris*
*Tokyo*

Eerke A. Boiten John Derrick
Graeme Smith (Eds.)

# Integrated Formal Methods

4th International Conference, IFM 2004
Canterbury, UK, April 4-7, 2004
Proceedings

Springer

Volume Editors

Eerke A. Boiten
John Derrick
University of Kent
Computing Laboratory
Canterbury, Kent, CT2 7NF, UK
E-mail:{E.A.Boiten/J.Derrick}@kent.ac.uk

Graeme Smith
University of Queensland
School of Information Technology and Electrical Engineering
4072 Brisbane, Australia
E-mail: smith@itee.uq.edu.au

Library of Congress Control Number: 2004102974

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

ISSN 0302-9743
ISBN 3-540-21377-5 Springer-Verlag Berlin Heidelberg New York



Typesetting: Camera-ready by author, data conversion by PTP-Berlin, Protago-TeX-Production GmbH
Printed on acid-free paper SPIN: 10992623 06/3142 5 4 3 2 1 0

# Preface

The fourth conference in the series of international meetings on Integrated Formal Methods, IFM, was held in Canterbury, UK, 4–7 April 2004. The conference was organized by the Computing Laboratory at the University of Kent, whose main campus is just outside the ancient town of Canterbury, part of the county of Kent.

Kent is situated in the southeast of England, and the university sits on a hill overlooking the city of Canterbury and its world-renowned cathedral. The University of Kent was granted its Royal Charter in 1965. Today there are almost 10,000 full-time and part-time students, with over 110 nationalities represented.

The IFM meetings have proven to be particularly successful. The first meeting was held in York in 1999, and subsequently we held events in Germany in 2000, and then Finland in 2002. The conferences are held every 18 months or so, and attract a wide range of participants from Europe, the Americas, Asia and Australia. The conference is now firmly part of the formal methods conference calendar. The conference has also evolved in terms of themes and subjects represented, and this year, in line with the subject as a whole, we saw more work on verification as some of the challenges in this subject are being met.

The work reported at IFM conferences can be seen as part of the attempt to manage complexity by combining paradigms of specification and design, so that the most appropriate design tools are used at different points in the life-cycle. In part this is about combining specification formalisms, and this happens, for example, when one combines state-based and event-based languages to produce integrated notations capable of covering a wider range of the design spectrum than would otherwise be feasible. However, the work of IFM goes beyond that, as we can see in this proceedings.

Indeed, increasingly specification is only the start of a process that includes verification as an explicit aim, and this work was heavily represented in this year's conference. This was also reflected in the talks by invited speakers who represented both academic and industry perspectives on the subject.

Tom Ball talked about his team's work on SLAM and the static driver verifier, and described the use of formal methods in Microsoft. Ursula Martin, of Queen Mary, University of London, talked about her work on design verification for control engineering, and Tom Melham of Oxford gave a talk entitled "Integrating Model Checking and Theorem Proving in a Reflective Functional Language." Tom Ball's talk was sponsored by FME (Formal Methods Europe), to whom we are particularly grateful. FME also held their Annual General Meeting on the Sunday prior to the main conference. We are also grateful to Jim Woodcock for agreeing to give a tutorial on the Unifying Theories of Programming, jointly with Ana Cavalcanti. FORTEST, a UK national network on Formal Methods and Testing, also joined us for the final day when members attended talks on testing and then held an informal workshop after the main conference.

The contributed talks were grouped into a number of sessions, this year covering:

- Automating program analysis
- State-/event-based verification
- Formalizing graphical notations
- Refinement
- Object orientation
- Hybrid and timed automata
- Integration frameworks
- Verifying interactive systems
- Testing and assertions

In total there were 65 submissions, of which we accepted 24 after the usual refereeing process. We are grateful to all those involved in the reviewing process and subsequent programme committee discussion. An important note of thanks must also be given to all those who helped locally.

We hope that these proceedings will serve as a useful source of reference for not only the attendees, but also the wider community. We look forward to further IFM meetings where we can continue the discussion on the best ways to engineer both hardware and software systems with the ultimate aim of increased reliability and robustness.

April 2004

Eerke Boiten
John Derrick
Graeme Smith

## Program Committee

Didier Bert (France)
Eerke Boiten (Co-chair, UK)
Jonathan Bowen (UK)
Michael Butler (UK)
Paul Curzon (UK)
Jim Davies (UK)
John Derrick (Co-chair, UK)
Jin Song Dong (Singapore)
John Fitzgerald (UK)
Andrew Galloway (UK)
Chris George (Macau)
Wolfgang Grieskamp (US)
Henri Habrias (France)
Susumu Hayashi (Japan)
Maritta Heisel (Germany)
Michel Lemoine (France)
Shaoying Liu (Japan)
Dominique Méry (France)
Luigia Petre (Finland)
Judi Romijn (The Netherlands)
Thomas Santen (Germany)
Steve Schneider (UK)
Wolfram Schulte (US)
Kaisa Sere (Finland)
Jane Sinclair (UK)
Graeme Smith (Co-chair, Australia)

Bill Stoddart (UK)
Kenji Taguchi (UK)
W.J. (Hans) Toetenel (The Netherlands)
Heike Wehrheim (Germany)
Kirsten Winter (Australia)
Jim Woodcock (UK)

## Sponsors

In addition to FME sponsorship of an invited talk, we are grateful to BCS FACS (the Formal Aspects of Computing Science Specialist Group of the British Computer Society, http://www.bcs.org.uk/) for sponsoring the best paper award.


## 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 conference would lose its quality status. To the best of our knowledge the list below is accurate. We apologize for any omissions or inaccuracies.

Bernhard K. Aichernig
Marcus Alanen
Pascal André
Jim Armstrong
Mike Barnett
Gerd Behrmann
Dag Björklund
Victor Bos
Pontus Boström
Sylvain Boulmé
Robert Büssow
Ana Cavalcanti
Orieta Celiku
Christine Choppy
Corina Cirstea
Dang Van Hung
Henning Dierks
Roger Duke
Steve Dunne
Neil Evans
Li Yuan Fang
Ansgar Fehnker
Leonardo Freitas
Biniam Gebremichael
Michael Goldsmith
Andy Gravell
Stefan Hallerstede
Ian Hayes
Steffen Helke
Jon Jacky
Nigel Jefferson
Sara Kalvala
Maciej Koutny
Yves Ledru
Hui Liang
Zhiming Liu
Stephan Merz
Pierre Michel
Arjan J. Mooij
MohammadReza Mousavi
Catherine Oriat
Stephen Paynter
Maria Pietkiewicz-Koutny
Juha Plosila
Pascal Poizat
Mike Poppleton
Ivan Porres
Marie-Laure Potet
Viorel Preoteasa
Arend Rensink
Steve Riddle
Michael Rusinowitch
Gwen Salaün
Cristina Seceleanu
Dirk Seifert
Colin Snook
Mariëlle Stoelinga
Cedric Stoquer
Carsten Sühl
Jun Sun
Xinbei Tang
Nikolai Tillmann
Helen Treharne
Leonidas Tsiopoulos
Margus Veanes
Sergiy Vilkomir
Marina Waldén

Hai Wang
Virginie Wiels
Hirokazu Yatsu
Volker Zerbe
Frank Zeyda
Andrea Zisman
Steffen Zschaler

# Table of Contents

## Invited Talks



## Tutorial



## Contributed Papers