Lecture Notes in Computer Science 1051
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

Advisory Board: W. Brauer D. Gries J. Stoer

Marie-Claude Gaudel James Woodcock (Eds.)

FME'96: Industrial Benefit and Advances in Formal Methods

Third International Symposium
of Formal Methods Europe
Co-Sponsored by IFIP WG 14.3
Oxford, UK, March 18-22, 1996
Proceedings

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany

Juris Hartmanis, Cornell University, NY, USA

Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

Marie-Claude Gaudel
Laboratoire de Recherche en Informatique, Université de Paris-Sud et CNRS
Bâtiment 490, F-91405 Orsay-cedex, France

James Woodcock
Computing Laboratory, Oxford University
Wolfson Building, Parks Road, Oxford OX1 3QD, United Kingdom

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Industrial benefit and advances in formal methods : proceedings / FME '96, Third International Symposium of Formal Methods Europe, Oxford, UK, March 1996. Marie-Claude Gaudel ; James Woodcock (ed.). Co-sponsored by IFIP WG 14.3. - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo : Springer, 1996
(Lecture notes in computer science ; Vol. 1051)
ISBN 3-540-60973-3
NE: Gaudel, Marie-Claude [Hrsg.]; FME <3, 1996, Oxford>; GT

CR Subject Classification (1991): D.1-2, D.3.1,F.3.1, J.1

ISBN 3-540-60973-3 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN 10512716 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Preface

This volume contains the proceedings of the Third Formal Method Europe Symposium. This series of Symposia aims to promote the interests of users, researchers, and developers of precise mathematical methods in software development, and to report advances in this field.

The FME Symposia are the successors of the four VDM symposia organised by "VDM Europe", an advisory board sponsored by the Commission of the European Union. After the last VDM symposium, VDM Europe became "Formal Methods Europe", with the mission of supporting the industrial use of formal methods for computer systems development. The first FME symposium was held in Odensee in April 1993, the second in Barcelona in September 1994; the scope of these symposia, which had already been widened to include Z, was extended to include all formal methods of software development.

This is emphasized this time by the fact that this symposium is co-sponsored by the IFIP Working Group 14.3 "Foundations of Systems Specifications", a recently created group which mainly works in the area of algebraic specifications.

FME'96 is being held at St Hugh's College in Oxford from 18 to 22 March 1996.

Like the previous FME symposia, this one focuses on industrial applicability. Its theme is *The Application and Demonstrated Industrial Benefit of Formal Methods, Their New Horizons and Strengthened Foundations*. Accordingly, three kinds of paper were solicited: reports on industry usage, research papers on existing methods (for instance extensions, innovative case studies, ...), and articles on stimulating theoretical research with strong potential applications.

Over the last few years, the use of formal methods has significantly progressed. These proceedings contain descriptions of applications to numerous and important areas: information systems, medical systems, aerospace and avionics, nuclear safety, energy, telecommunications, traffic modeling and transportation systems, etc.

103 papers were submitted, from 20 countries; 35 of them were accepted, roughly 8 on industry usage, 21 on existing methods, and 6 on theoretical research (some papers should be in two categories, thus these figures are not completely accurate). As can be seen in the following table of contents, the addressed topics cover the main existing methods plus several important and general problems such as: the role of formal methods in requirement analysis, user interfaces for formal methods, performance analysis, fault-tolerance, testing, reuse, and transformations.

The invited speakers are C.A.R. Hoare, from Oxford University, Terje Siversten, from the OECD Halden Reactor Project in Norway, and Jan Peleska, from JP Software-Consulting and the University of Bremen, reflecting the scope of the symposium, from foundations to industrial applications.

Moreover, the symposium will include 8 tutorials, some poster sessions, and an exhibition of formal-method tools.

The program committee of FME'96 is as follows: Egidio Astesiano*, Dominique Bolignano*, Gottfried Egger*, Hartmut Ehrig, Marie-Claude Gaudel*, René Jacquart*, Cliff Jones*, Bernd Krieg-Bruckner*, Peter Gorm Larsen*, Robert Milne, Peter Mosses*, Maurice Naftalin, Fernando Orejas*, Jan Storbank Pedersen*, Nico Plat*, John Rushby*, Jim Woodcock*.

We sincerely thank all the program committee members, especially those who managed to attend the selection meeting (the ones with * in the list above), and the referees listed on the next page for their care and advice.

Thanks are due to Michel Beaudouin-Lafon for providing the program used to collect the review forms. Evelyne Jorion, Bruno Marre, and Mountaz Zizi had to deal with a large number of submitted papers and reviews, and to prepare these proceedings. They did an excellent job and deserve special thanks for their contribution.

In addition, the following persons have played an essential role in the preparation of this symposium: Alejandro Moya, CEU, for his continued support; Peter Lucas, chair of Formal Method Europe; Hans-Jeorg Kreowski, chair of IFIP WG14.3 "Foundations of Systems Specifications"; and Alfred Hofmann, Springer-Verlag.

Thanks are also due to the organising committee of FME'96: Ana Cavalcanti, Anna Morris, Andrew Simpson and Maureen York from Oxford University; Bruno Marre and Mountaz Zizi from LRI, CNRS-Université de Paris-Sud.

FME'96 has been supported by the commission of the European Union, CRI, Formal Systems (Europe) Ltd, IFAD, Oxford University, Praxis plc, and Prentice Hall International.

Orsay, January 1996

Marie-Claude Gaudel
Jim Woodcock

External Referees

All submitted papers, whether accepted or rejected, were refereed by programme committee members and a number of external referees. This symposium would not have been possible without their voluntary and dedicated work.

Sten Agerholm
Marc Aiguier
Roswitha Bardohl
Michel Beaudouin-Lafon
Joffroy Beauquier
Michel Bidoit
Pierre Bieber
Robin Bloomfield
Frederic Boniol
Alexander Borusan
S. Brookes
Bettina Buth
Eric ten Cate
Jacques Cazin
Maura Cerioli
Ghassan Chehaibar
Christine Choppy
Ingo Classen
Tim Clement
Mirko Conrad
Patrice Cros
Werner Damm
Olivier Danvy
C.J. Dahl
Mourad Debbabi
Carlos Delgado-Kloos
Roger Duke
Heiko Dörr
Christian Engel
Andreas Fett
John Fitzgerald
David de Frutos-Escrig
Robert Geisler
F. Geurts
Reinhard German
Andrew Gordon
Wolfgang Grieskamp
Jan Friso Groote
Martin Grosse-Rhode
Jim Grundy
Ulrich Hannemann
Bo Stig Hansen
Kirsten Mark Hansen
Ian Hayes
Jifeng He
Maritta Heisel
Friedrich von Henke
Matthew Hennessy
Stephan Herrmann
Jan Hiemer
Michaela Huhn
Wil Janssen
Kurt Jensen
Gisela John
Stuart Kent
Marcus Klar
Torsten Klein
Tjabbe Kloppenburg
Peter Kluit
Kevin Lano
Frank Lattemann
Michel Lemoine
Jacques Loeckx
Rita Loogen
Michael Mac an Airchinnigh
Bernd Mahr
Bruno Marre
Javier Martinez
Jan de Meer
Pierre Michel
Kees Middelburg
Eugenio Moggi
Brian Monahan
Paul Mukherjee
Robert Nieuwenhuis
E.-R. Olderog
Florence Pagani
H. Partsch
Jan Peleska
Alfonso Pierantonio
Soren Prehn
Kees Pronk
Zhenyu Qian
Gianna Reggio
Leila Ribeiro
Willem-Paul de Roever
Bill Roscoe
Sadegh Sadeghipour
Ina Schieferdecker
Christel Seguin
N. Shankar
Hui Shi
Harbhajan Singh
Jeanine Souquieres
Mike Spivey
Mario Suedholt
Frans Ververs
Guy Vidal-Naquet
Walter Vogler
Frederic Voisin
Henrik Voss
Auke Woerlee
Virginie Wiels
Alan Williams
Burkhart Wolff
Eoin Woods
Elena Zucca

We apologise if we have inadvertently omitted a referee from the above list. To the best of our knowledge the list is accurate.

Tutorials

The tutorials form an important part of FME'96 symposium. Copies of the tutorial material will be distributed to all participants in the tutorials. We would like to thank all those who have kindly been willing to give these tutorials.
The tutorials are:

Formal Development of Object-oriented Systems in VDM++
by S. Goldsack and K. Lano, Dept. of Computing, Imperial College, UK.

Formal Development in B Abstract Machine Notation
by K. Lano and H. Haughton, Dept. of Computing, Imperial College, UK

A Tutorial on Action Semantics
by Peter D. Mosses, University of Aarhus, DK.

The Requirements State Machine Language and its Application to the Traffic Alert and Collision Avoidance System II (TCAS II).
by Mats P.E. Heimdahl, Michigan State University.

Tutorial on CSP and FDR
by Bill Roscoe, Oxford University.

The ProCoS Approach to the Design of Real-Time Systems: Linking Different Formalisms
by A.P. Ravn, Technical University of Denmark, Department of Computer Science, DK.

Tutorial on ACL2
by Matt Kaufmann, J.Strother Moore, and William D. Young, Computational Logic Inc.

An Introduction to Some Advanced Capabilities of PVS
by Sam Owre and John Rushby, Computer Science Laboratory, SRI International, Menlo Park, California, USA.

Table of Contents

Session 3b: VDM

Session 4a: User Interfaces for Formal Methods

Session 4b: Z

Session 5: Distributed Systems (1)

Session 6: Larch and LP

Session 7a: Model Checking (1)

Session 7b: Distributed Systems (2)

Session 8: Testing and Debugging

Session 9: Architecture and Reuse

Session10: Transformations

Session 11: Model Checking (2)