

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

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-Verlag. Violations are liable for prosecution under the German Copyright Law.

© Springer-Verlag Berlin Heidelberg 1996
Printed in Germany

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

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

Invited Lectures

How did Software get so Reliable Without Proof?1
C. A. R. Hoare

A Case Study on the Formal Development of a Reactor Safety System..... 18
Terje Sivertsen

*Test Automation for Safety-Critical Systems:
Industrial Application and Future Developments*39
Jan Peleska

Session 1: B

Quantitative Analysis of an Application of Formal Methods60
J. Bicarregui, J. Dick and E. Woods

Applying the B Technologies to CICS.....74
J. Hoare, J. Dick, D. Neilson and I. Sørensen

Session 2: Action Systems

Refining Action Systems within B-Tool85
M. Waldén and K. Sere

Integrating Action Systems and Z in a Medical System Specification..... 105
V. Kasurinen and K. Sere

Session 3a: Requirements

Formalizing Anaesthesia: a Case Study in Formal Specification 120
R. Groenboom, E. Saaman, E. Rotterdam and G. Renardel de Lavalette

*A New System Engineering Methodology Coupling Formal Specification
and Performance Evaluation* 140
J. Martins and J.-P. Hubaux

Formalizing New Navigation Requirements for NASA's Space Shuttle 160
Ben L. Di Vito

Session 3b: VDM

Combining VDM-SL Specifications with C++ Code..... 179
B. Fröhlich and P.G. Larsen

Data Reification without Explicit Abstraction Functions 195
T. Clement

*Formal and Informal Specifications of a Secure System Component:
Final Results in a Comparative Study*..... 214
T. M. Brookes, J. S. Fitzgerald and P.G. Larsen

Session 4a: User Interfaces for Formal Methods

Visual Verification of Safety and Liveness..... 228
A. Valmari and M. Setälä

Graphical Development of Consistent System Specifications 248
B. Schätz, H. Hußmann and M. Broy

Deduction in the Verification Support Environment (VSE) 268
D. Hutter, B. Langenstein, C. Sengler, J. H. Siekmann, W. Stephan and A. Wolpers

Session 4b: Z

Consistency and Refinement for Partial Specification in Z..... 287
E. Boiten, J. Derrick, H. Bowman and M. Steen

*Combining Statecharts and Z for the Design
of Safety-Critical Control Systems*..... 307
M. Weber

Integrating Real-time Scheduling Theory and Program Refinement..... 327
C. Fidge, M. Utting, P. Kearney and I. Hayes

Session 5: Distributed Systems (1)

*Using a Logical and Categorical Approach for the Validation of
Fault-Tolerant Systems*..... 347
C. Seguin and V. Wiels

Local Nondeterminism in Asynchronously Communicating Processes 367
F. S. de Boer and M. van Hulst

Session 6: Larch and LP

*Identification of and Solutions to Shortcomings of LCL,
a Larch/C Interface Specification Language* 385
P. Chalin, P. Grogono and T. Radhakrishnan

Formal Specification and Verification of the pGVT Algorithm 405
B. Kannikeswaran, R. Radhakrishnan, P. Frey, P. Alexander and P. A. Wilsey

Session 7a: Model Checking (1)

Automatic Verification of a Hydroelectric Power Plant..... 425
R. Pugliese and E. Tronci

Experiences in Embedded Scheduling 445
David M. Jackson

*Model Checking in Practice: An Analysis of the ACCESS.busTM Protocol
using SPIN*..... 465
B. Boigelot and P. Godefroid

Session 7b: Distributed Systems (2)

*The Incremental Development of Correct Specifications
for Distributed Systems*..... 479
S. Kleuker and H. Tjabben

A Theory of Distributing Train Rescheduling 499
C. George

*An Improved Translation of SA/RT Specification Model
to High-Level Timed Petri Nets*..... 518
L. Shi and P. Nixon

Session 8: Testing and Debugging

From Testing Theory to Test Driver Implementation 538
J. Peleska and M. Siegel

Program Slicing using Weakest Preconditions 557
J. J. Comuzzi and J. M. Hart

Session 9: Architecture and Reuse

A Formal Approach to Architectural Design Patterns 576
 P. S. C. Alencar, D. D. Cowan and C. J. P. Lucena

*Modular Completeness: Integrating the Reuse of Specified Software
 in Top-Down Program Development* 595
 J. Zwiers, U. Hannemann, Y. Lakhneche, W.-P. de Roever and F. Stomp

Session10: Transformations

A Strategic Approach to Transformational Design 609
 J. Bohn and W. Janssen

Correct and User-Friendly Implementations of Transformation Systems..... 629
 Kolyang, T. Santen and B. Wolff

Session 11: Model Checking (2)

An Example of use of Formal Methods to Debug an Embedded Software 649
 A. Arnold, D. Bégay and J.-P. Radoux

*Experiments in Theorem Proving and Model Checking
 for Protocol Verification*..... 662
 K. Havelund and N. Shankar

Procedure-Level Verification of Real-time Concurrent Systems 682
 F. Wang and C.-T. Lo

Author's Index 703