Lecture Notes in Computer Science 1313
Edited by G. Goos, J. Hartmanis and J. van Leeuwen

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

John Fitzgerald Cliff B. Jones
Peter Lucas (Eds.)

FME '97: Industrial Applications and Strengthened Foundations of Formal Methods

4th International Symposium
of Formal Methods Europe
Graz, Austria, September 15-19, 1997
Proceedings

Springer

Series Editors

Gerhard Goos, Karlsruhe University, Germany

Juris Hartmanis, Cornell University, NY, USA

Jan van Leeuwen, Utrecht University, The Netherlands

Volume Editors

John Fitzgerald
University of Newcastle upon Tyne, Centre for Software Reliability
Bedson Building, NE1 7RU Newcastle upon Tyne, United Kingdom
E-mail: john.fitzgerald@ncl.ac.uk

Cliff B. Jones
Director Applications Division, Harlequin Ltd., Queens Court
Wilmslow Road, SK9 7QD Cheshire, United Kingdom
E-mail: cbj@harlequin.co.uk

Peter Lucas
Technical University Graz, Institute for Software Technology
Münzgrabenstr. 11/2, A-8010 Graz, Austria
E-mail: lucas@ist.tu-graz.ac.at

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Industrial applications and strengthened foundations of formal methods : proceedings / FME '97, 4th International Symposium of Formal Methods Europe, Graz, Austria, September 15 - 19, 1997. John Fitzgerald ... (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Santa Clara ; Singapore ; Tokyo : Springer, 1997
(Lecture notes in computer science ; Vol. 1313)
ISBN 3-540-63533-5

CR Subject Classification (1991): D.1-2, D.3.1,F.3.1, J.1, K.6

ISSN 0302-9743
ISBN 3-540-63533-5 Springer-Verlag Berlin Heidelberg New York

Typesetting: Camera-ready by author
SPIN 10545840 06/3142 – 5 4 3 2 1 0 Printed on acid-free paper

Preface

This volume contains the proceedings of the fourth international symposium of Formal Methods Europe. The conference, which took place at the Technical University of Graz, Austria, in September 1997, was the eighth in a series which began in Brussels in 1987 with the first of four symposia organised by the VDM Europe group. Later, when VDM Europe widened its scope to become Formal Methods Europe (FME), the current symposium series replaced the VDM conferences. Now FME is a group of practitioners and researchers from industrial and academic institutions who share the aim of encouraging the use of sound mathematically based techniques in the engineering development of computing systems. The group is supported by the Commission of the European Union.

The FME Symposium, which traditionally takes place every eighteen months, reports current work in the area of software development methods that combine mathematical rigour with applicability in the commercial context. The majority of the papers describe industrial applications, extensions to existing techniques or case studies. Papers on theory are accepted only where they show clear potential applicability.

Formal methods are increasingly recognised as a viable technology for the development of computing systems. The papers in this volume bear witness to the importance now being attached to the integration of formal methods with existing development practices. Such integration can be achieved through the provision of common frameworks for a variety of notations and techniques, or by linking formal modelling and analysis techniques to widely accepted tools and notations for systematic development. The problem of gaining acceptance for the use of an unfamiliar formalism is addressed through work to provide graphical notations with sound bases.

As technological advances in formal methods continue to be reported, dissemination of results to industry assumes ever greater importance. Managers and engineers must be able to make informed choices from the range of development tools and techniques available. Since the previous symposium in 1996, FME has responded to this need by organising seminars for industry in ten countries, developing databases, bibliographies and frequently-asked question files recording information on formal methods, their applications and tool support. At the time of writing, the databases provide reports on nearly ninety industrial applications and over fifty support tools. Resources for managers have been developed in variety of media including broadcast video and World Wide Web pages. Further details on these activities are given in the section on FME Dissemination Actions below.

This volume presents 35 papers accepted out of 97 submissions from 21 countries. In addition to submitted papers, the symposium was addressed by four invited speakers: Hermann Kopetz of the Technical University of Vienna, Loe Feijs of Philips Research Laboratories in the Netherlands, Robin Bloomfield of Adelard in the UK and, at the conference dinner, Heinz Zemanek who initiated much of the international collaboration on formal methods with the famous 1964 Baden-bei-Wien conference on "Formal Language Definition Languages".

The international nature of FME'97, its combination of academic and industrial participants and its mixture of reports on technological development and concrete application, continue the tradition of the FME and VDM Symposia. It is to be hoped that this symposium will foster future collaboration to the benefit of the computing industry as a whole.

Newcastle upon Tyne, July 1997

J. S. Fitzgerald
C. B. Jones
P. Lucas

Acknowledgements

We are grateful to the many colleagues who have contributed to the organisation and success of FME'97.

Programme Committee

John Fitzgerald (PC co-Chair)	Brendan Mahony
Cliff Jones (PC co-Chair)	Lynn Marshall
Manfred Broy	Dominique Mery
George Cleland	Peter D. Mosses
Peter Froome	José Oliveira
Chris George	Nico Plat
Shinichi Honiden	Andrzej Tarlecki
Daniel Jackson	Martyn Thomas
Carlos José Pereira de Lucena	Rob Witty
Doug McIlroy	Joakim von Wright

Organising Committee

Peter Lucas (OC Chair)	Petra Pichler
Brigitte Froehlich	Andreas Bollin
Christian Schinagl	Andreas Ausserhofer

We also acknowledge the valuable contributions of Alejandro Moya at the Commission of the European Union, for his continued support of Formal Methods Europe, and Alfred Hofmann at Springer-Verlag for continued interest in publishing the proceedings. The Centre for Software Reliability at the University of Newcastle upon Tyne provided considerable infrastructure support for the programme committee. We are especially grateful to Alison Sheavills for her hard work handling submitted papers, reviews and arrangements for the programme committee.

We would specially like to thank the Principal of the Technical University Graz, Univ.Prof. Irolt Kilman for his support in hosting FME'97. In addition we acknowledge the contributions of the following: Mrs. Almut Fehringer, Tourist Office Graz, for her perfect organising of accommodation; Mrs. Elisabeth Pirker, Technical University Graz, for graphical design and layout and finally Type & Print Ltd. for support and assistance in printing.

Symposium Sponsors

The generous support of the following companies and institutions has contributed to the success of the Symposium:

The Technical University Graz, Austria
The Mayor of the City of Graz, Austria
Tourist Office Graz, Austria
The Austrian Computer Society, Vienna
Canon Office Systems, Austria
TCplus Computer Systems, Austria
Casinos Austria AG, Graz
IFAD - The Institute for Applied Computer Science, Denmark
CRI Computer Resources International A/S, Denmark
The Harlequin Group Limited, U.K.

External Referees

All submitted papers were reviewed by members of the Programme Committee and a number of external referees, without whose hard work the symposium would not be possible. To the best of our knowledge the list below is accurate: we apologise for any inaccuracies or omissions.

Paulo Alencar	José Alferes	Jim Armstrong
Roland Backhouse	Leonor Barroca	José Bernardo Barros
Angelo E. Bean	M.A. Bednarczyk	Sonia Bergamaschi
Marcin Białasik	Andrzej Borzyszkowski	Luc Bougé
Richard J. Boulton	S. Brookes	Michael Butler
Gian Luca Cattani	Antonio Cerone	Tim Clement
Ian Cottam	Radhia Cousot	Régis Cridlig
Paul Curzon	Ludwik Czaja	Dang Van Hung
Juergen Dingel	Katherine Eastaughfte	Javier Esparza
J.L. Fiadeiro	Colin Fidge	Marcus Felipe Fontoura
M. Fuchs	Simon Gay	J. Paul Gibson
Eric Goubault	J.-Ch. Grégoire	Pascal Gribomont
Jim Grundy	Michael R. Hansen	John Harrison
Ian Hayes	Görel Hedin	B. Hemeury
Pedro Rangel Henriques	John Herbert	Ursula Hinkel
Christoph Hofmann	Tadashi Iijima	Misbah Islam
Yoshinao Isobe	Janusz Jabłonowski	David Janin
Tomasz Janowski	P. Johnson	Claire Jones
Darrell Kindred	Carlos Delgado Kloos	Beata Konikowska
Ingolf Krueger	Linas Laibinis	Thomas Långbacka
K. Lano	Kim G. Larson	Sławomir Lasota
Rogerio de Lemos	Kurt Lichtner	Peter Lindsay
Witold Lukaszewicz	Leo Pini Magalhaes	Saeko Matsuura

Bruno Mermet
Anna Mikhajlova
Richard Moore
George Necula
David Von Oheimb
Paweł Pączkowski
Jan Philipps
Ceri Rees
Olivier Roux
Amer Saeed
Monika Schmidt
Peter Scholz
Kaisa Sere
Katharina Spies
J. Straunstrup
Mark Utting
Qiwen Xu
George Yee
Zhou Chaochen
Stephen Merz
Marius Minea
Olaf Mueller
Luis Nova
Peter Ørbæk
Barbara Paech
Michael Pilling
Mauno Rönkkö
Rimvydas Rukšėnas
Bernhard Schätz
Erik M. Schmidt
Aleksy Schubert
Oscar Slotosch
Jason Steggles
Su Thomas
José Manuel Valença
J. Yantcher
Lu Yuan
John Zic
Kees Middelburg
Danilo Montesi
Kenji Nagahashi
Robert O'Callahan
Maris Ozols
Prakash Panangaden
Anders P. Ravn
Kristoffer Rose
Mark Ryan
Birgit Schieder
Alexander B. Schmidt
Emil Sekerinski
Stefan Sokołowski
Magnus Steinby
Mitsukazu Unchiyama
Marina Waldén
Hiroka zu Yatsu
Amy Moormann Zaremski

Tutorials

The tutorials form an important part of the FME Symposium. We are grateful to all those who kindly submitted tutorial proposals. The following tutorials were scheduled for the two days preceding the research symposium:

Semantics and Logic for Provable Fault-Tolerance
Tomasz Janowski, UNU/IIST

ACL2
J. Strother Moore, Matt Kaufmann, William D. Young, Computational Logic Inc.

Formal Software Development Using Cogito
T. P. Kearney, O. Traynor, University of Queensland

Industrial Training and University Education in Formal Methods
Michael Hinchey, José Oliveira, New Jersey Institute of Technology, University of Minho

Tool Demonstrations

In parallel with all the other activities at FME'97, tools supporting formal methods were demonstrated in an exhibition. At the time of writing, the following tools were due to be demonstrated at FME'97. However, further demonstrations are expected.

AtelierB demonstration: Thierry Servat, Clement Roches, Steria Mediterranée, France.

3D Visual Tool Supporting Derivation of Operational Specification for Parallel Programs: E. Trichina, J. Oinonen, Advanced Computing Research Center, University of South Australia, Australia.

TAS and IsaWin: Generic Interfaces for Transformational Program Development and Theorem Proving: Christoph Lueth, Bremen Institute for Safe Systems, University of Bremen, Germany.

RAISE Tool Demonstration: Jan Storbank Pedersen, Computer Resources International A/S, Denmark.

VDM Technology: Peter Gorm Larsen, Institute for Applied Computer Science (IFAD), Denmark.

XBarnacle: A Semi-automated Proof Tool: Helen Lowe, Dept. of Computing, Napier University, United Kingdom.

VST Hans Martin Hoercher, Vossloh-Systemtechnik GmbH, Germany.

SDT and ITEX: Magnus Herner, Telelogic AB, Sweden.

FME Dissemination Actions

In the two years prior to this symposium, the members of FME have been involved in three dissemination actions aiming to raise awareness of available formal methods technologies in the wider professional community. The target audience has been industrial software developers, especially those who wish to explore the use of formal techniques but who are unaware of the technical choices, available methods, tools and previous experiences of other applications. Results from the projects described here are all accessible from the FME hub web site at `http://www.cs.TCD.ie/FME`, or from the addresses indicated below. All three actions have been supported under the European Systems and Software Initiative of the CEU.

The **FMEInfRes** project maintains databases of formal methods applications, support tools, bibliographies and frequently-asked questions. Information may be accessed on the FME hub page mentioned above. Entries for the databases are actively sought. Those with information about industrial applications should contact Nico Plat (Email: `Nico.Plat@ACM.org`). Providers of support tools should contact Tim Denvir (Email: `t-denvir@dircon.co.uk`).

The **FMEIndSem** project has organised seminars for industry in ten European countries and has established national industrial interest groups. Further information can be found at `http://www.ifad.dk/projects/fmeindsem.html`.

The **FM-Guides** project provides information for managers in industry on the benefits of applying formal techniques. Material is provided in a variety of media, including web pages (`http://www.cybercable.tm.fr/1997/Formal` and video. The main contact is Eric Delalonde (Email: `edelalon@ecom.cgs.fr`).

Table of Contents

Diagrams and Programming Languages for Programmable Controllers 1
Stuart Anderson, Konstantinos Tourlas

Graphical Specification and Reasoning: Case Study Generalised Railroad Crossing 20
Henning Dierks, Cheryl Dietz

A Graphic Notation for Formal Specifications of Dynamic Systems 40
Gianna Reggio, Mauro Larosa

A Semantic Integration of Object-Z and CSP for the Specification of Concurrent Systems 62
Graeme Smith

Class Refinement and Interface Refinement in Object-Oriented Programs . 82
Anna Mikhajlova, Emil Sekerinski

Formalizing Requirements for Distributed Systems with Trace Diagrams .. 102
Stephan Kleuker

Consistent Graphical Specification of Distributed Systems 122
Franz Huber, Bernhard Schätz, Geralf Einert

Design of Reactive Control Systems for Event-Driven Operations 142
K. Lano, A. Sanchez

An M-Net Semantics for a Real-Time Extension of μSDL 162
Hans Fleischhack, Josef Tapken

Reconciling Real-Time with Asynchronous Message Passing 182
M. Broy, R. Grosu, C. Klein

Specifying the Remote Controlling of Valves in an Explosion Test Environment 201
Martin Schönhoff, Mojgan Kowsari

PICGAL: Practical Use of Formal Specification to Develop a Complex Critical System 221
Lionel Devauchelle, Peter Gorm Larsen, Henrik Voss

Mathematical Modeling and Analysis of an External Memory Manager ... 237
William D. Young, William R. Bevier

Automatic Translation of VDM-SL Specifications into Gofer 258
Paul Mukherjee

Towards an Integrated CASE and Theorem Proving Tool for VDM-SL 278
Sten Agerholm, Jacob Frost

Specification of Required Non-determinism 298
K. Lano, J. Bicarregui, J. Fiadeiro, A. Lopes

A Corrected Failure-Divergence Model for CSP in Isabelle/HOL 318
H. Tej, B. Wolff

A Proof Obligation Generator for VDM-SL 338
Bernhard K. Aichernig, Peter Gorm Larsen

Verification of Cryptographic Protocols: An Experiment 358
Marc Mehdi Ayadi, Dominique Bolignano

TLA + PROMELA: Conjecture, Check, Proof. Engineering New Protocols Using Methods and Formal Notations. 378
J.-Ch. Grégoire

A TLA Solution to the Specification and Verification of the RLP1 Retransmission Protocol 398
Abdelillah Mokkedem, Michael J. Ferguson, Robert deB. Johnston

An Efficient Technique for Deadlock Analysis of Large Scale Process Networks 418
J.M.R. Martin, S.A. Jassim

Implementing a Model Checker for LEGO 442
Shenwei Yu, Zhaohui Luo

Formal Verification of Transformations for Peephole Optimization 459
A. Dold, F.W. von Henke, H. Pfeifer, H. Rueß

A Meta-Method for Formal Method Integration 473
Richard F. Paige

Reuse of Verified Design Templates Through Extended Pattern Matching . 495
David Hemer, Peter A. Lindsay

A Compositional Proof System for Shared Variable Concurrency 515
F.S. de Boer, U. Hannemann, W.-P. de Roever

A Framework for Modular Formal Specification and Verification 533
Pierre Michel, Virginie Wiels

A Timed Semantics for the STATEMATE Implementation of Statecharts . 553
Carsta Petersohn, Luis Urbina

Using PVS to Prove a Z Refinement: A Case Study 573
David W.J. Stringer-Calvert, Susan Stepney, Ian Wand

Verification of Reactive Systems Using DisCo and PVS 589
Pertti Kellomäki

Term Rewrite Systems to Derive Set Boolean Operations on 2D Objects .. 605
David Cazier, Jean-François Dufourd

A Normal Form Reduction Strategy for Hardware/Software Partitioning .. 624
Leila Silva, Augusto Sampaio, Edna Barros

Viewpoint Consistency in Z and LOTOS: A Case Study 644
Eerke Boiten, Howard Bowman, John Derrick, Maarten Steen

A UNITY Mapping Operator for Distributed Programs 665
Michel Charpentier

Author Index 685