



**Springer**

*Berlin*

*Heidelberg*

*New York*

*Hong Kong*

*London*

*Milan*

*Paris*

*Tokyo*

Jin Song Dong Jim Woodcock (Eds.)

# Formal Methods and Software Engineering

5th International Conference  
on Formal Engineering Methods, ICFEM 2003  
Singapore, November 5-7, 2003  
Proceedings



Springer

## Series Editors

Gerhard Goos, Karlsruhe University, Germany  
Juris Hartmanis, Cornell University, NY, USA  
Jan van Leeuwen, Utrecht University, The Netherlands

## Volume Editors

Jin Song Dong  
National University of Singapore, Computer Science Department  
3 Science Drive 2, Singapore 117543  
E-mail: dongjs@comp.nus.edu.sg

Jim Woodcock  
University of Kent, Computing Laboratory  
Canterbury, Kent, CT2 7NF, UK  
E-mail: J.C.P.Woodcock@kent.ac.uk

## Cataloging-in-Publication Data applied for

A catalog record for this book is available from the Library of Congress.

Bibliographic information published by Die Deutsche Bibliothek  
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie;  
detailed bibliographic data is available in the Internet at <<http://dnb.ddb.de>>.

CR Subject Classification (1998): D.2.4, D.2, F.3, D.3, F.4

ISSN 0302-9743

ISBN 3-540-20461-X 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 is a part of Springer Science+Business Media

[springeronline.com](http://springeronline.com)

© Springer-Verlag Berlin Heidelberg 2003  
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik  
Printed on acid-free paper SPIN: 10967843 06/3142 5 4 3 2 1 0

# Preface

This volume contains the proceedings of the 2003 International Conference on Formal Engineering Methods (ICFEM 2003). The conference was the fifth in a series that began in 1997. ICFEM 2003 was held in Singapore during 5–7 November 2003.

ICFEM 2003 aimed to bring together researchers and practitioners from industry, academia, and government to advance the state of the art in formal engineering methods and to encourage a wider uptake of formal methods in industry.

The Program Committee received 91 submissions from more than 20 countries in various regions. After each paper was reviewed by at least three referees in each relevant field, 34 high-quality papers were accepted based on originality, technical content, presentation and relevance to formal methods and software engineering. We wish to sincerely thank all authors who submitted their work for consideration. We would also like to thank the Program Committee members and other reviewers for their great efforts in the reviewing and selecting process.

We are indebted to the three keynote speakers, Prof. Ian Hayes of the University of Queensland, Prof. Mathai Joseph of the Tata Research, Development and Design Centre, and Dr. Colin O'Halloran of QinetiQ, for accepting our invitation to address the conference.

ICFEM 2003 was well organized. It could not have been successful without the hard work and efforts of our organization, program and steering committee members. We would particularly like to thank Jifeng He and P.S. Thiagarajan for overseeing general issues of the conference, Martin Henz for handling local organization, Hugh Anderson and Aminah Ayu for handling registrations, Hai Wang for maintaining the conference Website, Shengchao Qin and Zongyan Qiu for taking care of publicity, and Yuanfang Li for his excellent assistance in preparing the proceedings with Jun Sun and in setting up and maintaining the Web review system CyberChair (developed by R. van de Stadt). Finally, our thanks to Springer-Verlag for their help with the publication.

ICFEM 2003 was sponsored and organized by the Computer Science Department, National University of Singapore. More information on this conference can be found at: <http://nt-appn.comp.nus.edu.sg/fm/icfem2003/>

# Organization

## Conference Committee

Conference Co-chairs:	Jifeng He (IIST, United Nations U.) P.S. Thiagarajan (National U. of Singapore)
Program Co-chairs:	Jin Song Dong (National U. of Singapore) Jim Woodcock (U. of Kent)
Publicity Co-chairs:	Shengchao Qin (National U. of Singapore) Zongyan Qiu (Peking University)
Local Organization Chair:	Martin Henz (National U. of Singapore)
Registration:	Hugh Anderson (National U. of Singapore)
Webmasters:	Yuanfang Li (National U. of Singapore) Wang Hai (National U. of Singapore)
Proceedings Assistant Editor:	Yuanfang Li (National U. of Singapore)

## Program Committee

Vasu Alagar	Kyo Chul Kang	Thomas Santen
Richard Banach	Kung-Kiu Lau	Klaus-Dieter Schewe
Jonathan Bowen	Shaoying Liu	Wolfram Schulte
Manfred Broy	Zhiming Liu	Graeme Smith
Michael Butler	Huimin Lin	Paul Swatman
Ana Cavalcanti	Peter Lindsay	Kenji Taguchi
Dan Craigen	Brendan Mahony	Sofiène Tahar
Jim Davies	Huaikou Miao	T.H. Tse
Jin Song Dong	Jeff Offutt	Farn Wang
Kai Engelhardt	Richard Paige	Yi Wang
John Fitzgerald	Abhik Roychoudhury	Jim Woodcock
Marc Frappier	Motoshi Saeki	Hongjun Zheng
Andy Galloway	Augusto Sampaio	Hong Zhu

## Referees

Parosh Abdulla	Alessandra Cavarra	Danielle Fowler
Otmane Ait-Mohamed	Sungdeok Cha	Benoit Fraikin
Behzad Akbarpour	Haiming Chen	Frédéric Gervais
Juan Carlos Augusto	Yifeng Chen	Andy Gravell
Ho-Jung Bang	Hung Dang Van	Jim Grundy
Luis. S. Barbosa	Neville Dean	Stefan Gruner
Phil Brooke	Roger Duke	Ali Habibi
Zining Cao	Colin Fidge	Ping Hao

## VIII Organization

John Harrison	Hui Liang	Harold Simmons
Sven Hartmann	Sebastian Link	Carlo Simon
Ian Hayes	Jim McCarthy	Jing Sun
Steffen Helke	Alistair McEwan	Jun Sun
David Hemer	Sun Meng	Pasha Shabalin
Shui-Ming Ho	Yassine Mokhtari	Linda Yue Tang
Xiaoning Huang	Alexandre Mota	P.S. Thiagarajan
Ralf Huuck	Tohru Naoi	Alexei Tretiakov
Cornelia Inggs	Muan Yong Ng	Mark Utting
Czeslaw Jeske	Naoya Nitta	Frank D. Valencia
Jan Jürjens	Olga Ormandjieva	Sergiy Vilkomir
Florian Kammüller	N. Paramesh	Hai Wang
Siau-Cheng Khoo	Joey Paquet	Yan Wang
Moonjoo Kim	Anup Patnaik	Guido Wimmel
Soon-Kyeong Kim	Hong Peng	Kirsten Winter
Tai-Hyo Kim	Kasi Periyasamy	Satoshi Yamane
Markus Kirchberg	Paul Pettersson	Roland Yap Hock Chuan
Leonid Kof	Mike Poppleton	Hirokazu Yatsu
Ming Siem Kong	Stephane Lo Presti	Hongnian Yu
Maciej Koutny	Shengchao Qin	Ling Yuan
Kevin Lano	S. Ramesh	Patryk Zadarnowski
Mohamed Layouni	Ken Robinson	Wenhui Zhang
Reinhold Letz	Jan Romberg	Mao Zheng
Martin Leucker	Dirk Seifert	
Yuan Fang Li	Adnan Sherif	

## Steering Committee

Chair:	Jifeng He (IIST, United Nations U.)
Members:	Keijiro Araki (Kyushu U.)
	Jin Song Dong (National U. of Singapore)
	Chris George (IIST, United Nations U.)
	Mike Hinchey (NASA)
	Shaoying Liu (Hosei U.)
	John McDermid (U. of York)
	Carroll Morgan (U. of NSW)
	Tetsuo Tamai (U. of Tokyo)
	Jim Woodcock (U. of Kent)

# Table of Contents

## Invited Talks

Programs as Paths: An Approach to Timing Constraint Analysis . . . . .	1
<i>Ian J. Hayes</i>	
Model Based Code Verification . . . . .	16
<i>Colin O'Halloran</i>	
Adding Formalism to Methods or <i>Where and When Will Industry Use Formal Reasoning?</i> . . . . .	26
<i>Mathai Joseph</i>	

## Testing and Validation

Using Formal Methods to Serialize Synchronization Events . . . . .	34
<i>Jessica Chen</i>	
An AMBA-ARM7 Formal Verification Platform . . . . .	48
<i>Kong Woei Susanto and Tom Melham</i>	
Formalization, Testing and Execution of a Use Case Diagram . . . . .	68
<i>Wuwei Shen and Shaoying Liu</i>	
Service-Based Systems Engineering: Consistent Combination of Services . .	86
<i>Bernhard Schätz and Christian Salzmann</i>	

## State Diagrams

Using State Diagrams to Describe Concurrent Behaviour . . . . .	105
<i>Jim Davies and Charles Crichton</i>	
The Equivalence of Statecharts . . . . .	125
<i>Quan Long, Zongyan Qiu, and Shengchao Qin</i>	
Generic Interacting State Machines and Their Instantiation with Dynamic Features . . . . .	144
<i>David von Oheimb and Volkmar Lotz</i>	

## PVS/HOL

Using PVS to Prove Properties of Systems Modelled in a Synchronous Dataflow Language . . . . .	167
<i>Sanjai Rayadurgam, Anjali Joshi, and Mats P.E. Heimdahl</i>	



Formalising an Integrated Language in PVS .....	187
<i>Gwen Salaün and Christian Attiogbé</i>	

## Refinement

Modeling SystemC Fixed-Point Arithmetic in HOL .....	206
<i>Behzad Akbarpour and Sofiène Tahar</i>	
Adding Action Refinement to Stochastic True Concurrency Models .....	226
<i>Mila Majster-Cederbaum and Jinzhao Wu</i>	
Incremental Derivation of Abstraction Relations for Data Refinement .....	246
<i>Neil J. Robinson</i>	
Comparison of Data and Process Refinement .....	266
<i>Steve Reeves and David Streader</i>	
Compilation by Refinement for a Practical Assembly Language .....	286
<i>Geoffrey Watson</i>	

## Hybrid Systems

Java Card Code Generation from B Specifications .....	306
<i>Bruno Tatibouët, Antoine Requet, Jean-Christophe Voisinnet, and Ahmed Hammad</i>	
Efficient Path Finding with the Sweep-Line Method Using External Storage .....	319
<i>Lars Michael Kristensen and Thomas Mailund</i>	
Formal Development of a Distributed Logging Mechanism Supporting Disconnected Updates .....	338
<i>Yuechen Qian</i>	
Formal Proof of a Polychronous Protocol for Loosely Time-Triggered Architectures .....	359
<i>Mickaël Kerbæuf, David Nowak, and Jean-Pierre Talpin</i>	

## Z/Object-Z

A Z Based Approach to Verifying Security Protocols .....	375
<i>Benjamin W. Long, Colin J. Fidge, and Antonio Cerone</i>	
A Refinement Tool for Z .....	396
<i>Angela Freitas, Carla Nascimento, and Ana Cavalcanti</i>	
The Common Semantic Constructs of XML Family .....	416
<i>Hong Li Yang, Jun Gang Han, and Ke Gang Hao</i>	

## Petri Nets

Controller Synthesis for Object Petri Nets . . . . .	432
<i>Berndt Farwer, Saraswati Kalvala, and Kundan Misra</i>	
Towards a Workflow Model of Real-Time Cooperative Systems . . . . .	452
<i>Yuyue Du and Changjun Jiang</i>	
New Developments in Closed-Form Computation for GSPN Aggregation . . . . .	471
<i>Jörn Freiheit and Jonathan Billington</i>	

## Timed Automata

On Clock Difference Constraints and Termination in Reachability Analysis of Timed Automata . . . . .	491
<i>Johan Bengtsson and Wang Yi</i>	
Analyzing the Redesign of a Distributed Lift System in UPPAAL . . . . .	504
<i>Jun Pang, Bart Karstens, and Wan Fokkink</i>	
Verification of Timeliness QoS Properties in Multimedia Systems . . . . .	523
<i>Behzad Bordbar and Kozo Okano</i>	

## System Modeling and Checking

A Calculus for Set-Based Program Development . . . . .	541
<i>Georg Struth</i>	
Compositional Verification of a Switch Fabric from Nortel Networks . . . . .	560
<i>Hong Peng, Sofiène Tahar, and Yassine Mokhtari</i>	
Constraint-Based Model Checking of Data-Independent Systems . . . . .	579
<i>Beata Sarna-Starosta and C. R. Ramakrishnan</i>	
A Formal Model for the Block Device Subsystem of the Linux Kernel . . . . .	599
<i>Peter T. Breuer</i>	

## Semantics and Synthesis

A Mathematical Framework for Safecharts . . . . .	620
<i>Hamdan Dammag and Nimal Nissanke</i>	
A Relational Model for Formal Object-Oriented Requirement Analysis in UML . . . . .	641
<i>Zhiming Liu, He Jifeng, Xiaoshan Li, and Yifeng Chen</i>	
From Specification to Hardware Device: A Synthesis Algorithm . . . . .	665
<i>Vincenza Carchiolo, Michele Malgeri, and Giuseppe Mangioni</i>	

<b>Author Index</b> . . . . .	683
-------------------------------	-----