

Lecture Notes in Computer Science

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

2335

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Singapore

Tokyo

Michael Butler Luigia Petre Kaisa Sere (Eds.)

Integrated Formal Methods

Third International Conference, IFM 2002
Turku, Finland, May 15-18, 2002
Proceedings



Springer

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

Volume Editors

Michael Butler

University of Southampton, Department of Electronics and Computer Science
Declarative Systems and Software Engineering
Highfield, Southampton, SO17 1BJ, UK
E-mail: mjb@ecs.soton.ac.uk

Luigia Petre

Turku Centre for Computer Science
Lemminkäisenkatu 14A, 20520 Turku, Finland
E-mail: lpetre@abo.fi

Kaisa Sere

Åbo Akademi University, Department of Computer Science
Lemminkäisenkatu 14, 20520 Turku, Finland
E-mail: Kaisa.Sere@abo.fi

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Integrated formal methods : third international conference ; proceedings /
IFM 2002, Turku, Finland, May 15 - 18, 2002. Michael Butler ... (ed.). -
Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ;
Paris ; Tokyo : Springer, 2002
(Lecture notes in computer science ; Vol. 2335)
ISBN 3-540-43703-7

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

ISSN 0302-9743

ISBN 3-540-43703-7 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 New York
a member of BertelsmannSpringer Science+Business Media GmbH

<http://www.springer.de>

© Springer-Verlag Berlin Heidelberg 2002
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik
Printed on acid-free paper SPIN 10869773 06/3142 5 4 3 2 1 0

Preface

The third in a series of international conferences on Integrated Formal Methods, IFM 2002, was held in Turku, Finland, May 15–17, 2002. Turku, situated in the south western corner of the country, is the former capital of Finland. The conference was organized jointly by Åbo Akademi University and Turku Centre for Computer Science.

The theme of IFM 1999 was the integration of state and behavioral based formalisms. For IFM 2000 this was widened to include all aspects pertaining to the integration of formal methods and formal notations. One of the goals of IFM 2002 was to further investigate these themes. Moreover, IFM 2002 explored the relations between formal methods and graphical notations, especially the industrial standard language for software design, the Unified Modeling Language (UML).

The themes of IFM 2002 reflect what we believe is a growing trend in the Formal Methods and Software Engineering research communities. Over the last three decades, computer scientists have developed a range of formalisms focusing on particular aspects of behavior or analysis, such as sequential program structures, concurrent program structures, data and information structures, temporal reasoning, deductive proof, and model checking. Much effort is now being devoted to integrating these methods in order to combine their advantages and ensure they scale up to industrial needs. Graphical notations are now widely used in software engineering and there is growing recognition of the importance of providing these with the formal underpinnings and formal analysis capabilities found in formal methods.

The invited speakers for the conference represent a range of academic and industrial research experience. Eran Gery is Vice President for Rhapsody product development at I-Logix Inc. He is involved in the UML 2.0 consortium, and was a member of the UML founding team. Shmuel Katz is Professor of Computer Science at the Technion in Israel and leads research into the integration of specification notations and verification tools. Stuart Kent is Senior Lecturer in Computer Science at the University of Kent, UK and also works with IBM UK Research Laboratories on model-driven development of e-business systems.

In total there were 46 submissions for IFM 2002. Of these, 18 were selected for publication in the proceedings and presentation at the conference. Each paper was independently reviewed by several members of the Program Committee or their colleagues. The selection of the final 18 papers was based on the reviews followed by electronic discussion between the reviewers. In these proceedings, the papers are grouped into the following themes:

- Integration, Simulation, Animation
- From Specification to Verification
- Statecharts and B: Integration and Translation
- Model Checkers and Theorem Provers

- Links between Object-Z and CSP
- Combining Graphical and Formal Approaches
- Refinement and Proof

We hope that these proceedings will be of benefit both to the conference participants and to the wider community of researchers and practitioners in the field. The production of these proceedings would not have been possible without the invaluable help of the program committee members as well as their external referees, and of all the contributors who submitted papers to the conference.

March 2002

Michael Butler
Luigia Petre
Kaisa Sere

Organization

Michael Butler, University of Southampton, UK (PC Co-chair)
Luigia Petre, Turku Centre for Computer Science, Finland
Kaisa Sere, Åbo Akademi University, Turku, Finland (PC Co-chair)

Program Committee

Didier Bert (Grenoble, France)	Dominique Mery (Nancy, France)
Jonathan Bowen (London, UK)	Luigia Petre (Turku, Finland)
Michael Butler (Southampton, UK)	Thomas Santen (Berlin, Germany)
Jim Davies (Oxford, UK)	Steve Schneider (London, UK)
John Derrick (Kent, UK)	Wolfram Schulte (Redmond, USA)
Jin Song Dong (Singapore)	Kaisa Sere (Turku, Finland)
John Fitzgerald (Manchester, UK)	Jane Sinclair (Warwick, UK)
Andrew Galloway (York, UK)	Graeme Smith (Queensland, Australia)
Chris George (Macao)	Bill Stoddart (Teesside, UK)
Wolfgang Grieskamp (Redmond, USA)	Kenji Taguchi (Uppsala, Sweden)
Henri Habrias (Nantes, France)	W J (Hans) Toetenel (Delft, Holland)
Susumu Hayashi (Kobe, Japan)	Heike Wehrheim (Oldenburg, Germany)
Maritta Heisel (Magdeburg, Germany)	Jim Woodcook (Oxford, UK)
Michel Lemoine (Toulouse, France)	
Shaoying Liu (Tokyo, Japan)	

Referees

Christian Attiogbé	Carla Ferreira	Mauno Rönkkö
Mike Barnett	Andy Gravell	Andrew Simpson
Christie Bolton	Steffen Helke	Colin Snook
Marcello Bonsangue	Jean-Yves Lafaye	Jing Sun
Alessandra Cavarra	Kung-Kiu Lau	Carsten Sühl
Orieta Celiku	Ivan Porres Paltor	Koichi Takahasi
Gabriel Ciobanu	Viorel Preoteasa	Dang Van Hung
Steve Dunne	Rimvydas Ruksenas	

Sponsoring Institution

Turku Centre for Computer Science, Turku, Finland

Table of Contents

Invited Talk: Eran Gery

Rhapsody: A Complete Life-Cycle Model-Based Development System	1
<i>Eran Gery, David Harel, and Eldad Palachi</i>	

Integration, Simulation, Animation

An Integrated Semantics for UML Class, Object and State Diagrams Based on Graph Transformation	11
<i>Sabine Kuske, Martin Gogolla, Ralf Kollmann, and Hans-Jörg Kreowski</i>	
Stochastic Process Algebras Meet Eden	29
<i>Natalia López, Manuel Núñez, and Fernando Rubio</i>	

From Specification to Verification

From Implicit Specifications to Explicit Designs in Reactive System Development	49
<i>K. Lano, D. Clark, and K. Androutsopoulos</i>	
Basic-REAL: Integrated Approach for Design, Specification and Verification of Distributed Systems	69
<i>V.A. Nepomniaschy, N.V. Shilov, E.V. Bodin, and V.E. Kozura</i>	
Assume-Guarantee Algorithms for Automatic Detection of Software Failures	89
<i>Mohammad Zulkernine and Rudolph E. Seviora</i>	

Statecharts and B: Integration and Translation

Contributions for Modelling UML State-Charts in B	109
<i>Hung Ledang and Jeanine Souquières</i>	
Translating Statecharts to B	128
<i>Emil Sekerinski and Rafik Zurob</i>	

Invited Talk: Shmuel Katz

A Framework for Translating Models and Specifications	145
<i>Shmuel Katz and Orna Grumberg</i>	

Model Checkers and Theorem Provers

Model Checking Object-Z Using ASM	165
<i>Kirsten Winter and Roger Duke</i>	
Formalization of Cadence SPW Fixed-Point Arithmetic in HOL.....	185
<i>Behzad Akbarpour, Abdelkader Dekdouk, and Sofiène Tahar</i>	
Formally Linking MDG and HOL Based on a Verified MDG System.....	205
<i>Haiyan Xiong, Paul Curzon, Sofiène Tahar, and Ann Blandford</i>	

Links between Object-Z and CSP

Refinement in Object-Z and CSP	225
<i>Christie Bolton and Jim Davies</i>	
Combining Specification Techniques for Processes, Data and Time	245
<i>Jochen Hoenicke and Ernst-Rüdiger Olderog</i>	
An Integration of Real-Time Object-Z and CSP for Specifying Concurrent Real-Time Systems	267
<i>Graeme Smith</i>	

Invited Talk: Stuart Kent

Model Driven Engineering	286
<i>Stuart Kent</i>	

Combining Graphical and Formal Approaches

The Design of a Tool-Supported Graphical Notation for Timed CSP.....	299
<i>Phillip J. Brooke and Richard F. Paige</i>	
Combining Graphical and Formal Development of Open Distributed Systems	319
<i>Einar B. Johnsen, Wenhui Zhang, Olaf Owe, and Demissie B. Aredo</i>	
Translations between Textual Transition Systems and Petri Nets.....	339
<i>Katerina Korenblat, Orna Grumberg, and Shmuel Katz</i>	

Refinement and Proof

Specification and Proof of Liveness Properties under Fairness Assumptions in B Event Systems	360
<i>Héctor Ruíz Barradas and Didier Bert</i>	
Minimally and Maximally Abstract Retrenchments	380
<i>C. Jeske and R. Banach</i>	

Author Index	401
---------------------------	-----