

Lecture Notes in Computer Science

2469

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

Springer

Berlin

Heidelberg

New York

Barcelona

Hong Kong

London

Milan

Paris

Tokyo

Werner Damm Ernst-Rüdiger Olderog (Eds.)

Formal Techniques in Real-Time and Fault-Tolerant Systems

7th International Symposium, FTRTFT 2002

Co-sponsored by IFIP WG 2.2

Oldenburg, Germany, September 9-12, 2002

Proceedings



Springer

Series Editors

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

Volume Editors

Werner Damm
Ernst-Rüdiger Olderog
Fachbereich Informatik, Universität Oldenburg
Ammerländer Herrstr. 114-118, 26129 Oldenburg, Germany
E-mail: {damm,olderog}@informatik.uni-oldenburg.de

Cataloging-in-Publication Data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Formal techniques in real time and fault tolerant systems : 7th international symposium ; proceedings / FTRTFT 2002, Oldenburg, Germany, September 9 - 12, 2002. Werner Damm ; Ernst-Rüdiger Olderog (ed.).
Co-sponsored by IFIP WG 2.2. - Berlin ; Heidelberg ; New York ; Barcelona ; Hong Kong ; London ; Milan ; Paris ; Tokyo : Springer, 2002
(Lecture notes in computer science ; Vol. 2469)
ISBN 3-540-44165-4

CR Subject Classification (1998): D.3.1, F.3.1, C.1.m, C.3, B.3.4, B.1.3

ISSN 0302-9743

ISBN 3-540-44165-4 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: 10871306 06/3142 5 4 3 2 1 0

Preface

This volume contains the proceedings of FTRTFT 2002, the International Symposium on *Formal Techniques in Real-Time and Fault-Tolerant Systems*, held at the University of Oldenburg, Germany, 9–12 September 2002. This symposium was the seventh in a series of FTRTFT symposia devoted to problems and solutions in safe system design. The previous symposia took place in Warwick 1990, Nijmegen 1992, Lübeck 1994, Uppsala 1996, Lyngby 1998, and Pune 2000. Proceedings of these symposia were published as volumes 331, 571, 863, 1135, 1486, and 1926 in the LNCS series by Springer-Verlag. This year the symposium was co-sponsored by IFIP Working Group 2.2 on *Formal Description of Programming Concepts*.

The symposium presented advances in the development and use of formal techniques in the design of real-time, hybrid, fault-tolerant embedded systems, covering all stages from requirements analysis to hardware and/or software implementation. Particular emphasis was placed on UML-based development of real-time systems. Through invited presentations, links between the dependable systems and formal methods research communities were strengthened. With the increasing use of such formal techniques in industrial settings, the conference aimed at stimulating cross-fertilization between challenges in industrial usages of formal methods and advanced research.

In response to the call for papers, 39 submissions were received. Each submission was reviewed by four program committee members assisted by additional referees. At the end of the reviewing process, the program committee accepted 17 papers for presentation at the symposium.

These proceedings contain revised versions of the accepted papers addressing the following topics that constituted the sessions of the symposium:

- Synthesis and Scheduling
- Timed Automata
- Bounded Model Checking of Timed Systems
- Verification and Conformance Testing
- UML Models and Model Checking

The program of the symposium was enriched by two invited tutorials:

- J. McDermid, *Software Hazard and Safety Analysis*
- K.G. Larsen, *Advances in Real-Time Model Checking*

and by six invited lectures:

- G. Buttazzo, *Real-Time Operating Systems: Problems and Solutions*
- B.P. Douglass, *Real-Time UML*
- D. Kozen, *Efficient Code Certification for Open Firmware*
- A. Pnueli, *Applications of Formal Methods in Biology*

- J. Rushby, *An Overview of Formal Verification for the Time-Triggered Architecture*
- J. Sifakis, *Scheduler Modeling Based on the Controller Synthesis Paradigm*

These proceedings also contain two overview papers by the tutorial speakers and four papers and two abstracts by the other invited speakers.

Program Committee

The program committee of FTRTFT 2002 consisted of:

R. Alur, Pennsylvania	R. de Lemos, Kent
F.S. de Boer, Utrecht	O. Maler, Grenoble
M. Broy, München	E.-R. Olderog, Oldenburg (co-chair)
A. Burns, York	A. Pnueli, Rehovot
W. Damm, Oldenburg (co-chair)	A.P. Ravn, Aalborg
J. McDermid, York	W.P. de Roever, Kiel
T. Henzinger, Berkeley	J. Rushby, Stanford
B. Jonsson, Uppsala	D. Sangiorgi, Sophia-Antipolis
M. Joseph, Pune	J. Sifakis, Grenoble
K.G. Larsen, Aalborg	B. Steffen, Dortmund

Additional Referees

We are very grateful to the following persons who assisted in reviewing the submissions:

N. Audsley	J. Hooman	O. Niese	A. Sreenivas
E. Asarin	A. Hughes	T. Noll	M. Steffen
R. Banach	H. Hungar	D. von Oheimb	A. Tiwari
M. von der Beeck	A. de Groot	O. Rüthing	S. Tripakis
G. Behrmann	J. Knoop	G.K. Palshikar	R. Venkatesh
A. Bouajjani	M. Kyas	M. Périn	B. Victor
P. Bouyer	Y. Lakhnech	P. Pettersson	M. Vidyasagar
P. Braun	S. La Torre	C. Pierik	E. de Vink
M. Cerioli	P. Makowski	B. Schätz	R. Wiesniewski
D. Dams	N. Mitra	O. Slotosch	H. Wimmel
B. Dutertre	J.-F. Monin	O. Sokolsky	A. Wißpeintner
E. Fleury	L. Mounier	M. Sorea	W. Yi
M. Fränzle	M. Müller-Olm	K. Spies	S. Yovine

Steering Committee

The steering committee of the FTRTFT series of symposia consists of M. Joseph, Pune; A. Pnueli, Rehovot; H. Rischel, Lyngby; W.-P. de Roever, Kiel; J. Yytopil, Nijmegen.

Organizing Committee

A team of members of the Fachbereich Informatik, Universität Oldenburg, and the institute OFFIS helped us in organizing the FTRTFT 2002. We would like to thank Henning Dierks, Martin Fränze, Andrea Göken, Jochen Hoenicke, Bernhard Josko, Michael Möller, Christiane Stückemann, and Heike Wehrheim for their continuing support.

Sponsors

FTRTFT 2002 received generous support from the following institutions:

- Fachbereich Informatik, Universität Oldenburg
- OFFIS, Oldenburg
- Deutsche Forschungsgemeinschaft, Bonn (DFG)
- European IST-Project OMEGA
- BMW AG, München
- DaimlerChrysler AG, Stuttgart

Finally, we wish you, the reader of these proceedings, many new insights from studying the subsequent papers.

July 2002

W. Damm and E.-R. Olderog

Table of Contents

I Invited Tutorials

- UPPAAL Implementation Secrets 3
*Gerd Behrmann, Johan Bengtsson, Alexandre David, Kim G. Larsen,
Paul Pettersson, and Wang Yi*
- Software Hazard and Safety Analysis 23
John McDermid

II Invited Papers

- Real-Time Operating Systems: Problems and Novel Solutions 37
Giorgio Buttazzo
- Real-Time UML 53
Bruce Powel Douglass
- Eager Class Initialization for Java 71
Dexter Kozen and Matt Stillerman
- Applications of Formal Methods in Biology 81
Amir Pnueli
- An Overview of Formal Verification for the Time-Triggered Architecture . . 83
John Rushby
- Scheduler Modeling Based on the Controller Synthesis Paradigm 107
Joseph Sifakis

III Synthesis and Scheduling

- Component-Based Synthesis of Dependable Embedded Software 111
Arshad Jhumka, Martin Hiller, and Neeraj Suri
- From the Specification to the Scheduling of Time-Dependent Systems . . . 129
Christophe Lohr and Jean-Pierre Courtiat
- On Control with Bounded Computational Resources 147
Oded Maler, Bruce H. Krogh, and Moez Mahfoudh

IV Timed Automata I

- Decidability of Safety Properties of Timed Multiset Rewriting 165
Mitsuharu Yamamoto, Jean-Marie Cottin, and Masami Hagiya

Extending Timed Automaton and Real-Time Logic
to Many-Valued Reasoning 185
*Ana Fernández Vilas, José J. Pazos Arias,
and Rebeca P. Díaz Redondo*

Fault Diagnosis for Timed Automata 205
Stavros Tripakis

V Bounded Model Checking

Verification of Timed Automata via Satisfiability Checking 225
*Peter Niebert, Moez Mahfoudh, Eugene Asarin, Marius Bozga,
Oded Maler, and Navendu Jain*

Take It NP-Easy: Bounded Model Construction for Duration Calculus 245
Martin Fränzle

Towards Bounded Model Checking for the Universal Fragment of TCTL . . 265
Wojciech Penczek, Bożena Woźna, and Andrzej Zbrzezny

VI Verification and Conformance Testing

A Typed Interrupt Calculus 291
Jens Palsberg and Di Ma

Parametric Verification of a Group Membership Algorithm 311
Ahmed Bouajjani and Agathe Merceron

A Method for Testing the Conformance of Real Time Systems 331
Ahmed Khoumsi

VII UML Models and Model Checking

A Probabilistic Extension of UML Statecharts 355
David N. Jansen, Holger Hermanns, and Joost-Pieter Katoen

Eliminating Queues from RT UML Model Representations 375
Werner Damm and Bengt Jonsson

Model Checking – Timed UML State Machines and Collaborations 395
Alexander Knapp, Stephan Merz, and Christopher Rauh

VIII Timed Automata II

Partial Order Path Technique for Checking Parallel Timed Automata 417
Jianhua Zhao, He Xu, Xuandong Li, Tao Zheng, and Guoliang Zheng

Constructing Test Automata from Graphical Real-Time Requirements 433
Henning Dierks and Marc Lettrari

Author Index 455