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

Springer-Verlag Berlin Heidelberg New York
a member of BertelsmannSpringer Science+Business Media GmbH

http://www.springer.de

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

Additional Referees

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

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

Steering Committee

The steering committee of the FTRTFT series of symposia consists of M. Joseph, Pune; A. Pnueli, Rehvot; 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 Fränzle, 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