

Lecture Notes in Computer Science

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

1486

Anders P. Ravn Hans Rischel (Eds.)

Formal Techniques in Real-Time and Fault-Tolerant Systems

5th International Symposium, FTRTFT'98
Lyngby, Denmark, September 14-18, 1998
Proceedings



Springer

Series Editors

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

Volume Editors

Anders P. Ravn
Hans Rischel
Technical University of Denmark
Department of Information Technology
Building 344, DK-2800 Lyngby, Denmark
E-mail: {apr,rischel}@it.dtu.dk

Cataloging-in-Publication data applied for

Die Deutsche Bibliothek - CIP-Einheitsaufnahme

Formal techniques in real time and fault tolerant systems : 5th international symposium ; proceedings / FTRTFT '98, Lyngby, Denmark, September 14 - 18, 1998. Anders P. Ravn ; Hans Rischel (ed.). - Berlin ; Heidelberg ; New York ; Barcelona ; Budapest ; Hong Kong ; London ; Milan ; Paris ; Singapore ; Tokyo : Springer, 1998 (Lecture notes in computer science ; 1486) ISBN 3-540-65003-2

CR Subject Classification (1991): D.3.1, F.3.1, C.1.m, C.3, B.3.4, B.1.3, D.4.5, D.4.7

ISSN 0302-9743

ISBN 3-540-65003-2 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 1998
Printed in Germany

Typesetting: Camera-ready by author
SPIN 10638813 06/3142 - 5 4 3 2 1 0 Printed on acid-free paper

Preface

Embedded systems have become a hot topic in computer science because technology has made computers very powerful and very inexpensive. Thus it becomes possible and economically feasible to embed sophisticated computational models for the control of physical systems even in common appliances, automobiles, etc. Such applications must conform to physical laws dictated by their construction and their intended use, i.e., the computations must interact with a dynamical system which has timing constraints on when certain actions must occur. The computations have hard real-time constraints. Furthermore, some of the applications must continue to work even in the presence of intermittent or permanent faults in the electronics, thus they must be fault tolerant.

Engineering of embedded systems must thus rely on models for real-time and fault-tolerant computing. Mathematical foundations for developing, understanding and applying such models are the topic of this school and symposium. It is the fifth in a line of international schools and symposia; the previous ones were held in Warwick 1989, at Nijmegen 1992, at Lübeck 1994, and in Uppsala 1996. The proceedings of the symposia are published in LNCS 331, 571, 863, and 1135.

The lectures at the school are given by Albert Benveniste (IRISA, Rennes, France), Gérard Le Lann (INRIA Le Chesnay, France), Jan Peleska (Bremen, Germany), Jørgen Staunstrup (Lyngby, Denmark), and Frits Vaandrager (Nijmegen, The Netherlands). Invited presentations at the symposium are given by Connie Heitmeyer (Naval Res. Lab., USA), John Knight (Virginia, USA), Amir Pnueli (Weizmann Inst., Israel), and Joseph Sifakis (VERIMAG, France). We thank the lecturers and speakers for their contributions.

The program committee selected 22 papers for presentation. In addition the symposium has 5 tool demonstrations with short presentations in this volume.

This school and symposium is supported by the Technical University of Denmark, in particular the Department of Information Technology, and by the Danish Technical Research Council. The school is also supported by The Danish Research Academy via The Graduate School in Microelectronics. Local publicity has been supported by DELTA and IFAD. We are very grateful for this support which has made this event possible.

We shall also like to thank the steering committee for valuable advice, and to thank Disa la Cour, Maria Hansen, and Karin S. Mogensen for their enthusiastic practical support.

Lyngby, July 1998

Anders P. Ravn, Hans Rischel

Program Committee

Ralph-Johan Back (Åbo Akademi, Turko)
 A. Burns (Univ. of York)
 C. Dwork (IBM Almaden)
 T. Henzinger (Cornell Univ., Ithaca, N.Y.)
 J. Hooman (Eindhoven Univ. of Technology)
 B. Jonsson (Uppsala Univ.)
 M. Joseph (Univ. of Warwick)
 Y. Lakhnech (Kiel)
 K. Larsen (Aalborg Univ.)
 N. Leveson (Univ. of Washington)
 J. Madsen (DTU, Lyngby)
 D. Mandrioli (Pol. Milano)
 A. Mok (Univ. of Texas, Austin)
 E.-R. Olderog (Univ. of Oldenburg)
 J. Parrow (Royal Inst. of Technology, Stockholm)
 A. Pnueli (Weizmann Inst., Rehovot)
 A.P. Ravn (co-chair) (DTU, Lyngby)
 H. Rischel (co-chair) (DTU, Lyngby)
 W.-P. de Roever (Univ. of Kiel)
 J. Sifakis (IMAG-LGI, Grenoble)
 J. Vytopil (Kath. Univ., Nijmegen)
 Chaochen Zhou (UNU/IIST, Macau)

Steering Committee

M. Joseph (Univ. of Warwick)
 A. Pnueli (Weizmann Inst., Rehovot)
 H. Rischel (DTH, Lyngby)
 W.-P. de Roever (Univ. of Kiel)
 J. Vytopil (Kath. Univ., Nijmegen)

Referees

Henrik R. Andersen	Henrik Hulgaard	Erich Mikk	Hongyan Sun
Saddek Bensalem	Dang Van Hung	Simon Mørk	Luis Urbina
Henning Dierks	Wang Ji	Xu Qiwen	Poul F. Williams
Pablo Giambiagi	Burghard v. Karger	Kaisa Sere	Hanno Wupper
H. Griffioen	Johan Lilius	Michael Schenke	Wang Yi
Michael R. Hansen	Hans H. Løvengreen	Steve Schneider	
Anne Haxthausen	Angelika Mader	Jens U. Skakkebæk	

Contents

Invited Lectures

Challenges in the Utilization of Formal Methods	1
J. C. Knight	
On the Need for "Practical" Formal Methods	18
C. Heitmeyer	
A General Framework for the Composition of Timed Systems	27
J. Sifakis	

Selected Presentations

Temporal Logic

Operational and Logical Semantics for Polling Real-Time Systems	29
H. Dierks, A. Fehnker, A. Mader, F. Vaandrager	
A Finite-Domain Semantics for Testing Temporal Logic Specifications	41
A. Coen-Porisini, M. Pradella, P. San Pietro	
Duration Calculus of Weakly Monotonic Time	55
P. K. Pandya, Dang Van Hung	

Requirements Engineering

Reuse in Requirements Engineering: Discovery and Application of a Real-Time Requirement Pattern	65
R. Gotzhein, M. Kronenburg, C. Peper	
A Modular Visual Model for Hybrid Systems	75
R. Grosu, T. Stauner, M. Broy	
Integrating Real-Time Structured Design and Formal Techniques	92
D. Priddin, A. Burns	
Duration Calculus in the Specification of Safety Requirements	103
S. Veloudis, N. Nissanke	

Analysis Techniques

Automated Stream-Based Analysis of Fault-Tolerance	113
S. D. Stoller, F. B. Schneider	
Designing a Provably Correct Robot Control System Using a 'Lean' Formal Method	123
A. Cau, C. Czarnecki, H. Zedan	
Static Analysis to Identify Invariants in RSML Specifications	133
D. Y. W. Park, J. U. Skakkebæk, D. L. Dill	
Partition Refinement in Real-Time Model Checking	143
R. L. Spelberg, H. Toeteneel, M. Ammerlaan	

Verification

Formal Verification of Stabilizing Systems	158
M. Siegel	

Synchronizing Clocked Transition Systems	173
M. Poel, J. Zwiers	
Some Decidability Results for Duration Calculus under Synchronous Interpretation	186
M. Satpathy, Dang Van Hung, P. K. Pandya	
Fair Synchronous Transition Systems and Their Liveness Proofs	198
A. Pnueli, N. Shankar, E. Singerman	
Model Checking	
Dynamical Properties of Timed Automata	210
A. Puri	
An Algorithm for the Approximative Analysis of Rectangular Automata ..	228
J. Preußig, S. Kowalewski, H. Wong-Toi, T.A. Henzinger	
On Checking Parallel Real-Time Systems for Linear Duration Properties ..	241
J. Zhao, Dang Van Hung	
A Practical and Complete Algorithm for Testing Real-Time Systems	251
R. Cardell-Oliver, T. Glover	
Applications	
Mechanical Verification of Clock Synchronization Algorithms	262
D. Schwier, F. von Henke	
Compiling Graphical Real-Time Specifications into Silicon	272
M. Fränzle, K. Lüth	
Towards a Formal Semantics of Verilog Using Duration Calculus	282
G. Schneider, Q. Xu	
Tools Demonstrations	
The ICOS Synthesis Environment	294
K. Lüth	
KRONOS: A Model-Checking Tool for Real-Time Systems	298
M. Bozga, C. Daws, O. Maler, A. Olivero, S. Tripakis, S. Yovine	
SGLOT: A Visual Tool for Structural LOTOS Specifications	303
M. Marrero, A. Suárez, E. Carrión, E. Macías	
Discrete-Time Promela and Spin	307
D. Bošnački, D. Dams	
MOBY/PLC – Graphical Development of PLC-Automata	311
J. Tapken, H. Dierks	
Invited Paper	
Predictability in Critical Systems	315
G. Le Lann	
Author Index	339