

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zurich, Switzerland

John C. Mitchell

Stanford University, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

Oscar Nierstrasz

University of Bern, Switzerland

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

New York University, NY, USA

Doug Tygar

University of California, Berkeley, CA, USA

Moshe Y. Vardi

Rice University, Houston, TX, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Yassine Lakhnech Sergio Yovine (Eds.)

Formal Techniques, Modelling and Analysis of Timed and Fault-Tolerant Systems

Joint International Conferences
on Formal Modelling and Analysis of Timed Systems, FORMATS 2004
and Formal Techniques in Real-Time and Fault-Tolerant Systems, FTRTFT 2004
Grenoble, France, September 22-24, 2004
Proceedings

Volume Editors

Yassine Lakhnech

Sergio Yovine

Verimag Laboratory

2 av. de Vignate, 38610 Grenoble, France

E-mail: {Yassine.Lakhnech, Sergio.Yovine}@imag.fr

Library of Congress Control Number: 2004112582

CR Subject Classification (1998): D.3.1, F.3.1, C.1.m, C.3, B.3.4, B.1.3, D.2.4

ISSN 0302-9743

ISBN 3-540-23167-6 Springer 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. Violations are liable to prosecution under the German Copyright Law.

Springer is a part of Springer Science+Business Media

springeronline.com

© Springer-Verlag Berlin Heidelberg 2004

Printed in Germany

Typesetting: Camera-ready by author, data conversion by Olgun Computergrafik

Printed on acid-free paper SPIN: 11324249 06/3142 5 4 3 2 1 0

Preface

This volume contains the proceedings of the joint conference on *Formal Modelling and Analysis of Timed Systems* (FORMATS) and *Formal Techniques in Real-Time and Fault Tolerant Systems* (FTRTFT), held in Grenoble, France, on September 22–24, 2004. The conference united two previously independently organized conferences FORMATS and FTRTFT. FORMATS 2003 was organized as a satellite workshop of CONCUR 2003 and was related to three independently started workshop series: MTCS (held as a satellite event of CONCUR 2000 and CONCUR 2002), RT-TOOLS (held as a satellite event of CONCUR 2001 and FLoC 2002) and TPTS (held at ETAPS 2002). FTRTFT is a symposium that was held seven times before: in Warwick 1988, Nijmegen 1992, Lübeck 1994, Uppsala 1996, Lyngby 1998, Pune 2000 and Oldenburg 2002. The proceedings of these symposia were published as volumes 331, 571, 863, 1135, 1486, 1926, and 2469 in the LNCS series by Springer.

This joint conference is dedicated to the advancement of the theory and practice of the modelling, design and analysis of real-time and fault-tolerant systems. Indeed, computer systems are becoming increasingly widespread in real-time and safety-critical applications such as embedded systems. Such systems are characterized by the crucial need to manage their complexity in order to produce reliable designs and implementations. The importance of timing aspects, performance and fault-tolerance is continuously growing. Formal techniques offer a foundation for systematic design of complex systems. They have beneficial applications throughout the engineering process, from the capture of requirements through specification, design, coding and compilation, down to the hardware that embeds the system into its environment. The joint conference is devoted to considering the problems and the solutions in designing real-time and/or fault-tolerant systems, and to examining how well the use of advanced design techniques and formal methods for design, analysis and verification serves in relating theory to practice.

We received 70 paper submissions out of which 24 were selected for publication. Each submission received an average of 3 referee reviews. The conference program included three invited talks, by Greg Bollella (Sun Microsystems Laboratories), Paul Feautrier (LIP, École Normale Supérieure de Lyon, France) and Peter Ryan (School of Computing Science, University of Newcastle upon Tyne, UK).

We would like to thank all the Program Committee members and the sub-referees. Our thanks also go to the Steering Committee members of FORMATS and FTRTFT. We also thank Claudia Laidet who assisted us in organizing the conference.

July 2004

Yassine Lakhnech and Sergio Yovine
Program Chairs

Joint Conference FORMATS 2004 and FTRTFT 2004

Organization

The joint conference FORMATS and FTRTFT 2004 was organized by VERIMAG (<http://www-verimag.imag.fr>) with the support of: IMAG (Institut d'Informatique et Mathématiques Appliquées de Grenoble), CNRS (Centre National de Recherche Scientifique), Université Joseph Fourier, and INPG (Institut National Polytechnique de Grenoble), as well as the city of Grenoble.

Program Committee

Luca de Alfaro (UCSC, USA)
Eugene Asarin (LIAFA, France)
Patricia Bouyer (LSV, France)
Flavio Corradini (Univ. di L'Aquila Italy)
Jordi Cortadella (UPC Spain)
Pedro D'Argenio (FAMAF, Argentina)
Alain Girault (INRIA, France)
Tom Henzinger (Berkeley, USA)
Mathai Joseph (TCS, India)
Marta Kwiatkowska (Univ. Birmingham, UK)
Yassine Lakhnech (VERIMAG, co-chair, France)
Kim Larsen (Aalborg University, Denmark)
Claude Le Pape (Ilog SA, France)
Ernst-Ruediger Olderog (Univ. Oldenburg)
Jens Palsberg (UCLA, USA)
P. Madhusudan (Univ. Pennsylvania, USA)
Amir Pnueli (NYU, USA)
Jean-Francois Raskin (ULB, Belgium)
Willem-Paul de Roever (Univ. Kiel, Germany)
John Rushby (SRI, USA)
Henny Sipma (Stanford, USA)
Steve Vestal (Honeywell, USA)
Wang Yi (Uppsala University, Sweden)
Sergio Yovine (VERIMAG, co-chair, France)

Referees

M. Baclet	M. Dufлот	J. Ober
G. Behrmann	E. Dumitrescu	A. Oliveras
M. Bernardo	H. Fecher	Ju Pang
P. Bhaduri	J.C. Fernandez	J. Pearson
I. Bozga	E. Fleury	P. Pettersson
M. Bozga	P. Ganty	C. Picaronny
V. Braberman	G. Geeraerts	M. Pouzet
M. Bujorianu	G. Goessler	V. Prabhu
D.R. Cacciagrano	O. Grinchtein	J.I. Rasmussen
P. Caspi	D. Guelev	E. Rutten
F. Cassez	H. Kalla	T.C. Ruys
A. Chakrabarti	V. Khomenko	G. Saiz
S. Chakraborty	P. Krcal	C. Sanchez
R. Clariso	T. Krilavicius	S. Sankaranarayanan
A. Collomb	M. Kyas	A. Skou
S. Cotton	F. Laroussinie	J. Sproston
R. Culmone	L. Lavagno	M. Steffen
A. David	G. Luetngen	L. Tesei
C. Daws	B. Lukoschus	P.S. Thiagarajan
S. Demri	N. Markey	Ting Zhang
M. De Wulf	M. Mikucionis	S. Tripakis
M.R. Di Berardini	L. Mokrushin	R. Venkatesh
H. Dierks	L. Mounier	N. Wolovick
D. Di Ruscio	S. Neuendorffer	Wang Xu
C. Dima	B. Nielsen	T. Yoneda
L. Doyen	G. Norman	Yi Zhang
D. D'Souza	I. Ober	

Table of Contents

Invited Papers

From Software to Hardware and Back	1
<i>Paul Feautrier</i>	
Of Elections and Electrons	3
<i>Peter Y. Ryan</i>	

Regular Papers

Formal Verification of an Avionics Sensor Voter Using SCADE	5
<i>Samar Dajani-Brown, Darren Cofer, and Amar Bouali</i>	
Mixed Delay and Threshold Voters in Critical Real-Time Systems	21
<i>Chiheb Kossentini and Paul Caspi</i>	
Towards a Methodological Approach to Specification and Analysis of Dependable Automation Systems	36
<i>Simona Bernardi, Susanna Donatelli, and Giovanna Dondossola</i>	
On Two-Sided Approximate Model-Checking: Problem Formulation and Solution via Finite Topologies	52
<i>Jennifer M. Davoren, Thomas Moor, R.P. Goré, Vaughan Coulthard, and Anil Nerode</i>	
On Timed Automata with Input-Determined Guards	68
<i>Deepak D'Souza and Nicolas Tabareau</i>	
Decomposing Verification of Timed I/O Automata	84
<i>Dilsun Kırık Kaynar and Nancy Lynch</i>	
Symbolic Model Checking for Simply-Timed Systems	102
<i>Nicolas Markey and Philippe Schnoebelen</i>	
Robustness and Implementability of Timed Automata	118
<i>Martin De Wulf, Laurent Doyen, Nicolas Markey, and Jean-François Raskin</i>	
Real-Time Testing with Timed Automata Testers and Coverage Criteria ..	134
<i>Moez Krichen and Stavros Tripakis</i>	
Monitoring Temporal Properties of Continuous Signals	152
<i>Oded Maler and Dejan Nickovic</i>	

A Unified Fault-Tolerance Protocol	167
<i>Paul Miner, Alfons Geser, Lee Pike, and Jeffrey Maddalon</i>	
Automating the Addition of Fail-Safe Fault-Tolerance: Beyond Fusion-Closed Specifications	183
<i>Felix C. Gärtner and Arshad Jhumka</i>	
Modeling and Verification of a Fault-Tolerant Real-Time Startup Protocol Using Calendar Automata	199
<i>Bruno Dutertre and Maria Sorea</i>	
Static Fault-Tolerant Real-Time Scheduling with “Pseudo-topological” Orders	215
<i>Cătălin Dima, Alain Girault, and Yves Sorel</i>	
The Influence of Durational Actions on Time Equivalences	231
<i>Harald Fecher</i>	
Bounded Model Checking for Region Automata	246
<i>Fang Yu, Bow-Yaw Wang, and Yao-Wen Huang</i>	
Some Progress in Satisfiability Checking for Difference Logic	263
<i>Scott Cotton, Eugene Asarin, Oded Maler, and Peter Niebert</i>	
Model-Checking for Weighted Timed Automata	277
<i>Thomas Brihaye, Véronique Bruyère, and Jean-François Raskin</i>	
Symbolic Model Checking for Probabilistic Timed Automata	293
<i>Marta Kwiatkowska, Gethin Norman, Jeremy Sproston, and Fuzhi Wang</i>	
Structured Modeling of Concurrent Stochastic Hybrid Systems	309
<i>Mikhail Bernadsky, Raman Sharykin, and Rajeev Alur</i>	
Computing Schedules for Multithreaded Real-Time Programs Using Geometry	325
<i>Philippe Gerner and Thao Dang</i>	
Forward Reachability Analysis of Timed Petri Nets	343
<i>Parosh Aziz Abdulla, Johann Deneux, Pritha Mahata, and Aletta Nylén</i>	
Lazy Approximation for Dense Real-Time Systems	363
<i>Maria Sorea</i>	
Learning of Event-Recording Automata	379
<i>Olga Grinchtein, Bengt Jonsson, and Martin Leucker</i>	
Author Index	397