

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

Alfred Kobsa

University of California, Irvine, CA, 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

Microsoft Research, Cambridge, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Darren Cofer Alessandro Fantechi (Eds.)

Formal Methods for Industrial Critical Systems

13th International Workshop, FMICS 2008
L'Aquila, Italy, September 15-16, 2008
Revised Selected Papers

Volume Editors

Darren Cofer
Rockwell Collins
7805 Telegraph Rd. 100, Bloomington, MN 55438, USA
E-mail: ddcofer@rockwellcollins.com

Alessandro Fantechi
Università di Firenze, Dipartimento di Sistemi e Informatica
Via S. Marta 3, 50139 Firenze, Italy
E-mail: fantechi@dsi.unifi.it

Library of Congress Control Number: 2009930950

CR Subject Classification (1998): D.2.4, D.2, D.3, C.3, F.3

LNCS Sublibrary: SL 2 – Programming and Software Engineering

ISSN 0302-9743
ISBN-10 3-642-03239-7 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-03239-4 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.com

© Springer-Verlag Berlin Heidelberg 2009
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12711871 06/3180 5 4 3 2 1 0

Preface

The aim of the FMICS workshop series is to provide a forum for researchers who are interested in the development and application of formal methods in industry. In particular, these workshops are intended to bring together scientists and practitioners who are active in the area of formal methods and interested in exchanging their experiences in the industrial usage of these methods. These workshops also strive to promote research and development for the improvement of formal methods and tools for industrial applications.

The topics for which contributions to FMICS 2008 were solicited included, but were not restricted to, the following:

- Design, specification, code generation and testing based on formal methods
- Verification and validation of complex, distributed, real-time systems and embedded systems
- Verification and validation methods that address shortcomings of existing methods with respect to their industrial applicability (e.g., scalability and usability issues)
- Tools for the development of formal design descriptions
- Case studies and experience reports on industrial applications of formal methods, focusing on lessons learned or identification of new research directions
- Impact of the adoption of formal methods on the development process and associated costs
- Application of formal methods in standardization and industrial forums

The workshop included six sessions of regular contributions in the areas of model checking, testing, software verification, real-time performance, and industrial case studies. There were also three invited presentations, given by Steven Miller, Rance Cleaveland, and Werner Damm, covering the application of formal methods in the avionics and automotive industries.

Moreover, a panel was organized on the topic “Formal Methods in Commercial SW Development Tools.” The aim of this panel was to promote discussion of current and foreseen applications of formal methods within model-based development frameworks that include formal analysis and generation methods for software design.

Out of the 36 submissions to FMICS 2008, 14 papers were accepted for presentation at the workshop, as well as two short presentations to serve as an introduction to the panel. We wish to thank the members of the Program Committee and the additional reviewers for their careful evaluation of the submitted papers. We also acknowledge the effort of all the members of the Program Committee in constructive discussions during the electronic program selection meeting. Special

thanks for the efforts devoted to the organization of the workshop go to the staff of the ASE 2008 conference, with which this workshop was co-located.

September 2008

Darren Cofer
Alessandro Fantechi

The FMICS 2008 workshop was hosted by the warm people of L'Aquila, Italy, and by the historic buildings of the city. Workshop participants had the occasion to stroll in the peaceful narrow streets of the old center, and to visit the magnificent monuments and churches that were built in the city several centuries ago.

On Monday, April 6, 2009, a severe earthquake hit the city, followed by more aftershocks in the following days. Hundreds of lives were lost, thousands were injured, and many houses and major historical buildings collapsed or were severely damaged. The vivid images in the memories of the workshop participants have been replaced by pictures of destruction from the media.

It is our hope that the proud, tireless and industrious people of the Abruzzo region will one day be able to bring back the city and the region to what the FMICS guests experienced.

April 2009

Darren Cofer
Alessandro Fantechi

Organization

FMICS 2008 was organized by the ERCIM Working Group on Formal Methods for Industrial Critical Systems.

Program Chairs

Darren Cofer

Alessandro Fantechi

Rockwell Collins, USA

Università di Firenze and ISTI-CNR, Italy

Program Committee

Maria Alpuente

Alvaro Arenas

Lubos Brim

Wan Fokkink

Patrice Godefroid

Leszek Holenderski

Roope Kaivola

Stefan Kowalewski

Stefania Gnesi

Mark Lawford

Stefan Leue

Radu Mateescu

Charles Pecheur

Francois Pilarski

Ralf Pinger

Murali Rangarajan

Marco Roveri

Ina Schieferdecker

Wilfried Steiner

Universidad Politècnica de Valencia, Spain

STFC RAL, UK

Masaryk University, Czech Republic

Vrije Universiteit Amsterdam, The Netherlands

Microsoft Research, USA

Philips Research, The Netherlands

Intel, USA

RWTH Aachen, Germany

ISTI-CNR, Italy

McMaster University, Canada

University of Konstanz, Germany

INRIA Rhone-Alpes, France

Université Catholique de Louvain, Belgium

Airbus, France

Siemens, Germany

Honeywell, USA

IRST, Italy

Fraunhofer FOKUS, Germany

TTTech, Austria

Additional Referees

Jiri Barnat

Robert Beers

Dragan Bosnacki

Goetz Botterweck

Marco Bozzano

Calame Jens

Masaryk University, Czech Republic

Intel, USA

Eindhoven University of Technology,
The Netherlands

Lero, Ireland

Fondazione Bruno Kessler, Italy

CWI, The Netherlands

VIII Organization

Alessio Ferrari	Università di Firenze, Italy
Jan Friso Groote	Eindhoven University of Technology, The Netherlands
Jose Iborra	Universidad Politècnica de Valencia, Spain
Christophe Joubert	Universidad Politècnica de Valencia, Spain
Dmitry Korchemny	Intel, USA
Alexandre Korobkine	McMaster University, Canada
Frédéric Lang	INRIA Rhone-Alpes, France)
Giovanni Lombardi	ISTI-CNR, Italy
Franco Mazzanti	ISTI-CNR, Italy
Stefan Milius	Siemens, Germany
Francisco Javier Oliver	Universidad Politècnica de Valencia, Spain
Lucian Patcas	McMaster University, Canada
Bas Ploeger	Eindhoven University of Technology, The Netherlands
Erik Reeber	Intel, USA
Viktor Schuppan	Fondazione Bruno Kessler, Italy
Wendelin Serwe	INRIA Rhone-Alpes, France
Andrey Tchaltsev	Fondazione Bruno Kessler, Italy
Maurice H. ter Beek	ISTI-CNR, Italy
Francesco Tiezzi	Università di Firenze, Italy
Stefano Tonetta	Fondazione Bruno Kessler, Italy
Alicia Villanueva	Universidad Politècnica de Valencia, Spain
Michael Whalen	Rockwell Collins, USA
Anton Wijs	INRIA Rhone-Alpes, France

Table of Contents

Invited Presentations

Formal Methods for Critical Systems (Invited Speaker)	1
<i>Steven P. Miller</i>	
Model-Based Verification of Automotive Control Software (Invited Speaker)	2
<i>Rance Cleaveland</i>	
Contract-Based Analysis of Automotive and Avionics Applications: The SPEEDS Approach (Invited Speaker)	3
<i>Werner Damm</i>	

Panel

Panel Discussion on Formal Methods in Commercial Software Development Tools	4
<i>Alessandro Fantechi and Alessio Ferrari</i>	

Research Papers

LETO - A Lustre-Based Test Oracle for Airbus Critical Systems	7
<i>Guy Durrieu, Hélène Waeselynck, and Virginie Wiels</i>	
Extending Structural Test Coverage Criteria for LUSTRE Programs with Multi-clock Operators	23
<i>Virginia Papailiopoulos, Laya Madani, Lydie du Bousquet, and Ioannis Parissis</i>	
Fighting State Space Explosion: Review and Evaluation	37
<i>Radek Pelánek</i>	
Local Quantitative LTL Model Checking	53
<i>Jiří Barnat, Luboš Brim, Ivana Černá, Milan Česka, and Jana Tůmová</i>	
Efficient Symbolic Model Checking for Process Algebras	69
<i>José Vander Meulen and Charles Pecheur</i>	
Reentrant Readers-Writers: A Case Study Combining Model Checking with Theorem Proving	85
<i>Bernard van Gastel, Leonard Lensink, Sjaak Smetters, and Marko van Eekelen</i>	

Using CSP B Components: Application to a Platoon of Vehicles	103
<i>Samuel Colin, Arnaud Lanoix, Olga Kouchnarenko, and Jeanine Souquières</i>	
Formal Verification of the Implementability of Timing Requirements . . .	119
<i>Xiayong Hu, Mark Lawford, and Alan Wassying</i>	
Dynamic Event-Based Runtime Monitoring of Real-Time and Contextual Properties	135
<i>Christian Colombo, Gordon J. Pace, and Gerardo Schneider</i>	
Can Flash Memory Help in Model Checking?	150
<i>Jiří Barnat, Luboš Brim, Stefan Edelkamp, Damian Sulewski, and Pavel Šimeček</i>	
From Informal Requirements to Property-Driven Formal Validation . . .	166
<i>Alessandro Cimatti, Marco Roveri, Angelo Susi, and Stefano Tonetta</i>	
Automated Certification of Non-Interference in Rewriting Logic	182
<i>Mauricio Alba-Castro, María Alpuente, and Santiago Escobar</i>	
Formal Verification of Safety Functions by Reinterpretation of Functional Block Based Specifications	199
<i>Erzsébet Németh and Tamás Bartha</i>	
Using Datalog and Boolean Equation Systems for Program Analysis . . .	215
<i>María Alpuente, Marco A. Feliú, Christophe Joubert, and Alicia Villanueva</i>	
Author Index	233