Lecture Notes in Computer Science 5596

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

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

Springer

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

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	Rockwell Collins, USA
Alessandro Fantechi	Università di Firenze and ISTI-CNR, Italy

Program Committee

Maria Alpuente	Universidad Politècnica de Valencia, Spain
Alvaro Arenas	STFC RAL, UK
Lubos Brim	Masaryk University, Czech Republic
Wan Fokkink	Vrije Universiteit Amsterdam, The Netherlands
Patrice Godefroid	Microsoft Research, USA
Leszek Holenderski	Philips Research, The Netherlands
Roope Kaivola	Intel, USA
Stefan Kowalewski	RWTH Aachen, Germany
Stefania Gnesi	ISTI-CNR, Italy
Mark Lawford	McMaster University, Canada
Stefan Leue	University of Konstanz, Germany
Radu Mateescu	INRIA Rhone-Alpes, France
Charles Pecheur	Universitè Catholique de Louvain, Belgium
Francois Pilarski	Airbus, France
Ralf Pinger	Siemens, Germany
Murali Rangarajan	Honeywell, USA
Marco Roveri	IRST, Italy
Ina Schieferdecker	Fraunhofer FOKUS, Germany
Wilfried Steiner	TTTech, Austria

Additional Referees

Jiri Barnat	Masaryk University, Czech Republic
Robert Beers	Intel, USA
Dragan Bosnacki	Eindhoven University of Technology, The Netherlands
Goetz Botterweck	Lero, Ireland
Marco Bozzano	Fondazione Bruno Kessler, Italy
Calame Jens	CWI, The Netherlands

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

Panel

Research Papers