Lecture Notes in Computer Science 7437

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

Mariëlle Stoelinga Ralf Pinger (Eds.)

Formal Methods for Industrial Critical Systems

17th International Workshop, FMICS 2012
Paris, France, August 27-28, 2012
Proceedings

Springer

Volume Editors

Mariëlle Stoelinga
University of Twente, Department of Computer Science
Formal Methods and Tools
P.O. Box 217, 7500 AE Enschede, The Netherlands
E-mail: marielle@cs.utwente.nl

Ralf Pinger
Siemens AG, Infrastructure and Cities Sector
Mobility and Logistics Division, Rail Automation
Ackerstraße 22, 38126 Braunschweig, Germany
E-mail: ralf.pinger@siemens.com

ISSN 0302-9743 e-ISSN 1611-3349
ISBN 978-3-642-32468-0 e-ISBN 978-3-642-32469-7
DOI 10.1007/978-3-642-32469-7
Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012943602

CR Subject Classification (1998): D.2.4, F.3.1, D.2, C.3, J.1, J.2, F.1.1

LNCS Sublibrary: SL 2 – Programming and Software Engineering

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Preface

This volume contains the papers presented at FMICS 2012, the 17th International Workshop on Formal Methods for Industrial Critical Systems, taking place August 27–28, 2012, in Paris, France. Previous workshops of the ERCIM Working Group on Formal Methods for Industrial Critical Systems were held in Oxford (March 1996), Cesena (July 1997), Amsterdam (May 1998), Trento (July 1999), Berlin (April 2000), Paris (July 2001), Malaga (July 2002), Trondheim (June 2003), Linz (September 2004), Lisbon (September 2005), Bonn (August 2006), Berlin (July 2007), L'Aquila (September 2008), Eindhoven (November 2009), Antwerp (September 2010), and Trento (August 2011). The FMICS 2012 workshop was co-located with the 18th International Symposium on Formal Methods (FM 2012).

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, FMICS brings together scientists and engineers that are active in the area of formal methods and interested in exchanging their experiences in the industrial usage of these methods. The FMICS workshop series also strives to promote research and development for the improvement of formal methods and tools for industrial applications.

The topics of interest include, but are not limited to:

- Design, specification, code generation and testing based on formal methods
- Methods, techniques and tools to support automated analysis, certification, debugging, learning, optimization and transformation of complex, distributed, dependable, 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

This year we received 37 submissions. Papers had to pass a rigorous review process in which each paper received three reports. The international Program Committee of FMICS 2012 decided to select 14 papers for presentation during the workshop and inclusion in these proceedings. The workshop was highly enriched by our two invited talks given by Dimitra Giannakopoulou, NASA Ames, USA, and Hubert Garavel, INRIA Grenoble Rhone-Alpes, France.

We would like to thank the local organizers Kamel Barkaoui, CNAM Paris, and Béatrice Bérard, University Pierre et Marie Curie, for taking care of all the local arrangements in Paris, the ERCIM FMICS working group coordinator Radu Mateescu, INRIA Grenoble, for his fruitful discussions, and especially Alessandro Fantechi, Università degli Studi di Firenze and ISTI-CNR, Italy, for inviting us to co-chair this workshop, EasyChair for supporting the review process, Springer for the publication, all Program Committee members and external reviewers for their substantial reviews and discussions, all authors for submitting 37 papers and all attendees of the workshop. Thanks to all for making FMICS 2012 a success.

August 2012

Mariëlle Stoelinga
Ralf Pinger

Organization

Program Committee

Lubos Brim	Masaryk University, Czech Republic
Alessandro Cimatti	FBK-irst, Italy
Maria Del Mar Gallardo	University of Malaga, Spain
Michael Dierkes	Rockwell Collins, France
Cindy Eisner	IBM Haifa, Israel
Georgios Fainekos	Arizona State University, USA
Alessandro Fantechi	DSI - Università di Firenze, Italy
Holger Hermanns	Saarland University, Germany
Michaela Huhn	Technische Universität Clausthal, Institut für Informatik, Germany
Franjo Ivancic	NEC Laboratories America, Inc., USA
Joost-Pieter Katoen	RWTH Aachen, Germany
Stefan Kowalewski	RWTH Aachen University, Germany
Juliana Küster Filipe Bowles	University of St. Andrews, UK
Frederic Lang	INRIA Rhône-Alpes / VASY, France
Odile Laurent	Airbus, France
Stefan Leue	University of Konstanz, Germany
Tiziana Margaria	University of Potsdam, Germany
Mieke Massink	CNR-ISTI, Italy
David Parker	University of Oxford, UK
Corina Pasareanu	CMU/NASA Ames Research Center, USA
Thomas Peikenkamp	OFFIS e.V., Germany
Jan Peleska	TZI, Universität Bremen, Germany
Ralf Pinger	Siemens AG, Braunschweig, Germany
Jakob Rehof	TU Dortmund, Germany
Judi Romijn	Movares, The Netherlands
John Rushby	SRI International, USA
Gwen Salaün	Grenoble INP - INRIA - LIG, France
Bernhard Schätz	TU München, Germany
Marjan Sirjani	Reykjavik University, Reykjavik, Iceland
Mariëlle Stoelinga	University of Twente, The Netherlands

Additional Reviewers

Acharya, Mithun	Belinfante, Axel
Barnat, Jiri	Biallas, Sebastian
Beer, Adrian	Blech, Jan Olaf

Bracciali, Andrea
Bushnell, David
Ceska, Milan
Düdder, Boris
Edmunds, Andrew
Eggers, Andreas
Gay, Gregory
Gdemann, Matthias
Genov, Blagoy
Gorbachuk, Elena
Hartmanns, Arnd
Hayden, Richard
Hugues, Jerome
Hölzl, Florian
Jafari, Ali
Khamespanah, Ehsan
Khosravi, Ramtin
Kratochvila, Tomas
Lapschies, Florian
Leitner-Fischer, Florian
Martens, Moritz
Merino, Pedro
Nguyen, Viet Yen
Noll, Thomas
Ouederni, Meriem
Shafiei, Nastaran
Sieverding, Sven
Tabaei Befrouei, Mitra
Ter Beek, Maurice H.
Teufl, Sabine
Yue, Haidi

Three Decades of Success Stories in Formal Methods

Hubert Garavel*
with contributions of Susanne Graf

INRIA/LIG – CONVECS team
655 avenue de l'Europe, 38330 Montbonnot St Martin, France
hubert.garavel@inria.fr
http://convecs.inria.fr/people/Hubert.Garavel

Abstract. This talk presents a selection of successful applications of formal methods to real-life problems. Similar studies already appeared in the scientific literature but are not, we believe, entirely satisfactory. On the one hand, in the cumulative list of applications considered by these studies, certain formal methods are over-represented while others are not mentioned. On the other hand, the essential role of verification tools is not always acknowledged as strongly as it should be.

To ensure a broader coverage of the diversity of formal methods, we selected a set of thirty case-studies, while prior studies often limited themselves to a dozen. These case-studies are distributed regularly over the past three decades, one per year between 1982 and 2011.

We tried to give a balanced panorama of formal methods by featuring different formal approaches (mathematical notations, theorem proving, model checking, static analysis, etc.), different models of computations (sequential, synchronous, asynchronous, timed, probabilistic, hybrid, etc.), and different application domains (hardware, software, telecommunication, embedded systems, operating systems, compilers, etc.).

In our selection, we focused on practical applications of formal methods rather than theoretical results alone. Contrary to some other studies, we gave priority to repeatable experiments, privileging approaches supported by software tools rather than "heroic" approaches relying on pen-and-paper manipulation of mathematical symbols.

Obviously, exhaustivity is impossible as the number and diversity of applications of formal methods cannot be reduced to a collection of thirty samples. Also, we do not claim that our selection represents the "best" case studies ever published, but simply that they correspond to pioneering and inspiring work that the young generation should keep in mind.

* This study is part of a formal methods survey that has been funded by the German Federal Agency BSI (*Bundesamt für Sicherheit in der Informationstechnik*) under project 875 initiated and led by Dr. Anastasia-Maria Leventi-Peetz.

To Scale or Not to Scale: Experience with Formal Methods and NASA Systems

Dimitra Giannakopoulou

NASA Ames Research Center, USA
dimitra.giannakopoulou@nasa.gov

Abstract. The safety-critical nature of aerospace systems mandates the development of advanced formal verification techniques that provide desired correctness guarantees. In this talk, we will discuss our experience with the development and use of formal method techniques in the context of aerospace systems. We will first provide an overview of approaches that we have developed over the last decade for scaling exhaustive verification through divide-and-conquer principles. In particular, we will present learning-based frameworks for automatically generating component abstractions. Such abstractions can be used for documentation, or more efficient modular reasoning. In the domain of human-automation interaction systems, these abstractions can be used for human operators to understand what to expect from their interactions with the system.

The techniques that will be presented use a variety of approaches, including model checking, predicate abstraction, and symbolic execution. Despite the progress that we have made in developing and applying sophisticated formal methods frameworks, the issue of scalability still remains the Achilles tendon in this domain. We will discuss scalability and the trade-offs that we have made in our work, as well as our perspective for the future application of formal methods in industry.

Table of Contents