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
VIII Organization

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
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

Real-Time Specification Patterns and Tools .............................................. 1  
* Nouha Abid, Silvano Dal Zilio, and Didier Le Botlan *

Automated Extraction of Abstract Behavioural Models from JMS Applications ......................................................... 16  
* Elvira Albert, Bjarte M. Østvold, and José Miguel Rojas *

Certifying and Reasoning on Cost Annotations in C Programs .......... 32  
* Nicolas Ayache, Roberto M. Amadio, and Yann Régis-Gianas *

Waiting for Locks: How Long Does It Usually Take? ..................... 47  
* Christel Baier, Marcus Daum, Benjamin Engel, Hermann Härtig, Joachim Klein, Sascha Klüppelholz, Steffen Märcker, Hendrik Tews, and Marcus Völp *

Microcontroller Assembly Synthesis from Timed Automaton Task Specifications ................................................................. 63  
* Victor Bandur, Wolfram Kahl, and Alan Wassyng *

Tool Chain to Support Automated Formal Verification of Avionics Simulink Designs ................................................................. 78  
* Jiří Barnat, Jan Beran, Lubos Brim, Tomas Kratochvíla, and Petr Ročkai *

Range Analysis of Binaries with Minimal Effort ........................... 93  
* Edd Barrett and Andy King *

Combining Analyses for C Program Verification ................................ 108  
* Loïc Correnson and Julien Signoles *

Model Checking the FlexRay Startup Phase ................................. 131  
* Sjoerd Cranen *

Model-Based Risk Assessment Supporting Development of HSE Plans for Safe Offshore Operations ................................................. 146  
* Rainer Droste, Christoph Läsche, Cilli Sobiech, Eckard Böde, and Axel Hahn *

Modular Automated Verification of Flexible Manufacturing Systems with Metric Temporal Logic and Non-Standard Analysis .......... 162  
* Luca Ferrucci, Dino Mandrioli, Angelo Morzenti, and Matteo Rossi *
Optimizing the Robustness of Software against Communication Latencies in Distributed Reactive Embedded Systems .......................... 177

Vlad Popa and Wolfgang Schwitzer

A Formal Design of a Tool for Static Analysis of Upper Bounds on Object Calls in Java ......................................................... 192

Konrad Siek and Paweł T. Wojciechowski

Checking Properties Described by State Machines: On Synergy of Instrumentation, Slicing, and Symbolic Execution ...................... 207

Jiří Slabý, Jan Strejček, and Marek Trtík

Author Index ............................................................................ 223