Preface

This volume contains the papers presented at FMICS 2011, the 16th International Workshop on Formal Methods for Industrial Critical Systems, taking place August 29–30, 2011, in Trento, Italy. 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), and Antwerp (September 2010). The FMICS 2011 workshop was co-located with the 19th IEEE International Requirements Engineering Conference (RE 2011).

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 bring together scientists and engineers who are active in the area of formal methods and are 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.

Thus, topics of interest for FMICS 2011 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, 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 39 submissions. Papers underwent a rigorous review process, and received three or four review reports. After the review process, the international Program Committee of FMICS 2011 decided to select 16 papers for presentation during the workshop and inclusion in these proceedings. The workshop featured two invited talks by Leonardo de Moura (Microsoft Research, USA) and Joost-Pieter Katoen (RWTH Aachen University, Germany); this volume includes two extended abstracts written by our invited speakers.
Following a tradition established over the past few years, the European Association of Software Science and Technology (EASST) offered an award to the best FMICS paper. This year, the reviewers selected the contribution by Thomas Reinbacher, Joerg Brauer, Martin Horauer, Andreas Steininger and Stefan Kowalewski on “Past Time LTL Runtime Verification for Microcontroller Binary Code.” Further information about the FMICS working group and the next FMICS workshop can be found at: http://www.inrialpes.fr/vasy/fmics.

We would like to thank the local organizers Anna Perini and Angelo Susi (Fondazione Bruno Kessler - IRST, Trento, Italy) for taking care of all the local arrangements to host FMICS in Trento, the ERCIM FMICS working group Coordinator Alessandro Fantechi (Univ. degli Studi di Firenze and ISTI-CNR, Italy) for guiding us when necessary, Jan Olaf Blech (fortiss GmbH, Germany) for acting as Publicity Chair and coordinating the publication process, EasyChair for supporting the review process, Springer for taking over the publication, all the members of the Program Committee for their great work during the review process, the external reviewers for their participation during the review process of the submissions, all the authors for submitting papers to the workshop, and the authors who participate in the workshop in Trento. All these people contributed to the success of the 2011 edition of FMICS.

August 2011

Bernhard Schätz
Gwen Salaïn
Organization

Program Committee

María Alpuente
Jiri Barnat
Josh Berdine
Jan Olaf Blech
Rance Cleaveland
Cindy Eisner
Wan Fokkink
Stefania Gnesi
Holger Hermanns
Daniel Kaestner
Stefan Kowalewski
Daniel Kroening
Frederic Lang
Kim G. Larsen
Diego Latella
Timo Latvala
Corina Pasareanu
Charles Pecheur
Ernesto Pimentel
Marco Roveri
John Rushby
Gwen Salaün
Thomas Santen
Bernhard Schätz
Marjan Sirjani
Jaco Van De Pol
Helmut Veith
UPV, Spain
Masaryk University, Czech Republic
Microsoft Research, Cambridge, UK
fortiss GmbH, Germany
University of Maryland, USA
IBM Haifa Research Laboratory, Israel
Vrije Universiteit Amsterdam, The Netherlands
ISTI-CNR, Italy
Saarland University, Germany
AbsInt GmbH, Germany
RWTH Aachen University, Germany
Computing Laboratory, Oxford University, UK
INRIA Rhône-Alpes / VASY, France
Aalborg University, Denmark
ISTI-CNR, Pisa, Italy
Space Systems, Finland
CMU/NASA Ames Research Center, USA
UC Louvain, France
University of Malaga, Spain
FBK-irst, Italy
SRI International, USA
Grenoble INP - INRIA - LIG, France
European Microsoft Innovation Center, Aachen, Germany
fortiss GmbH, Germany
Reykjavik University, Iceland
University of Twente, The Netherlands
TU Wien, Austria

Additional Reviewers

Biallas, Sebastian
Blom, Stefan
Bortolussi, Luca
Bozzano, Marco
Brauer, Jörg
Bulychev, Peter
Ceska, Milan
Crouzen, Pepijn
Dražan, Sven
Dräger, Klaus
Eisentraut, Christian
Escobar, Santiago
Fantechi, Alessandro
Ferrari, Alessio
Haller, Leopold
Hartmanns, Arnd
Hatefiardakani, Hassan
He, Nannan
Heckmann, Reinhold
Ilic, Dubravka
Kant, Gijs
Ketema, Jeroen
Khakpour, Narges
Khosravi, Ramtin
Konnov, Igor
Loreti, Michele
Mateescu, Radu
Mazzanti, Franco
Mousavi, Mohammadreza
Mover, Sergio
Nimal, Vincent
Olsen, Petur
Ouederni, Meriem
Panizo, Laura
Pfaller, Christian
Poll, Erik
Reinbacher, Thomas
Romero, Daniel
Sabouri, Hamideh
Sanan, David
Schuppan, Viktor
Serwe, Wendelin
Steiner, Wilfried
Tautschnig, Michael
Ter Beek, Maurice H.
Timmer, Mark
Titolo, Laura
Tonetta, Stefano
Trachtenherz, David
Tumova, Jana
Varpaaniemi, Kimmo
Villanueva, Alicia
Voss, Sebastian
Zuleger, Florian
# Table of Contents

Towards Trustworthy Aerospace Systems: An Experience Report .......................... 1  
*Joost-Pieter Katoen*

Satisfiability at Microsoft ......................................................................................... 5  
*Leonardo de Moura*

Lightweight Verification of a Multi-Task Threaded Server: A Case Study with the Plural Tool .......................................................... 6  
*Néstor Cataño and Ijaz Ahmed*

Runtime Verification of Typical Requirements for a Space Critical SoC Platform ................................................................. 21  
*Luca Ferro, Laurence Pierre, Zeineb Bel Hadj Amor, Jérôme Lachaize, and Vincent Lefftz*

Past Time LTL Runtime Verification for Microcontroller Binary Code ................................................................. 37  
*Thomas Reinbacher, Jörg Brauer, Martin Horauer, Andreas Steininger, and Stefan Kowalewski*

A SAT-Based Approach for the Construction of Reusable Control System Components ................................................................. 52  
*Daniel Côté, Benoît Fraikin, Marc Frappier, and Richard St-Denis*

Formal Safety Analysis in Industrial Practice ........................................................ 68  
*Ilyas Daskaya, Michaela Huhn, and Stefan Milius*

Structural Test Coverage Criteria for Integration Testing of LUSTRE/SCADE Programs ................................................................. 85  
*Virginia Papailiopoulou, Ajitha Rajan, and Ioannis Parissis*

Formal Analysis of a Triplex Sensor Voter in an Industrial Context ............... 102  
*Michael Dierkes*

Experiences with Formal Engineering: Model-Based Specification, Implementation and Testing of a Software Bus at Neopost. 117  
*Marten Sijsema, Mariëlle I.A. Stoelinga, Axel Belinfante, and Lawrence Marinelli*

Symbolic Power Analysis of Cell Libraries .......................................................... 134  
*Matthias Raffelsieper and MohammadReza Mousavi*
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>An Automated Semantic-Based Approach for Creating Tasks from Matlab Simulink Models</td>
<td>149</td>
</tr>
<tr>
<td>Matthias Büker, Werner Damm, Günter Ehmen, and Ingo Stierand</td>
<td></td>
</tr>
<tr>
<td>Performability Measure Specification: Combining CSRL and MSL</td>
<td>165</td>
</tr>
<tr>
<td>Alessandro Aldini, Marco Bernardo, and Jeremy Sproston</td>
<td></td>
</tr>
<tr>
<td>Model Checking and Co-simulation of a Dynamic Task Dispatcher Circuit Using CADP</td>
<td>180</td>
</tr>
<tr>
<td>Etienne Lantreibecq and Wendelin Serwe</td>
<td></td>
</tr>
<tr>
<td>Transforming SOS Specifications to Linear Processes</td>
<td>196</td>
</tr>
<tr>
<td>Frank P.M. Stappers, Michel A. Reniers, and Sven Weber</td>
<td></td>
</tr>
<tr>
<td>Formal Verification of Real-Time Data Processing of the LHC Beam Loss Monitoring System: A Case Study</td>
<td>212</td>
</tr>
<tr>
<td>Naghmeh Ghafari, Ramana Kumar, Jeff Joyce, Bernd Dehning, and Christos Zamantzas</td>
<td></td>
</tr>
<tr>
<td>Hierarchical Modeling and Formal Verification. An Industrial Case Study Using Reo and Vereofy</td>
<td>228</td>
</tr>
<tr>
<td>Joachim Klein, Sascha Klüppelholz, Andries Stam, and Christel Baier</td>
<td></td>
</tr>
<tr>
<td>Modeling and Verifying Timed Compensable Workflows and an Application to Health Care</td>
<td>244</td>
</tr>
<tr>
<td>Ahmed Shah Mashiyat, Fazle Rabbi, and Wendy MacCaull</td>
<td></td>
</tr>
<tr>
<td><strong>Author Index</strong></td>
<td>261</td>
</tr>
</tbody>
</table>