

*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

*TU Dortmund University, 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 for Informatics, Saarbruecken, Germany*

Gwen Salaün Bernhard Schätz (Eds.)

# Formal Methods for Industrial Critical Systems

16th International Workshop, FMICS 2011  
Trento, Italy, August 29-30, 2011  
Proceedings



Springer

Volume Editors

Gwen Salaün  
Grenoble INP - INRIA - LIG  
Montbonnot Saint-Martin, France  
E-mail: gwen.salaun@inria.fr

Bernhard Schätz  
fortiss GmbH  
München, Germany  
E-mail: schaezt@fortiss.org

ISSN 0302-9743  
ISBN 978-3-642-24430-8  
DOI 10.1007/978-3-642-24431-5  
Springer Heidelberg Dordrecht London New York

e-ISSN 1611-3349  
e-ISBN 978-3-642-24431-5

Library of Congress Control Number: 2011936880

CR Subject Classification (1998): D.2.4, D.2, D.3, C.3, C.2.4, F.3, I.6

LNCS Sublibrary: SL 2 – Programming and Software Engineering

© Springer-Verlag Berlin Heidelberg 2011

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.

The use of general descriptive names, registered names, trademarks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

*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 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 Salaün

# Organization

## Program Committee

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

## Additional Reviewers

Biallas, Sebastian	Crouzen, Pepijn
Blom, Stefan	Dražan, Sven
Bortolussi, Luca	Dräger, Klaus
Bozzano, Marco	Eisentraut, Christian
Brauer, Jörg	Escobar, Santiago
Bulychev, Peter	Fantechi, Alessandro
Ceska, Milan	Ferrari, Alessio

VIII Organization

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
<i>Joost-Pieter Katoen</i>	
Satisfiability at Microsoft . . . . .	5
<i>Leonardo de Moura</i>	
Lightweight Verification of a Multi-Task Threaded Server: A Case Study with the Plural Tool . . . . .	6
<i>Néstor Cataño and Ijaz Ahmed</i>	
Runtime Verification of Typical Requirements for a Space Critical SoC Platform . . . . .	21
<i>Luca Ferro, Laurence Pierre, Zeineb Bel Hadj Amor, Jérôme Lachaize, and Vincent Lefftz</i>	
Past Time LTL Runtime Verification for Microcontroller Binary Code . . . . .	37
<i>Thomas Reinbacher, Jörg Brauer, Martin Horauer, Andreas Steininger, and Stefan Kowalewski</i>	
A SAT-Based Approach for the Construction of Reusable Control System Components . . . . .	52
<i>Daniel Côté, Benoît Fraikin, Marc Frappier, and Richard St-Denis</i>	
Formal Safety Analysis in Industrial Practice . . . . .	68
<i>Ilyas Daskaya, Michaela Huhn, and Stefan Milius</i>	
Structural Test Coverage Criteria for Integration Testing of LUSTRE/SCADE Programs . . . . .	85
<i>Virginia Papailiopoulos, Ajitha Rajan, and Ioannis Parissis</i>	
Formal Analysis of a Triplex Sensor Voter in an Industrial Context . . . . .	102
<i>Michael Dierkes</i>	
Experiences with Formal Engineering: Model-Based Specification, Implementation and Testing of a Software Bus at Neopost. . . . .	117
<i>Marten Sijtema, Mariëlle I.A. Stoelinga, Azel Belinfante, and Lawrence Marinelli</i>	
Symbolic Power Analysis of Cell Libraries . . . . .	134
<i>Matthias Raffelsieper and MohammadReza Mousavi</i>	



An Automated Semantic-Based Approach for Creating Tasks from Matlab Simulink Models . . . . .	149
<i>Matthias Bucker, Werner Damm, Gunter Ehmen, and Ingo Stierand</i>	
Performability Measure Specification: Combining CSRL and MSL . . . . .	165
<i>Alessandro Aldini, Marco Bernardo, and Jeremy Sproston</i>	
Model Checking and Co-simulation of a Dynamic Task Dispatcher Circuit Using CADP . . . . .	180
<i>Etienne Lantreibecq and Wendelin Serwe</i>	
Transforming SOS Specifications to Linear Processes . . . . .	196
<i>Frank P.M. Stappers, Michel A. Reniers, and Sven Weber</i>	
Formal Verification of Real-Time Data Processing of the LHC Beam Loss Monitoring System: A Case Study . . . . .	212
<i>NaghmeH Ghafari, Ramana Kumar, Jeff Joyce, Bernd Dehning, and Christos Zamantzas</i>	
Hierarchical Modeling and Formal Verification. An Industrial Case Study Using Reo and Vereofy . . . . .	228
<i>Joachim Klein, Sascha Kluppelholz, Andries Stam, and Christel Baier</i>	
Modeling and Verifying Timed Compensable Workflows and an Application to Health Care . . . . .	244
<i>Ahmed Shah Mashiyat, Fazle Rabbi, and Wendy MacCaull</i>	
<b>Author Index</b> . . . . .	261