

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

University of Dortmund, Germany

Madhu Sudan

Massachusetts Institute of Technology, MA, USA

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max-Planck Institute of Computer Science, Saarbruecken, Germany

Stefan Leue Pedro Merino (Eds.)

Formal Methods for Industrial Critical Systems

12th International Workshop, FMICS 2007
Berlin, Germany, July 1-2, 2007
Revised Selected Papers

Volume Editors

Stefan Leue
University of Konstanz
Department of Computer and Information Science
78457 Konstanz, Germany
E-mail: stefan.leue@uni-konstanz.de

Pedro Merino
University of Málaga
Department of Computer Science
Campus de Teatinos, 29071, Málaga, Spain
E-mail: pedro@lcc.uma.es

Library of Congress Control Number: 2008926951

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 3-540-79706-8 Springer Berlin Heidelberg New York
ISBN-13 978-3-540-79706-7 Springer Berlin Heidelberg New York

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.

Springer is a part of Springer Science+Business Media
springer.com

© Springer-Verlag Berlin Heidelberg 2008
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper SPIN: 12266005 06/3180 5 4 3 2 1 0

Preface

The FMICS 2007 workshop was affiliated with the Computer-Aided Verification (CAV) conference and held at the Park-Inn Hotel Alexanderplatz in Berlin, Germany, July 1–2, 2007.

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 experience 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 2007 were solicited included, but were not restricted to, the following:

- Design, specification, code generation and testing with formal methods
- Verification and validation of complex, distributed, real-time systems and embedded systems
- Verification and validation methods that aim at circumventing shortcomings of existing methods with respect to their industrial applicability
- Tools for the design and development of formal descriptions
- Case studies and project reports on formal methods-related projects with industrial participation (e.g., safety critical systems, mobile systems, object-based distributed systems)
- Application of formal methods in standardization and industrial forums

The workshop included five sessions of regular contributions and three invited presentations, given by Charles Pecheur, Thomas Henzinger and Gérard Berry. At the workshop, a participants' proceedings volume was made available to all participants. This LNCS volume reports on the presentations given at FMICS 2007 in archival form. The papers included in this volume were selected after a second round of peer reviewing by the FMICS 2007 Program Committee from those papers accepted for presentation at FMICS 2007. Out of the 31 submissions to FMICS 2007, 15 papers were accepted for presentation at the workshop, and revised versions of all accepted papers are included in this volume.

FMICS 2007 attracted 33 participants, some of which are members of the FMICS working group, from 14 different countries.

Following a tradition established over the past few years, the European Association of Software Science and Technology (EASST) has offered an award to the best FMICS paper. The Program Committee decided to confer the FMICS 2007 best paper award to the paper “An Approach to Formalization and Analysis of Message Passing Libraries,” written by Robert Palmer, Michael DeLisi, Ganesh Gopalakrishnan and Robert M. Kirby.

Further information about the FMICS working group and the next FMICS workshop can be found at: <http://www.inrialpes.fr/vasy/fmics>.

We wish to thank the members of the Program Committee and the additional reviewers for their careful evaluation of the submitted papers during both rounds of reviewing. We also appreciate the effort of all members of the Program Committee in making judicious choices and engaging in constructive discussions during the electronic program selection meeting. We are very grateful to the local organizers of the CAV conference for their organizational support, and to the University of Dortmund for allowing us to use their Online Conference Service.

February 2008

Stefan Leue
Pedro Merino

Organization

Program Committee

Per Bjesse (Synopsys, USA)
Lubos Brim (Masaryk University, Czech Republic)
Marsha Chechik (University of Toronto, Canada)
Darren Cofer (Rockwell Collins, USA)
Stefania Gnesi (ISTI-CNR, Italy)
Patrice Godefroid (Microsoft Research, USA)
Michael Goldsmith (Formal Systems, UK)
David Harel (Weizmann Institute of Science, Israel)
Connie Heitmeyer (Naval Research Laboratory, USA)
Leszek Holenderski (Philips, The Netherlands)
Joost-Pieter Katoen (RWTH Aachen, Germany)
Roope Kaivola (Intel, USA)
Stefan Kowalewski (RWTH Aachen, Germany)
Salvatore La Torre (Universita' degli Studi di Salerno, Italy)
Martin Leucker (TU München, Germany)
Stefan Leue (University of Konstanz, Germany), Co-chair
Radu Mateescu (INRIA Rhone-Alpes, France)
Pedro Merino (University of Malaga, Spain), Co-chair
David Parker (University of Oxford, UK)
Charles Pecheur (Université Catholique de Louvain, Belgium)
Francois Pilarski (Airbus, France)
Andreas Podelski (University of Freiburg, Germany)
Jakob Rehof (University of Dortmund, Germany)
John Rushby (SRI International, USA)
Don Sannella (University of Edinburgh, UK)
Ina Schieferdecker (Fraunhofer FOKUS, Germany)
Anna Slobodova (Intel, USA)
Jaco van de Pol (CWI, The Netherlands)
Farn Wang (National Taiwan University, Taiwan)
Willem Visser (SEVEN Networks, USA)

Additional Reviewers

David Aspinall (University of Edinburgh, UK)
Dave Berry (University of Edinburgh, UK)
Jesse Bingham (Intel, USA)
Iavor S. Diatchki (Galois Connections Inc., USA)
Alessandro Fantechi (DSI-UNIFI, Italy)

Daniel Kluender (RWTH Aachen, Germany)
Sascha Klueppelholz (TU Dresden, Germany)
Frédéric Lang (INRIA Rhone-Alpes, France)
Patrick Maier (University of Edinburgh, UK)
Stefan Maus (University of Freiburg, Germany)
Franco Mazzanti (ISTI-CNR, Italy)
Thomas Noll (RWTH Aachen, Germany)
Laurence Pierre (Université de Nice Sophia-Antipolis, France)
Bastian Schlich (RWTH Aachen University, Germany)
Nassim Seghir (Max Planck Institute, Germany)
Wendelin Serwe (INRIA Rhone-Alpes, France)
Maurice ter Beek (ISTI-CNR, Italy)
Carsten Weise (RWTH Aachen, Germany)
Anton Wijs (CWI, Amsterdam, The Netherlands)
Sebastian Winter (TU München, Germany)
Ivan S. Zapreev (University of Twente, The Netherlands)

Table of Contents

Invited Presentations

Verification of Embedded Software: From Mars to Actions.....	1
<i>Charles Pecheur</i>	
Synchronous Design and Verification of Critical Embedded Systems Using SCADE and Esterel	2
<i>Gérard Berry</i>	

Research Papers

Static Analysis of the Accuracy in Control Systems: Principles and Experiments.....	3
<i>Eric Goubault, Sylvie Putot, Philippe Baufreton, and Jean Gassino</i>	
Application of Static Analyses for State Space Reduction to Microcontroller Assembly Code	21
<i>Bastian Schlich, Jann Löll, and Stefan Kowalewski</i>	
Checking the TWIN Elevator System by Translating Object-Z to SMV	38
<i>Sören Preibusch and Florian Kammüller</i>	
Introducing Time in an Industrial Application of Model-Checking	56
<i>Lionel van den Berg, Paul Strooper, and Kirsten Winter</i>	
Integration of Formal Analysis into a Model-Based Software Development Process	68
<i>Michael Whalen, Darren Cofer, Steven Miller, Bruce H. Krogh, and Walter Storm</i>	
Formal Verification with Isabelle/HOL in Practice: Finding a Bug in the GCC Scheduler.....	85
<i>Lars Gesellensetter, Sabine Glesner, and Elke Salecker</i>	
Computing Worst-Case Response Times in Real-Time Avionics Applications.....	101
<i>Murali Rangarajan and Darren Cofer</i>	
Machine Checked Formal Proof of a Scheduling Protocol for Smartcard Personalization	115
<i>Leonard Lensink, Sjaak Smeters, and Marko van Eekelen</i>	

An Action/State-Based Model-Checking Approach for the Analysis of Communication Protocols for Service-Oriented Applications	133
<i>Maurice H. ter Beek, A. Fantechi, S. Gnesi, and F. Mazzanti</i>	
Model Classifications and Automated Verification	149
<i>Radek Pelánek</i>	
An Approach to Formalization and Analysis of Message Passing Libraries	164
<i>Robert Palmer, Michael DeLisi, Ganesh Gopalakrishnan, and Robert M. Kirby</i>	
Analysis of a Session-Layer Protocol in mCRL2: Verification of a Real-Life Industrial Implementation	182
<i>Marko van Eekelen, Stefan ten Hoedt, René Schreurs, and Yaroslav S. Usenko</i>	
Automatic Certification of Java Source Code in Rewriting Logic	200
<i>Mauricio Alba-Castro, María Alpuente, and Santiago Escobar</i>	
Reverse Engineered Formal Models for GUI Testing	218
<i>Ana C.R. Paiva, João C.P. Faria, and Pedro M.C. Mendes</i>	
Automatic Interoperability Test Case Generation Based on Formal Definitions	234
<i>Alexandra Desmoulin and César Viho</i>	
Author Index	251