

Commenced Publication in 1973

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

Editorial Board

David Hutchison

Lancaster University, Lancaster, UK

Takeo Kanade

Carnegie Mellon University, Pittsburgh, PA, USA

Josef Kittler

University of Surrey, Guildford, UK

Jon M. Kleinberg

Cornell University, Ithaca, NY, USA

Friedemann Mattern

ETH Zürich, Zürich, Switzerland

John C. Mitchell

Stanford University, Stanford, CA, USA

Moni Naor

Weizmann Institute of Science, Rehovot, Israel

C. Pandu Rangan

Indian Institute of Technology, Madras, India

Bernhard Steffen

TU Dortmund University, Dortmund, Germany

Demetri Terzopoulos

University of California, Los Angeles, CA, USA

Doug Tygar

University of California, Berkeley, CA, USA

Gerhard Weikum

Max Planck Institute for Informatics, Saarbrücken, Germany

More information about this series at <http://www.springer.com/series/7408>

Manuel Núñez · Matthias Güzdemann (Eds.)

Formal Methods for Industrial Critical Systems

20th International Workshop, FMICS 2015
Oslo, Norway, June 22–23, 2015
Proceedings

Editors

Manuel Núñez
Universidad Complutense de Madrid
Madrid
Spain

Matthias Güdemann
Systerel
Aix-en-Provence
France

ISSN 0302-9743

ISSN 1611-3349 (electronic)

Lecture Notes in Computer Science

ISBN 978-3-319-19457-8

ISBN 978-3-319-19458-5 (eBook)

DOI 10.1007/978-3-319-19458-5

Library of Congress Control Number: 2015940351

LNCS Sublibrary: SL2 – Programming and Software Engineering

Springer Cham Heidelberg New York Dordrecht London

© Springer International Publishing Switzerland 2015

This work is subject to copyright. All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, 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.

The publisher, the authors and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, express or implied, with respect to the material contained herein or for any errors or omissions that may have been made.

Printed on acid-free paper

Springer International Publishing AG Switzerland is part of Springer Science+Business Media
(www.springer.com)

Preface

This volume contains the papers presented at FMICS 2015, the 20th International Workshop on Formal Methods for Industrial Critical Systems, which was held during June 22–23, 2015, in Oslo, Norway. The FMICS 2015 workshop took place as a collocated event of the 20th International Symposium on Formal Methods, FM 2015.

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 who 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 20 submissions. Each of these submissions went through a rigorous review process in which each paper received at least three reports. We selected 12 papers for presentation during the workshop and inclusion in these proceedings. The workshop also featured invited talks by Kim G. Larsen (Aalborg University, Denmark) and by Marielle Petit-Doche (Systerel, France). In addition, two invited talks by Dino Distefano (Queen Mary University, UK and Facebook) and José Meseguer (University of Illinois, USA) organized by the Workshop on Automated Specification and Verification of Web Systems were open to FMICS participants.

We would like to thank the ERCIM FMICS working group coordinator Radu Mateescu (Inria Grenoble and LIG) for his counselling and support during the organization of FMICS 2015. We would like to thank the FM 2015 workshops chairs Marieke Huisman and Volker Stolz for their help with the local arrangements in Oslo. We would like to thank the chairs of the 11th Workshop on Automated Specification and Verification of Web Systems, Maurice H. ter Beek (ISTI-CNR, Pisa, Italy) and Alberto Lluch Lafuente (Technical University of Denmark), for the generous offer to share their invited speakers with FMICS attendants. Finally, we would like to thank the Program Committee

members and external reviewers for their useful and detailed reviews and discussions, all authors for their submissions, and all attendees of the workshop.

June 2015

Manuel Núñez
Matthias Güdemann

Organization

Programm Committee Chairs

Manuel Núñez	Universidad Complutense de Madrid, Spain
Matthias Güdemann	Systerel, France

Programm Committee

María Alpuente	Universitat Politècnica de Valencia, Spain
Alvaro Arenas	IE University, Spain
Jiri Barnat	Masaryk University, Czech Republic
Jean-Paul Blanquart	Astrium Satellites, France
Eckard Böde	Offis, Germany
Mario Bravetti	University of Bologna, Italy
Michael Dierkes	Rockwell Collins, France
Cindy Eisner	IBM Research - Haifa, Israel
Alessandro Fantechi	Università di Firenze, Italy
Francesco Flammini	Ansaldo, Italy
María del Mar Gallardo	University of Málaga, Spain
Stefania Gnesi	ISTI-CNR, Italy
Matthias Güdemann	Systerel, France
Clément Houtmann	Google, Switzerland
Frédéric Lang	Inria and LIG, France
Luis Llana	Universidad Complutense de Madrid, Spain
Alberto Lluch	DTU, Denmark
Paqui Lucio	University of the Basque Country, Spain
Tiziana Margaria	University of Potsdam, Germany
Jasen Markovski	GN ReSound Benelux, The Netherlands
Radu Mateescu	Inria and LIG, France
David Mentré	Mitsubishi Research, France
Manuel Núñez	Universidad Complutense de Madrid, Spain
Charles Pecheur	Université Catholique de Louvain, Belgium
Ralf Pinger	Siemens AG, Germany
Jaco van de Pol	University of Twente, The Netherlands
Wendelin Serwe	Inria and LIG, France
Hans Svensson	Quviq, Sweden
Anton Wijs	Technical University of Eindhoven, The Netherlands
Fatiha Zaïdi	Université Paris-Sud XI, France

Additional Reviewers

Emilie Balland
Demis Ballis
Marcello M. Bersani
Paul Brauner
Laura Carnevali
Marcus Gerhold
Jeroen Meijer

Invited Talks

Formal Verification of Industrial Critical Software

Marielle Petit-Doche

Systerel, Les portes de l'Arbois, Bâtiment A — 1090, rue René Descartes
13857 Aix-en-Provence CEDEX 3, France
`marielle.petit-doche@systerel.fr`
`www.systerel.fr`

Abstract. In this talk I will review the challenges for using formal verification based on automatic tools, like model-checkers, in the industrial development process of safety critical systems is discussed. This usage must be integrated into an appropriate process and must allow for independent result-checking.

Our approach is illustrated with a case study from the `openETCS` ITEA2 research project using the Systerel Smart Solver S3, a modern SAT-based model-checker for equivalence checking and safety properties analysis of SCADE, C or Ada programs.

From Timed Automata to Stochastic Hybrid Games

Model Checking, Performance Evaluation, Synthesis and Optimization

Kim G. Larsen

Department of Computer Science, Aalborg University, Denmark

`kgl@cs.aau.dk`

Abstract. Timed automata [1] and games [3, 7], priced timed automata [2, 4] and energy automata [6] have emerged as useful formalisms for modeling real-time and energy-aware systems as found in several embedded and cyber-physical systems. During the last 20 years the real-time model checker UPPAAL has been developed allowing for efficient verification of hard timing constraints of timed automata. Moreover a number of significant branches exists, e.g. UPPAAL CORA providing efficient support for optimization, and UPPAAL TIGA allowing for automatic synthesis of strategies for given safety and liveness objectives. In the beginning of this decade the branch UPPAAL SMC [10, 11] has been released, providing a highly scalable new engine that supports (distributed) statistical model checking of stochastic hybrid automata (and games).

The most recent branch of the UPPAAL family is the tool UPPAAL STRATEGO [8, 9], that combines all of the above tools and extend the with techniques from machine learning, in order to generate, optimize, compare and explore consequences and performance of strategies synthesized for stochastic priced timed games in a userfriendly manner. In particular, UPPAAL STRATEGO allows for generation of strategies that simultaneously satisfy a number of hard real-time constraints, while having near optimal expected performance properties.

The various branches of UPPAAL have been applied in concerted fashions to a range of real-time and cyber-physical examples including schedulability and performance evaluation of mixed criticality systems, modeling and analysis of biological systems, energy-aware wireless sensor networks, synthesis and performance evaluation of smart grids and energy-aware buildings and battery-aware scheduling.

References

1. Alur, R., Dill, D.L.: A theory of timed automata. *Theor. Comput. Sci.* 126(2), 183–235 (1994)
2. Alur, R., La Torre, S., Pappas, G.J.: Optimal paths in weighted timed automata. In: Benedetto and Sangiovanni-Vincentelli [5], pp. 49–62, http://dx.doi.org/10.1007/3-540-45351-2_8
3. Behrmann, G., Cougnard, A., David, A., Fleury, E., Larsen, K.G., Lime, D.: Uppaal-tiga: Time for playing games! In: CAV. pp. 121–125 (2007)
4. Behrmann, G., Fehnker, A., Hune, T., Larsen, K.G., Pettersson, P., Romijn, J., Vaandrager, F.W.: Minimum-cost reachability for priced timed automata. In: Benedetto and Sangiovanni-Vincentelli [5], pp. 147–161, http://dx.doi.org/10.1007/3-540-45351-2_15

This work has been supported by the projects IDEA4CPS, SENSATION and CASSTING.

5. Benedetto, M.D.D., Sangiovanni-Vincentelli, A.L. (eds.): Hybrid Systems: Computation and Control, 4th International Workshop, HSCC 2001, Rome, Italy, March 28-30, 2001, Proceedings, Lecture Notes in Computer Science, vol. 2034. Springer (2001)
6. Bouyer, P., Fahrenberg, U., Larsen, K.G., Markey, N., Srba, J.: Infinite runs in weighted timed automata with energy constraints. In: Cassez, F., Jard, C. (eds.) Formal Modeling and Analysis of Timed Systems, 6th International Conference, FORMATS 2008, Saint Malo, France, September 15-17, 2008. Proceedings. Lecture Notes in Computer Science, vol. 5215, pp. 33–47. Springer (2008), http://dx.doi.org/10.1007/978-3-540-85778-5_4
7. Cassez, F., David, A., Fleury, E., Larsen, K.G., Lime, D.: Efficient on-the-fly algorithms for the analysis of timed games. In: CONCUR. pp. 66–80 (2005)
8. David, A., Jensen, P.G., Larsen, K.G., Legay, A., Lime, D., Sørensen, M.G., Taankvist, J.H.: On time with minimal expected cost! In: Cassez, F., Raskin, J. (eds.) Automated Technology for Verification and Analysis - 12th International Symposium, ATVA 2014, Sydney, NSW, Australia, November 3-7, 2014, Proceedings. Lecture Notes in Computer Science, vol. 8837, pp. 129–145. Springer (2014), http://dx.doi.org/10.1007/978-3-319-11936-6_10
9. David, A., Jensen, P.G., Larsen, K.G., Mikucionis, M., Taankvist, J.H.: Uppaal stratego. In: Baier, C., Tinelli, C. (eds.) Tools and Algorithms for the Construction and Analysis of Systems - 21st International Conference, TACAS 2015, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2015, London, UK, April 11-18, 2015. Proceedings. Lecture Notes in Computer Science, vol. 9035, pp. 206–211. Springer (2015), http://dx.doi.org/10.1007/978-3-662-46681-0_16
10. David, A., Larsen, K.G., Legay, A., Mikucionis, M., Poulsen, D.B., van Vliet, J., Wang, Z.: Statistical model checking for networks of priced timed automata. In: Fahrenberg, U., Tripakis, S. (eds.) Formal Modeling and Analysis of Timed Systems - 9th International Conference, FORMATS 2011, Aalborg, Denmark, September 21-23, 2011. Proceedings. Lecture Notes in Computer Science, vol. 6919, pp. 80–96. Springer (2011), http://dx.doi.org/10.1007/978-3-642-24310-3_7
11. David, A., Larsen, K.G., Legay, A., Mikucionis, M., Wang, Z.: Time for statistical model checking of real-time systems. In: Gopalakrishnan, G., Qadeer, S. (eds.) Computer Aided Verification - 23rd International Conference, CAV 2011, Snowbird, UT, USA, July 14-20, 2011. Proceedings. Lecture Notes in Computer Science, vol. 6806, pp. 349–355. Springer (2011), http://dx.doi.org/10.1007/978-3-642-22110-1_27

Contents

Formal Verification of Industrial Critical Software	1
<i>Marielle Petit-Doche, Nicolas Breton, Roméo Courbis, Yoann Fonteneau, and Matthias Gdemann</i>	

Applications

A Case Study on Formal Verification of the Anaxagoras Hypervisor Paging System with Frama-C	15
<i>Allan Blanchard, Nikolai Kosmatov, Matthieu Lemerre, and Frdric Loulergue</i>	
Intra-procedural Optimization of the Numerical Accuracy of Programs	31
<i>Nasrine Damouche, Matthieu Martel, and Alexandre Chapoutot</i>	
Formal Analysis and Testing of Real-Time Automotive Systems Using UPPAAL Tools	47
<i>Jin Hyun Kim, Kim G. Larsen, Brian Nielsen, Marius Mikuionis, and Petur Olsen</i>	
Successful Use of Incremental BMC in the Automotive Industry	62
<i>Peter Schrammel, Daniel Kroening, Martin Brain, Ruben Martins, Tino Teige, and Tom Bienmller</i>	

Protocols

Colored Petri Net Modeling of the Publish/Subscribe Paradigm in the Context of Web Services Resources	81
<i>Valentin Valero, Hermenegilda Maci, Gregorio Daz, and M. Emilia Cambronero</i>	
Model Checking a Server-Side Micro Payment Protocol	96
<i>Kaylash Chaudhary and Ansgar Fehnker</i>	

Specification and Analysis

Require, Test and Trace IT	113
<i>Bernhard K. Aichernig, Klaus Hrmaier, Florian Lorber, Dejan Nikovi, and Stefan Tiran</i>	

Applying Finite State Process Algebra to Formally Specify
a Computational Model of Security Requirements in the
Key2phone-Mobile Access Solution 128
*Sunil Chaudhary, Linfeng Li, Eleni Berki, Marko Helenius,
Juha Kela, and Markku Turunen*

Timed Mobility and Timed Communication for Critical Systems 146
Bogdan Aman and Gabriel Ciobanu

On the Formal Analysis of Photonic Signal Processing Systems 162
Umair Siddique, Sidi Mohamed Beillahi, and Sofiène Tahar

Verification

Automated Verification of Nested DFS 181
Jaco C. van de Pol

On the Formal Verification of Optical Quantum Gates in HOL 198
*Mohamed Yousri Mahmoud, Prakash Panangaden,
and Sofiène Tahar*

Author Index 213

Formal Methods for Industrial Critical Systems

20th International Workshop, FMICS 2015 Oslo, Norway,

June 22-23, 2015 Proceedings

Núñez, M.; Güdemann, M. (Eds.)

2015, XVI, 213 p. 61 illus., Softcover

ISBN: 978-3-319-19457-8