

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

Tiziana Margaria Bernhard Steffen (Eds.)

Leveraging Applications of Formal Methods, Verification and Validation

Applications and Case Studies

5th International Symposium, ISoLA 2012
Heraklion, Crete, Greece, October 15-18, 2012
Proceedings, Part II



Springer

Volume Editors

Tiziana Margaria

Universität Potsdam, Institut für Informatik
August-Bebel-Straße 89, 14482 Potsdam, Germany
E-mail: margaria@cs.uni-potsdam.de

Bernhard Steffen

Technische Universität Dortmund, Fakultät für Informatik
Otto-Hahn-Straße 14, 44227 Dortmund, Germany
E-mail: steffen@cs.tu-dortmund.de

ISSN 0302-9743

e-ISSN 1611-3349

ISBN 978-3-642-34031-4

e-ISBN 978-3-642-34032-1

DOI 10.1007/978-3-642-34032-1

Springer Heidelberg Dordrecht London New York

Library of Congress Control Number: 2012948288

CR Subject Classification (1998): D.2.4-5, D.2.1-3, D.3.3-4, D.4.1, D.4.5, D.4.7, F.1.1, F.3.1-2, I.2, C.2

LNCS Sublibrary: SL 1 – Theoretical Computer Science and General Issues

© Springer-Verlag Berlin Heidelberg 2012

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

Welcome to ISoLA 2012, the 4th International Symposium on Leveraging Applications of Formal Methods, Verification and Validation, that was held in Heraklion, Crete (Greece) during October 14–18, 2012, endorsed by EASST, the European Association of Software Science and Technology.

This year's event followed the tradition of its forerunners held 2004 and 2006 in Cyprus, 2008 in Chalkidiki, and 2010 in Crete, and the series of ISoLA Workshops in Greenbelt (USA) in 2005, Poitiers (France) in 2007, Potsdam (Germany) in 2009, and in Vienna (Austria) in 2011.

As in the previous editions, ISoLA 2012 provided a forum for developers, users, and researchers to discuss issues related to the adoption and use of rigorous tools and methods for the specification, analysis, verification, certification, construction, test, and maintenance of systems from the point of view of their different application domains. Thus, since 2004 the ISoLA series of events serves the purpose of bridging the gap between designers and developers of rigorous tools on the one hand, and users in engineering and in other disciplines on the other hand. It fosters and exploits synergetic relationships among scientists, engineers, software developers, decision makers, and other critical thinkers in companies and organizations. By providing a specific, dialogue-oriented venue for the discussion of common problems, requirements, algorithms, methodologies, and practices, ISoLA aims in particular at supporting researchers in their quest to improve the usefulness, reliability, flexibility, and efficiency of tools for building systems, and users in their search for adequate solutions to their problems.

The program of the symposium consisted of a collection of special tracks devoted to the following hot and emerging topics

- Adaptable and Evolving Software for Eternal Systems (R. Hähnle, I. Schäfer)
- Approaches for Mastering Change (M. Leucker, M. Lochau, I. Schäfer)
- Bioscientific Data Processing and Modeling (J. Kok, A.-L. Lamprecht, F. Verbeek, M. Wilkinson)
- Formal Methods for the Development and Certification of X-by-Wire Control Systems (A. Fantechi, F. Flammini, S. Gnesi)
- Handling Heterogeneity in Formal Development of HW and SW Systems (Y. Ait-Ameur, D. Mery)
- Learning Techniques for Software Verification and Validation (E.M. Clarke, M. Gheorghiu Bobaru, C. Pasareanu, D. Song)
- Model-Based Testing and Model Inference (K. Meinke, N. Walkinshaw)
- Processes and Data Integration in the Networked Healthcare (A. Braun v. Reinersdorff, T. Margaria, C. Rasche)
- Process-Oriented Geoinformation Systems and Applications (H. Asche)
- Quantitative Modeling and Analysis (J.-P. Katoen, K.G. Larsen)
- Runtime Verification: The Application Perspective (Y. Falcone, L. Zuck)

- Software Aspects of Robotic Systems (J. Knoop, D. Schreiner)
- Timing Constraints: Theory Meets Practice (B. Lisper, J. Nordlander, P. Quinton)

and of the following four events

- LearnLib Tutorial: From Finite Automata to Register Interface Programs (F. Howar, M. Isberner, M. Merten, B. Steffen)
- The RERS Grey-Box Challenge 2012: Analysis of Event-Condition-Action Systems (F. Howar, M. Isberner, M. Merten, B. Steffen, D. Beyer)
- Linux Driver Verification Workshop (D. Beyer, A. Petrenko)
- ITSy Day 2012 (T. Margaria, B. Steffen)

The ISoLA Symposium was itself part of the ISoLA Week, which signaled the steady growth of the community and included the following four co-located events:

- STRESS 2012 — International School on Tool-Based Rigorous Engineering of Software Systems (P.Chalin, J. Hatcliff, Robby, T. Margaria, B. Steffen)
- SEW 2012 — 35th IEEE Software Engineering Workshop (M. Hinchey, J. Bowen, H. Zhu)
- Graduate/Postgraduate Course on Soft Skills for IT Professionals in Science and Engineering (B. Floyd)
- FRCSS 2012 — 2nd Future Research Challenges for Software and Services (T. Margaria)

We thank the track organizers, the members of the Program Committee and their subreferees for their effort in selecting the papers to be presented, the Local Organization Chair, Petros Stratis, and the Easyconference team for their continuous precious support during the week as well as during the entire two-year period preceding the events, and Springer for being, as usual, a very reliable partner in the proceedings production. Finally, we are grateful to Horst Voigt for his Web support, and to Maik Merten, Johannes Neubauer, and Stephan Windmüller for their help with the online conference service (OCS).

Special thanks are due to the following organization for their endorsement: EASST (European Association of Software Science and Technology), and our own institutions — the TU Dortmund, and the University of Potsdam.

October 2012

Tiziana Margaria
Bernhard Steffen

Organization

Committees

Symposium Chair	Bernhard Steffen
Program Chair	Tiziana Margaria

Program Committee

Yamine Ait-Ameur	Björn Lisper
Hartmut Asche	Malte Lochau
Dirk Beyer	Karl Meinke
Mihaela Bobaru	Dominique Mery
Edmund Clarke	Alessandro Moschitti
Ylies Falcone	Johan Nordlander
Francesco Flammini	Corina Pasareanu
Stefania Gnesi	Alexander K. Petrenko
Reiner Hähnle	Sophie Quinton
John Hatcliff	Ina Schaefer
Falk Howar	Dietmar Schreiner
Joost-Pieter Katoen	Dawn Song
Joost Kok	Fons Verbeek
Jens Knoop	Neil Walkinshaw
Anna-Lena Lamprecht	Mark D. Wilkinson
Kim G. Larsen	Lenore Zuck
Martin Leucker	

Table of Contents – Part II

Linux Driver Verification

Linux Driver Verification (Position Paper)	1
<i>Dirk Beyer and Alexander K. Petrenko</i>	

Bioscientific Data Processing and Modeling

Bioscientific Data Processing and Modeling	7
<i>Joost Kok, Anna-Lena Lamprecht, Fons J. Verbeek, and Mark D. Wilkinson</i>	

Using Multiobjective Optimization and Energy Minimization to Design an Isoform-Selective Ligand of the 14-3-3 Protein	12
<i>Hernando Sanchez-Faddeev, Michael T.M. Emmerich, Fons J. Verbeek, Andrew H. Henry, Simon Grimshaw, Herman P. Spaink, Herman W. van Vlijmen, and Andreas Bender</i>	

Segmentation for High-Throughput Image Analysis: Watershed Masked Clustering	25
<i>Kuan Yan and Fons J. Verbeek</i>	

Efficient and Robust Shape Retrieval from Deformable Templates	42
<i>Alexander E. Nezhinsky and Fons J. Verbeek</i>	

OWL-DL Domain-Models as Abstract Workflows	56
<i>Ian Wood, Ben Vandervalk, Luke McCarthy, and Mark D. Wilkinson</i>	

Processes and Data Integration in the Networked Healthcare

Processes and Data Integration in the Networked Healthcare	67
<i>Andrea Braun von Reinersdorff, Tiziana Margaria, and Christoph Rasche</i>	

Simple Modeling of Executable Role-Based Workflows: An Application in the Healthcare Domain	70
<i>Tiziana Margaria, Steve Boßelmann, and Bertold Kujath</i>	

Considerations for Healthcare Applications in a Platform as a Service Environment	73
<i>Andreas Holubek and Christian Metzger</i>	

Reha-Sports: The Challenge of Small Margin Healthcare Accounting ... 75
Markus Doedt, Thomas Göke, Jan Pardo, and Bernhard Steffen

Timing Constraints: Theory Meets Practice

Timing Constraints: Theory Meets Practice 78
Björn Lisper, Johan Nordlander, and Sophie Quinton

A Simple and Flexible Timing Constraint Logic 80
Björn Lisper and Johan Nordlander

Generalized Weakly-Hard Constraints 96
Sophie Quinton and Rolf Ernst

Modeling a BSG-E Automotive System with the Timing Augmented
Description Language 111
*Marie-Agnès Peraldi-Frati, Arda Goknil, Morayo Adedjouma, and
Pierre Yves Gueguen*

Formal Analysis of TESLA Protocol in the Timed OTS/CafeOBJ
Method 126
Iakovos Ouranos, Kazuhiro Ogata, and Petros Stefanias

Formal Specification and Verification of Task Time Constraints for
Real-Time Systems 143
Ning Ge, Marc Pantel, and Xavier Crégut

The WCET Analysis Tool CalcWcet167 158
Raimund Kirner

Abstract Execution for Event-Driven Systems – An Application from
Automotive/Infotainment Development 173
Klaus Birken

Formal Methods for the Development and Certification of X-by-Wire Control Systems

Formal Methods for Intelligent Transportation Systems 187
Alessandro Fantechi, Francesco Flammini, and Stefania Gnesi

Model-Driven V&V Processes for Computer Based Control Systems:
A Unifying Perspective 190
*Francesco Flammini, Stefano Marrone, Nicola Mazzocca,
Roberto Nardone, and Valeria Vittorini*

Formal Methods in Avionic Software Certification: The DO-178C
Perspective 205
Gabriella Gigante and Domenico Pascarella

Product Line Engineering Applied to CBTC Systems Development	216
<i>Alessio Ferrari, Giorgio Oronzo Spagnolo, Giacomo Martelli, and Simone Menabeni</i>	

Improving Verification Process in Driverless Metro Systems: The MBAT Project	231
<i>Stefano Marrone, Roberto Nardone, Antonio Orazio, Ida Petrone, and Luigi Velardi</i>	

Optimising Ordering Strategies for Symbolic Model Checking of Railway Interlockings	246
<i>Kirsten Winter</i>	

Automated Generation of Safety Requirements from Railway Interlocking Tables	261
<i>Anne E. Harthausen</i>	

Distributing the Challenge of Model Checking Interlocking Control Tables	276
<i>Alessandro Fantechi</i>	

Quantitative Modelling and Analysis

Quantitative Modelling and Analysis	290
<i>Joost-Pieter Katoen and Kim Guldstrand Larsen</i>	

Schedulability of Herschel-Planck Revisited Using Statistical Model Checking	293
<i>Alexandre David, Kim Guldstrand Larsen, Axel Legay, and Marius Mikučionis</i>	

Checking Correctness of Services Modeled as Priced Timed Automata	308
<i>Aida Čaušević, Cristina Seceleanu, and Paul Pettersson</i>	

Software Aspects of Robotic Systems

Software Aspects of Robotic Systems	323
<i>Jens Knoop and Dietmar Schreiner</i>	

Process-Oriented Geoinformation Systems and Applications

Process-Oriented Geoinformation Systems and Applications	324
<i>Hartmut Asche</i>	

Concepts and Techniques of an Online 3D Atlas – Challenges in
Cartographic 3D Geovisualization 325
René Sieber, Livia Hollenstein, and Remo Eichenberger

**Handling Heterogeneity in Formal Development of
HW and SW Systems**

Handling Heterogeneity in Formal Developments of Hardware and
Software Systems 327
Yamine Ait-Ameur and Dominique Méry

Leveraging Formal Verification Tools for DSML Users: A Process
Modeling Case Study 329
Faiez Zalila, Xavier Crégut, and Marc Pantel

An Ontological Pivot Model to Interoperate Heterogeneous User
Requirements 344
Ilyès Boukhari, Ladjel Bellatreche, and Stéphane Jean

Author Index 359

Table of Contents – Part I

Adaptable and Evolving Software for Eternal Systems

Adaptable and Evolving Software for Eternal Systems (Track Summary)	1
<i>Reiner Hähnle and Ina Schaefer</i>	
Challenges in Defining a Programming Language for Provably Correct Dynamic Analyses	4
<i>Eric Bodden, Andreas Follner, and Siegfried Rasthofer</i>	
Eternal Embedded Software: Towards Innovation Experiment Systems	19
<i>Jan Bosch and Ulrik Eklund</i>	
A Liskov Principle for Delta-Oriented Programming	32
<i>Reiner Hähnle and Ina Schaefer</i>	
Scientific Workflows: Eternal Components, Changing Interfaces, Varying Compositions	47
<i>Anna-Lena Lamprecht and Tiziana Margaria</i>	
An Object Group-Based Component Model	64
<i>Michaël Lienhardt, Mario Bravetti, and Davide Sangiorgi</i>	
Automated Inference of Models for Black Box Systems Based on Interface Descriptions	79
<i>Maik Merten, Falk Howar, Bernhard Steffen, Patrizio Pellicione, and Massimo Tivoli</i>	
Model-Based Compatibility Checking of System Modifications	97
<i>Arnd Poetzsch-Heffter, Christoph Feller, Ilham W. Kurnia, and Yannick Welsch</i>	
A Generic Platform for Model-Based Regression Testing	112
<i>Philipp Zech, Michael Felderer, Philipp Kalb, and Ruth Breu</i>	

Approaches for Mastering Change

Approaches for Mastering Change	127
<i>Ina Schaefer, Malte Lochau, and Martin Leucker</i>	
A Formal Approach to Software Product Families	131
<i>Martin Leucker and Daniel Thoma</i>	

A Compositional Framework to Derive Product Line Behavioural Descriptions	146
<i>Patrizia Asirelli, Maurice H. ter Beek, Alessandro Fantechi, and Stefania Gnesi</i>	
Delta-Oriented Monitor Specification	162
<i>Eric Bodden, Kevin Falzon, Ka I. Pun, and Volker Stolz</i>	
Conflict Detection in Delta-Oriented Programming	178
<i>Michaël Lienhardt and Dave Clarke</i>	
Family-Based Analysis of Type Safety for Delta-Oriented Software Product Lines	193
<i>Ferruccio Damiani and Ina Schaefer</i>	
A Vision for Behavioural Model-Driven Validation of Software Product Lines	208
<i>Xavier Devroey, Maxime Cordy, Gilles Perrouin, Eun-Young Kang, Pierre-Yves Schobbens, Patrick Heymans, Axel Legay, and Benoit Baudry</i>	
Parameterized Preorder Relations for Model-Based Testing of Software Product Lines	223
<i>Malte Lochau and Jochen Kamischke</i>	
SmartTies – Management of Safety-Critical Developments	238
<i>Serge Autexier, Dominik Dietrich, Dieter Hutter, Christoph Lüth, and Christian Maeder</i>	
Tracking Behavioral Constraints during Object-Oriented Software Evolution	253
<i>Johan Dovland, Einar Broch Johnsen, and Ingrid Chieh Yu</i>	
Towards the Verification of Adaptable Processes	269
<i>Mario Bravetti, Cinzia Di Giusto, Jorge A. Pérez, and Gianluigi Zavattaro</i>	
Runtime Verification: The Application Perspective	
Runtime Verification: The Application Perspective	284
<i>Yliès Falcone and Lenore D. Zuck</i>	
What Does AI Have to Do with RV? (Extended Abstract)	292
<i>Klaus Havelund</i>	
A Case for “Piggyback” Runtime Monitoring	295
<i>Sylvain Hallé and Raphaël Tremblay-Lessard</i>	

A Unified Approach for Static and Runtime Verification: Framework and Applications	312
<i>Wolfgang Ahrendt, Gordon J. Pace, and Gerardo Schneider</i>	
Statistical Model Checking QoS Properties of Systems with SBIP	327
<i>Saddek Bensalem, Marius Bozga, Benoit Delahaye, Cyrille Jegourel, Axel Legay, and Ayoub Nouri</i>	
Monitoring Temporal Information Flow	342
<i>Rayna Dimitrova, Bernd Finkbeiner, and Markus N. Rabe</i>	
Dynamic Information-Flow Analysis for Multi-threaded Applications . . .	358
<i>Laurent Mounier and Emmanuel Sifakis</i>	
Bounded-Interference Sequentialization for Testing Concurrent Programs	372
<i>Niloofer Razavi, Azadeh Farzan, and Andreas Holzer</i>	
Runtime Verification of Biological Systems	388
<i>Alexandre David, Kim Guldstrand Larsen, Axel Legay, Marius Mikučionis, Danny Bøgsted Poulsen, and Sean Sedwards</i>	
Behavioral Specification Based Runtime Monitors for OSGi Services	405
<i>Jan Olaf Blech, Yliès Falcone, Harald Rueß, and Bernhard Schütz</i>	
Modelling and Decentralised Runtime Control of Self-stabilising Power Micro Grids	420
<i>Arnd Hartmanns and Holger Hermanns</i>	
Model-Based Testing and Model Inference	
Model-Based Testing and Model Inference	440
<i>Karl Meinke and Neil Walkinshaw</i>	
Algorithmic Improvements on Regular Inference of Software Models and Perspectives for Security Testing	444
<i>Roland Groz, Muhammad-Naeem Irfan, and Catherine Oriat</i>	
Test-Case Design by Feature Trees	458
<i>Takashi Kitamura, Ngoc Thi Bich Do, Hitoshi Ohsaki, Ling Fang, and Shunsuke Yatabe</i>	
Model-Based Static Code Analysis for MATLAB Models	474
<i>Zheng Lu and Supratik Mukhopadhyay</i>	
An Incremental Learning Algorithm for Extended Mealy Automata	488
<i>Karl Meinke and Fei Niu</i>	

Learning Techniques for Software Verification and Validation

Learning Techniques for Software Verification and Validation	505
<i>Corina S. Păsăreanu and Mihaela Bobaru</i>	
Learning Stochastic Timed Automata from Sample Executions	508
<i>André de Matos Pedro, Paul Andrew Crocker, and Simão Melo de Sousa</i>	
Learning Minimal Deterministic Automata from Inexperienced Teachers	524
<i>Martin Leucker and Daniel Neider</i>	
Model Learning and Test Generation for Event-B Decomposition	539
<i>Ionut Dinca, Florentin Ipate, and Alin Stefanescu</i>	
Inferring Semantic Interfaces of Data Structures	554
<i>Falk Howar, Malte Isberner, Bernhard Steffen, Oliver Bauer, and Bengt Jonsson</i>	
Learning-Based Test Programming for Programmers	572
<i>Alex Groce, Alan Fern, Martin Erwig, Jervis Pinto, Tim Bauer, and Amin Alipour</i>	

LearnLib Tutorial: From Finite Automata to Register Interface Programs

LearnLib Tutorial: From Finite Automata to Register Interface Programs	587
<i>Falk Howar, Malte Isberner, Maik Merten, and Bernhard Steffen</i>	
Automated Learning Setups in Automata Learning	591
<i>Maik Merten, Malte Isberner, Falk Howar, Bernhard Steffen, and Tiziana Margaria</i>	

RERS Grey-Box Challenge 2012

The RERS Grey-Box Challenge 2012: Analysis of Event-Condition-Action Systems	608
<i>Falk Howar, Malte Isberner, Maik Merten, Bernhard Steffen, and Dirk Beyer</i>	

Author Index	615
-------------------------------	-----