Lecture Notes in Computer Science 6416

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

4th International Symposium
on Leveraging Applications, ISoLA 2010
Heraklion, Crete, Greece, October 18-21, 2010
Proceedings, Part II

Springer

Volume Editors

Tiziana Margaria
University of Potsdam
August-Bebel-Str. 89
14482 Potsdam
Germany
E-mail: margaria@cs.uni-potsdam.de

Bernhard Steffen
TU Dortmund University
Otto-Hahn-Str. 14
44227 Dortmund
Germany
E-mail: steffen@cs.tu-dortmund.de

Library of Congress Control Number: 2010936699

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

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

ISSN 0302-9743
ISBN-10 3-642-16560-5 Springer Berlin Heidelberg New York
ISBN-13 978-3-642-16560-3 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.com

© Springer-Verlag Berlin Heidelberg 2010
Printed in Germany

Typesetting: Camera-ready by author, data conversion by Scientific Publishing Services, Chennai, India
Printed on acid-free paper 06/3180

Preface

This volume contains the conference proceedings of the 4th International Symposium on Leveraging Applications of Formal Methods, Verification and Validation, ISoLA 2010, which was held in Greece (Heraklion, Crete) October 18–21, 2010, and sponsored by EASST.

Following the tradition of its forerunners in 2004, 2006, and 2008 in Cyprus and Chalchidiki, and the ISoLA Workshops in Greenbelt (USA) in 2005, in Poitiers (France) in 2007, and in Potsdam (Germany) in 2009, ISoLA 2010 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, testing, and maintenance of systems from the point of view of their different application domains. Thus, the ISoLA series of events serves the purpose of bridging the gap between designers and developers of rigorous tools, and users in engineering and in other disciplines, and to foster and exploit synergetic relationships among scientists, engineers, software developers, decision makers, and other critical thinkers in companies and organizations. In particular, by providing a venue for the discussion of common problems, requirements, algorithms, methodologies, and practices, ISoLA aims at supporting researchers in their quest to improve the utility, 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 special tracks devoted to the following hot and emerging topics:

- Emerging services and technologies for a converging telecommunications/Web world in smart environments of the Internet of Things
- Learning techniques for software verification and validation
- Modeling and formalizing industrial software for verification, validation and certification
- Formal methods in model-driven development for service-oriented and cloud computing
- Tools in scientific workflow composition
- New challenges in the development of critical embedded systems—an "aeromotive" perspective
- Web science
- Leveraging formal methods through collaboration
- Resource and timing analysis
- Quantitative verification in practice
- Worst case traversal time (WCTT)
- Model transformation and analysis for industrial scale validation
- Certification of software-driven medical devices
- Formal languages and methods for designing and verifying complex engineering systems

- CONNECT: status and plan
- EternalS: mission and roadmap

and five co-located events

- Graduate/postgraduate course on "Soft Skills for IT Professionals in Science and Engineering"
- RERS—challenge on practical automata learning
- IT Simply Works—editorial meeting (ITSy)
- CONNECT internal meeting
- EternalS Task Force meetings

We thank the Track organizers, the members of the Program Committee and their subreferees for their effort in selecting the papers to be presented.

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.

August 2010

Tiziana Margaria
Bernhard Steffen

Organization

Committees

Symposium Chair

Tiziana Margaria	University of Potsdam, Germany

Program Chair

Bernhard Steffen	TU Dortmund, Germany

Program Committee

Yamine Ait Ameur	LISI/ENSMA, France
Frédéric Boniol	IRIT/ENSEEIHT, France
Anne Bouillard	ENS Cachan, France
Marc Boyer	ONERA, France
Karin Breitman	PUC-Rio, Brazil
Marco Antonio Casanova	PUC-Rio, Brazil
Samarjit Chakraborty	TU München, Germany
Noel Crespi	Institut Telecom, France
Rémi Delmas	ONERA, France
Howard Foster	City University London, UK
Pierre-Loïc Garoche	ONERA, France
Dimitra Giannakopoulou	CMU/NASA Ames, USA
Stefania Gnesi	ISTI-CNR, Pisa, Italy
Kevin Hammond	University of St Andrews, UK
Boudewijn Haverkort	ESI, The Netherlands
Michael Hinchey	LERO, Ireland
Valérie Issarny	INRIA, France
Visar Januzaj	TU Darmstadt, Germany
He Jifeng	East China Normal University, China
Joost-Pieter Katoen	RWTH Aachen University, Germany
Joost Kok	Leiden University, The Netherlands
Jens Knoop	Vienna University of Technology, Austria
Stefan Kugele	TU München, Germany
Anna-Lena Lamprecht	TU Dortmund, Germany
Kim G. Larsen	Aalborg University, Denmark
Boris Langer	Diehl Aerospace, Germany

Mark Lawford	McMaster University, Canada
Gyu Myoung Lee	Institut Télécom, France
Björn Lisper	Mälardalen University, Sweden
Zhiming Liu	UNU-IIST, Macao
Tom Maibaum	McMaster University, Canada
Steven Martin	LRI, France
Dominique Mery	University Nancy, France
Pascal Montag	Daimler AG, Germany
Alessandro Moschitti	University of Trento, Italy
Corina Pasareanu	CMU/NASA Ames, USA
Alexander K. Petrenko	ISPRAS, Moscow, Russia
Abhik Roychoudhury	NUS, Singapore
Christian Schallhart	Oxford University, UK
Jean-Luc Scharbarg	IRIT, France
Amal Seghrouchni	University Pierre and Marie Curie, France
Laura Semini	Pisa University, Italy
Giovanni Stea	Pisa University, Italy
Eric Thierry	ENS Lyon, France
Helmut Veith	Vienna University of Technology, Austria
Alan Wassyng	McMaster University, Canada
Virginie Wiels	ONERA, France
Mark D. Wilkinson	Heart and Lung Institute, and Canada
Rostislav Yavorskiy	Microsoft UK/Moscow, Russia
Lenore Zuck	University of Illinois at Chicago, USA

Table of Contents – Part II

EternalS: Mission and Roadmap

Introduction to the EternalS Track: Trustworthy Eternal Systems via Evolving Software, Data and Knowledge 1
Alessandro Moschitti

HATS: Highly Adaptable and Trustworthy Software Using Formal Methods 3
Reiner Hähnle

SecureChange: Security Engineering for Lifelong Evolvable Systems 9
Riccardo Scandariato and Fabio Massacci

3DLife: Bringing the Media Internet to Life 13
Ebroul Izquierdo, Tomas Piatrik, and Qianni Zhang

LivingKnowledge: Kernel Methods for Relational Learning and Semantic Modeling 15
Alessandro Moschitti

Task Forces in the Eternals Coordination Action 20
Reiner Hähnle

Modeling and Analyzing Diversity: Description of EternalS Task Force 1 23
Ina Schaefer

Modeling and Managing System Evolution: Description of EternalS Task Force 2 26
Michael Hafner

Self-adaptation and Evolution by Learning: Description of EternalS Task Force 3 30
Richard Johansson

Overview of Roadmapping by EternalS 32
Jim Clarke and Keith Howker

Formal Methods in Model-Driven Development for Service-Oriented and Cloud Computing

Adaptive Composition of Conversational Services through Graph Planning Encoding 35
Pascal Poizat and Yuhong Yan

Performance Prediction of Service-Oriented Systems with Layered Queueing Networks 51
Mirco Tribastone, Philip Mayer, and Martin Wirsing

Error Handling: From Theory to Practice 66
Ivan Lanese and Fabrizio Montesi

Modeling and Reasoning about Service Behaviors and Their Compositions 82
Aida Čaušević, Cristina Seceleanu, and Paul Pettersson

Design and Verification of Systems with Exogenous Coordination Using Vereofy 97
Christel Baier, Tobias Blechmann, Joachim Klein, Sascha Klüppelholz, and Wolfgang Leister

A Case Study in Model-Based Adaptation of Web Services 112
Javier Cámara, José Antonio Martín, Gwen Salaün, Carlos Canal, and Ernesto Pimentel

Quantitative Verification in Practice

Quantitative Verification in Practice (Extended Abstract) 127
Boudewijn R. Haverkort, Joost-Pieter Katoen, and Kim G. Larsen

Ten Years of Performance Evaluation for Concurrent Systems Using CADP 128
Nicolas Coste, Hubert Garavel, Holger Hermanns, Frédéric Lang, Radu Mateescu, and Wendelin Serwe

Towards Dynamic Adaptation of Probabilistic Systems 143
S. Andova, L.P.J. Groenewegen, and E.P. de Vink

UPPAAL in Practice: Quantitative Verification of a RapidIO Network 160
Jiansheng Xing, Bart D. Theelen, Rom Langerak, Jaco van de Pol, Jan Tretmans, and J.P.M. Voeten

Schedulability Analysis Using Uppaal: Herschel-Planck Case Study 175
Marius Mikučionis, Kim Guldstrand Larsen, Jacob Illum Rasmussen, Brian Nielsen, Arne Skou, Steen Ulrik Palm, Jan Storbank Pedersen, and Poul Hougaard

Model-Checking Temporal Properties of Real-Time HTL Programs 191
André Carvalho, Joel Carvalho, Jorge Sousa Pinto, and Simão Melo de Sousa

CONNECT: Status and Plans

Towards an Architecture for Runtime Interoperability 206
Amel Bennaceur, Gordon Blair, Franck Chauvel, Huang Gang, Nikolaos Georgantas, Paul Grace, Falk Howar, Paola Inverardi, Valérie Issarny, Massimo Paolucci, Animesh Pathak, Romina Spalazzese, Bernhard Steffen, and Bertrand Souville

On Handling Data in Automata Learning: Considerations from the CONNECT Perspective 221
Falk Howar, Bengt Jonsson, Maik Merten, Bernhard Steffen, and Sofia Cassel

A Theory of Mediators for Eternal Connectors 236
Paola Inverardi, Valérie Issarny, and Romina Spalazzese

On-The-Fly Interoperability through Automated Mediator Synthesis and Monitoring 251
Antonia Bertolino, Paola Inverardi, Valérie Issarny, Antonino Sabetta, and Romina Spalazzese

Dependability Analysis and Verification for CONNECTed Systems 263
Felicita Di Giandomenico, Marta Kwiatkowska, Marco Martinucci, Paolo Masci, and Hongyang Qu

Towards a Connector Algebra 278
Marco Autili, Chris Chilton, Paola Inverardi, Marta Kwiatkowska, and Massimo Tivoli

Certification of Software-Driven Medical Devices

Certification of Software-Driven Medical Devices 293
Mark Lawford, Tom Maibaum, and Alan Wassyng

Arguing for Software Quality in an IEC 62304 Compliant Development Process 296
Michaela Huhn and Axel Zechner

Trustable Formal Specification for Software Certification 312
Dominique Méry and Neeraj Kumar Singh

Design Choices for High-Confidence Distributed Real-Time Software 327
Sebastian Fischmeister and Akramul Azim

Assurance Cases in Model-Driven Development of the Pacemaker Software 343
Eunkyoung Jee, Insup Lee, and Oleg Sokolsky

Modeling and Formalizing Industrial Software for Verification, Validation and Certification

Improving Portability of Linux Applications by Early Detection of Interoperability Issues 357
Denis Silakov and Andrey Smachev

Specification Based Conformance Testing for Email Protocols 371
Nikolay Pakulin and Anastasia Tugaenko

Covering Arrays Generation Methods Survey 382
Victor Kuliamin and Alexander Petukhov

Resource and Timing Analysis

A Scalable Approach for the Description of Dependencies in Hard Real-Time Systems 397
Steffen Kollmann, Victor Pollex, Kilian Kempf, and Frank Slomka

Verification of Printer Datapaths Using Timed Automata 412
Georgeta Igna and Frits Vaandrager

Resource Analysis of Automotive/Infotainment Systems Based on Domain-Specific Models – A Real-World Example 424
Klaus Birken, Daniel Hünig, Thomas Rustemeyer, and Ralph Wittmann

Source-Level Support for Timing Analysis 434
Gergö Barany and Adrian Prantl

Practical Experiences of Applying Source-Level WCET Flow Analysis on Industrial Code 449
Björn Lisper, Andreas Ermedahl, Dietmar Schreiner, Jens Knoop, and Peter Gliwa

Worst-Case Analysis of Heap Allocations 464
Wolfgang Puffitsch, Benedikt Huber, and Martin Schoeberl

Partial Flow Analysis with oRange 479
Marianne de Michiel, Armelle Bonenfant, Clément Ballabriga, and Hugues Cassé

Towards an Evaluation Infrastructure for Automotive Multicore Real-Time Operating Systems 483
Jörn Schneider and Christian Eltges

Context-Sensitivity in IPET for Measurement-Based Timing Analysis 487
Michael Zolda, Sven Bünte, and Raimund Kirner

On the Role of Non-functional Properties in Compiler Verification 491
Jens Knoop and Wolf Zimmermann

Author Index 497

Table of Contents – Part I

New Challenges in the Development of Critical Embedded Systems – An "aeromotive" Perspective

New Challenges in the Development of Critical Embedded Systems—An "aeromotive" Perspective 1
Visar Januzaj, Stefan Kugele, Boris Langer, Christian Schallhart, and Helmut Veith

Certification of Embedded Software – Impact of ISO DIS 26262 in the Automotive Domain 3
Bernhard Schätz

Enforcing Applicability of Real-Time Scheduling Theory Feasibility Tests with the Use of Design-Patterns 4
Alain Plantec, Frank Singhoff, Pierre Dissaux, and Jérôme Legrand

Seamless Model-Driven Development Put into Practice 18
Wolfgang Haberl, Markus Herrmannsdoerfer, Stefan Kugele, Michael Tautschnig, and Martin Wechs

Timely Time Estimates 33
Andreas Holzer, Visar Januzaj, Stefan Kugele, and Michael Tautschnig

Compiler-Support for Robust Multi-core Computing 47
Raimund Kirner, Stephan Herhut, and Sven-Bodo Scholz

Formal Languages and Methods for Designing and Verifying Complex Embedded Systems

Thematic Track: Formal Languages and Methods for Designing and Verifying Complex Embedded Systems 58
Yamine Ait Ameur, Frédéric Boniol, Dominique Mery, and Virginie Wiels

Analyzing the Security in the GSM Radio Network Using Attack Jungles 60
Parosh Aziz Abdulla, Jonathan Cederberg, and Lisa Kaati

Formal Modeling and Verification of Sensor Network Encryption Protocol in the OTS/CafeOBJ Method 75
Iakovos Ouranos, Petros Stefaneas, and Kazuhiro Ogata

Model-Driven Design-Space Exploration for Embedded Systems: The Octopus Toolset 90
Twan Basten, Emiel van Benthum, Marc Geilen, Martijn Hendriks, Fred Houben, Georgeta Igna, Frans Reckers, Sebastian de Smet, Lou Somers, Egbert Teeselink, Nikola Trčka, Frits Vaandrager, Jacques Verriet, Marc Voorhoeve, and Yang Yang

Contract-Based Slicing 106
Daniela da Cruz, Pedro Rangel Henriques, and Jorge Sousa Pinto

Worst-Case Traversal Time (WCTT)

Special Track on Worst Case Traversal Time (WCTT) 121
Anne Bouillard, Marc Boyer, Samarjit Chakraborty, Steven Martin, Jean-Luc Scharbarg, Giovanni Stea, and Eric Thierry

The PEGASE Project: Precise and Scalable Temporal Analysis for Aerospace Communication Systems with Network Calculus 122
Marc Boyer, Nicolas Navet, Xavier Olive, and Eric Thierry

NC-Maude: A Rewriting Tool to Play with Network Calculus 137
Marc Boyer

DEBORAH: A Tool for Worst-Case Analysis of FIFO Tandems 152
Luca Bisti, Luciano Lenzini, Enzo Mingozzi, and Giovanni Stea

A Self-adversarial Approach to Delay Analysis under Arbitrary Scheduling 169
Jens B. Schmitt, Hao Wang, and Ivan Martinovic

Flow Control with (Min,+) Algebra 184
Euriell Le Corronc, Bertrand Cottenceau, and Laurent Hardouin

An Interface Algebra for Estimating Worst-Case Traversal Times in Component Networks 198
Nikolay Stoimenov, Samarjit Chakraborty, and Lothar Thiele

Towards Resource-Optimal Routing Plans for Real-Time Traffic 214
Alessandro Lori, Giovanni Stea, and Gigliola Vaglini

Partially Synchronizing Periodic Flows with Offsets Improves Worst-Case End-to-End Delay Analysis of Switched Ethernet 228
Xiaoting Li, Jean-Luc Scharbarg, and Christian Fraboul

Analyzing End-to-End Functional Delays on an IMA Platform 243
Michaël Lauer, Jérôme Ermont, Claire Pagetti, and Frédéric Boniol

Tools in Scientific Workflow Composition

Tools in Scientific Workflow Composition 258
Joost N. Kok, Anna-Lena Lamprecht, and Mark D. Wilkinson

Workflows for Metabolic Flux Analysis: Data Integration and Human Interaction 261
Tolga Dalman, Peter Droste, Michael Weitzel, Wolfgang Wiechert, and Katharina Nöh

Intelligent Document Routing as a First Step towards Workflow Automation: A Case Study Implemented in SQL 276
Carlos Soares and Miguel Calejo

Combining Subgroup Discovery and Permutation Testing to Reduce Reduncancy 285
Jeroen S. de Bruin and Joost N. Kok

Semantically-Guided Workflow Construction in Taverna: The SADI and BioMoby Plug-Ins 301
David Withers, Edward Kawas, Luke McCarthy, Benjamin Vandervalk, and Mark D. Wilkinson

Workflow Construction for Service-Oriented Knowledge Discovery 313
Vid Podpečan, Monika Žakova, and Nada Lavrač

Workflow Composition and Enactment Using jORCA 328
Johan Karlsson, Victoria Martín-Requena, Javier Ríos, and Oswaldo Trelles

A Linked Data Approach to Sharing Workflows and Workflow Results 340
Marco Roos, Sean Bechhofer, Jun Zhao, Paolo Missier, David R. Newman, David De Roure, and M. Scott Marshall

Emerging Services and Technologies for a Converging Telecommunications / Web World in Smart Environments of the Internet of Things

Towards More Adaptive Voice Applications 355
Jörg Ott

Telco Service Delivery Platforms in the Last Decade - A R&D Perspective 367
Sandford Bessler

Ontology-Driven Pervasive Service Composition for Everyday Life 375
Jiehan Zhou, Ekaterina Gilman, Jukka Riekki, Mika Rautiainen, and Mika Ylianttila

Navigating the Web of Things: Visualizing and Interacting with Web-Enabled Objects 390
Mathieu Boussard and Pierrick Thébault

Shaping Future Service Environments with the Cloud and Internet of Things: Networking Challenges and Service Evolution 399
Gyu Myoung Lee and Noel Crespi

Relay Placement Problem in Smart Grid Deployment 411
Wei-Lun Wang and Quincy Wu

Web Science

Towards a Research Agenda for Enterprise Crowdsourcing 425
Maja Vukovic and Claudio Bartolini

Analyzing Collaboration in Software Development Processes through Social Networks 435
Andréa Magalhães Magdaleno, Cláudia Maria Lima Werner, and Renata Mendes de Araujo

A Web-Based Framework for Collaborative Innovation 447
Donald Cowan, Paulo Alencar, Fred McGarry, Carlos Lucena, and Ingrid Nunes

A Distributed Dynamics for WebGraph Decontamination 462
Vanessa C.F. Gonçalves, Priscila M.V. Lima, Nelson Maculan, and Felipe M.G. França

Increasing Users' Trust on Personal Assistance Software Using a Domain-Neutral High-Level User Model 473
Ingrid Nunes, Simone Diniz Junqueira Barbosa, and Carlos J.P. de Lucena

Understanding IT Organizations 488
Claudio Bartolini, Karin Breitman, Simone Diniz Junqueira Barbosa, Mathias Salle, Rita Berardi, Glaucia Melissa Campos, and Erik Eidt

On the 2-Categorical View of Proofs 502
Cecilia Englander and Edward Hermann Haeusler

Model Transformation and Analysis for Industrial Scale Validation

WOMM: A Weak Operational Memory Model 519
Arnab De, Abhik Roychoudhury, and Deepak D'Souza

A Memory Model for Static Analysis of C Programs 535
Zhongxing Xu, Ted Kremenek, and Jian Zhang

Analysing Message Sequence Graph Specifications 549
Joy Chakraborty, Deepak D'Souza, and K. Narayan Kumar

Optimize Context-Sensitive Andersen-Style Points-To Analysis by Method Summarization and Cycle-Elimination 564
Li Qian, Zhao Jianhua, and Li Xuandong

A Formal Analysis of the Web Services Atomic Transaction Protocol with UPPAAL 579
Anders P. Ravn, Jiří Srba, and Saleem Vighio

SPARDL: A Requirement Modeling Language for Periodic Control System 594
Zheng Wang, Jianwen Li, Yongxin Zhao, Yanxia Qi, Geguang Pu, Jifeng He, and Bin Gu

AutoPA: Automatic Prototyping from Requirements 609
Xiaoshan Li, Zhiming Liu, Martin Schäf, and Ling Yin

Systematic Model-Based Safety Assessment Via Probabilistic Model Checking 625
Adriano Gomes, Alexandre Mota, Augusto Sampaio, Felipe Ferri, and Julio Buzzi

Learning Techniques for Software Verification and Validation

Learning Techniques for Software Verification and Validation – Special Track at ISoLA 2010 640
Dimitra Giannakopoulou and Corina S. Păsăreanu

Comparing Learning Algorithms in Automated Assume-Guarantee Reasoning 643
Yu-Fang Chen, Edmund M. Clarke, Azadeh Farzan, Fei He, Ming-Hsien Tsai, Yih-Kuen Tsay, Bow-Yaw Wang, and Lei Zhu

Inferring Compact Models of Communication Protocol Entities 658
Therese Bohlin, Bengt Jonsson, and Siavash Soleimanifard

Inference and Abstraction of the Biometric Passport 673
Fides Aarts, Julien Schmaltz, and Frits Vaandrager

From ZULU to RERS Lessons Learned in the ZULU Challenge 687
Falk Howar, Bernhard Steffen, and Maik Merten

Author Index 705