

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 Zurich, Zurich, 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, Chennai, 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/7407>

Tiziana Margaria · Bernhard Steffen (Eds.)

Leveraging Applications of Formal Methods, Verification and Validation

Verification

8th International Symposium, ISoLA 2018
Limassol, Cyprus, November 5–9, 2018
Proceedings, Part II

Editors

Tiziana Margaria
University of Limerick
Limerick, Ireland

Bernhard Steffen
TU Dortmund
Dortmund, Germany

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-03420-7 ISBN 978-3-030-03421-4 (eBook)
<https://doi.org/10.1007/978-3-030-03421-4>

Library of Congress Control Number: 2018960392

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

© Springer Nature Switzerland AG 2018, corrected publication 2019

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. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

Welcome to ISoLA 2018, the *8th International Symposium on Leveraging Applications of Formal Methods, Verification and Validation*, that was held in Limassol (Cyprus) during November 5–9, 2018, endorsed by EASST, the European Association of Software Science and Technology.

This year's event followed the tradition of its symposia forerunners held 2004 and 2006 in Cyprus, 2008 in Chalkidiki, 2010 and 2012 in Crete, 2014 and 2016 in Corfu, and the series of ISoLA Workshops in Greenbelt (USA) in 2005, Poitiers (France) in 2007, Potsdam (Germany) in 2009, in Vienna (Austria) in 2011, and 2013 in Palo Alto (USA).

As in the previous editions, ISoLA 2018 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 has served the purpose of bridging the gap between designers and developers of rigorous tools on 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:

- A Broader View on Verification: From Static to Runtime and Back
(Organizers: Wolfgang Ahrendt, Marieke Huisman, Giles Reger, Kristin Yvonne Rozier)
- Evaluating Tools for Software Verification
(Organizers: Markus Schordan, Dirk Beyer, Stephen F. Siegel)
- Towards a Unified View of Modeling and Programming
(Organizers: Manfred Broy, Klaus Havelund, Rahul Kumar, Bernhard Steffen)
- RV-TheToP: Runtime Verification from Theory to Industry Practice
(Organizers: Ezio Bartocci and Ylies Falcone)
- Rigorous Engineering of Collective Adaptive Systems
(Organizers: Rocco De Nicola, Stefan Jähnichen, Martin Wirsing)
- Reliable Smart Contracts: State of the Art, Applications, Challenges, and Future Directions
(Organizers: Gerardo Schneider, Martin Leucker, César Sánchez)

- Formal Methods in Industrial Practice—Bridging the Gap
(Organizers: Michael Felderer, Dilian Gurov, Marieke Huisman, Björn Lisper, Rupert Schlick)
- X-by-Construction
(Organizers: Maurice H. ter Beek, Loek Cleophas, Ina Schaefer, and Bruce W. Watson)
- Statistical Model Checking
(Organizers: Axel Legay and Kim Larsen)
- Verification and Validation of Distributed Systems
(Organizer: Cristina Seceleanu)
- Cyber-Physical Systems Engineering
(Organizers: J Paul Gibson, Marc Pantel, Peter Gorm Larsen, Jim Woodcock, John Fitzgerald)

The following events were also held:

- RERS: Challenge on Rigorous Examination of Reactive Systems (Bernhard Steffen)
- Doctoral Symposium and Poster Session (Anna-Lena Lamprecht)
- Industrial Day (Axel Hessenkämper, Falk Howar, Andreas Rausch)

Co-located with the ISoLA Symposium were:

- RV 2018: 18th International Conference on Runtime Verification (Saddek Bensalem, Christian Colombo, and Martin Leucker)
- STRESS 2018: 5th International School on Tool-based Rigorous Engineering of Software Systems (John Hatcliff, Tiziana Margaria, Robby, Bernhard Steffen)

Owing to the growth of ISoLA 2018, the proceedings of this edition are published in four volumes of LNCS: Part 1: Modeling, Part 2: Verification, Part 3: Distributed Systems, and Part 4: Industrial Practice. In addition to the contributions of the main conference, the proceedings also include contributions of the four embedded events and tutorial papers for STRESS.

We thank the track organizers, the members of the Program Committee and their referees for their effort in selecting the papers to be presented, the local Organization Chair, Petros Stratis, the EasyConferences 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 Kyriakos Georgiades for his continuous support for the website and the program, and to Markus Frohme and Julia Rehder for their help with the online conference service (EquinOCS).

Special thanks are due to the following organization for their endorsement: EASST (European Association of Software Science and Technology) and Lero – The Irish Software Research Centre, and our own institutions: TU Dortmund and the University of Limerick.

Organization

Symposium Chair

Bernhard Steffen TU Dortmund, Germany

Program Chair

Bernhard Steffen TU Dortmund, Germany

Program Committee

Wolfgang Ahrendt	Chalmers University of Technology, Sweden
Jesper Andersen	Deon Digital AG
Ezio Bartocci	TU Wien, Austria
Dirk Beyer	LMU Munich, Germany
Manfred Broy	Technische Universität München
Loek Cleophas	TU Eindhoven, The Netherlands
Rocco De Nicola	IMT School for Advanced Studies, Italy
Boris Döder	University of Copenhagen, Denmark
Ylies Falcone	University of Grenoble, France
Michael Felderer	University of Innsbruck, Austria
John Fitzgerald	Newcastle University, UK
Paul Gibson	Telecom Sud Paris, France
Kim Guldstrand Larsen	Aalborg University, Denmark
Dilian Gurov	KTH Royal Institute of Technology, Sweden
John Hatcliff	Kansas State University, USA
Klaus Havelund	Jet Propulsion Laboratory, USA
Fritz Henglein	University of Copenhagen, Denmark
Axel Hessenkämper	Hottinger Baldwin Messtechnik GmbH
Falk Howar	Dortmund University of Technology and Fraunhofer ISST, Germany
Marieke Huisman	University of Twente, The Netherlands
Michael Huth	Imperial College London, UK
Stefan Jaehnichen	TU Berlin, Germany
Rahul Kumar	Microsoft Research
Anna-Lena Lamprecht	Utrecht University, The Netherlands
Peter Gorm Larsen	Aarhus University, Denmark
Axel Legay	Inria, France
Martin Leucker	University of Lübeck, Germany

Björn Lisper	Mälardalen University, Sweden
Leif-Nissen Lundæk	XAIN AG
Tiziana Margaria	Lero, Ireland
Marc Pantel	Université de Toulouse, France
Andreas Rausch	TU Clausthal, Germany
Giles Reger	University of Manchester, UK
Robby	Kansas State University, USA
Kristin Yvonne Rozier	Iowa State University, USA
Ina Schaefer	TU Braunschweig, Germany
Rupert Schlick	AIT Austrian Institute of Technology, Austria
Gerardo Schneider	University of Gothenburg, Sweden
Markus Schordan	Lawrence Livermore National Laboratory, USA
Cristina Seceleanu	Mälardalen University, Sweden
Stephen F. Siegel	University of Delaware, USA
César Sánchez	IMDEA Software Institute, Spain
Bruce W. Watson	Stellenbosch University, South Africa
Martin Wirsing	LMU München, Germany
James Woodcock	University of York, UK
Maurice ter Beek	ISTI-CNR, Italy
Jaco van de Pol	University of Twente, The Netherlands

Additional Reviewers

Yehia Abd Alrahman	Neil Jones
Dhaminda Abeywickrama	Sebastiaan Joosten
Lenz Belzner	Gabor Karsai
Saddek Bensalem	Alexander Knapp
Egon Boerger	Timothy Lethbridge
Marius Bozga	Chunhua Liao
Tomas Bures	Alberto Lluch-Lafuente
Rance Cleaveland	Alessandro Maggi
Giovanna Di Marzo Serugendo	Dominique Méry
Matthew Dwyer	Birger Møller-Pedersen
Benedikt Eberhardinger	Stefan Naujokat
Rim El Ballouli	Ayoub Nouri
Thomas Gabor	Liam O'Connor
Stephen Gilmore	Doron Peled
Emma Hart	Thomy Phan
Arnd Hartmanns	Jeremy Pitt
Rolf Hennicker	Hella Ponsar
Petr Hnetynka	Andre Reichstaller
Reiner Hähnle	Jeff Sanders
Patrik Jansson	Sean Sedwards
Einar Broch Johnsen	Christoph Seidl

Bran Selic
Steven Smyth
Josef Strnadel
Jan Sürmeli
Louis-Marie Traonouez

Mirco Tribastone
Andrea Vandin
Markus Voelter
Franco Zambonelli
Natalia Zon

Contents – Part II

A Broader View on Verification: From Static to Runtime and Back

A Broader View on Verification: From Static to Runtime and Back (Track Summary)	3
<i>Wolfgang Ahrendt, Marieke Huisman, Giles Reger, and Kristin Yvonne Rozier</i>	
Monitoring Hyperproperties by Combining Static Analysis and Runtime Verification	8
<i>Borzoo Bonakdarpour, Cesar Sanchez, and Gerardo Schneider</i>	
Temporal Reasoning on Incomplete Paths	28
<i>Dana Fisman and Hillel Kugler</i>	
Towards a Notion of Coverage for Incomplete Program-Correctness Proofs	53
<i>Bernhard Beckert, Mihai Herda, Stefan Kobischke, and Mattias Ulbrich</i>	
Generating Inductive Shape Predicates for Runtime Checking and Formal Verification	64
<i>Jan H. Boockmann, Gerald Lüttgen, and Jan Tobias Mühlberg</i>	
Runtime Assertion Checking and Static Verification: Collaborative Partners	75
<i>Fonenantsoa Maurica, David R. Cok, and Julien Signoles</i>	
A Language-Independent Program Verification Framework	92
<i>Xiaohong Chen and Grigore Roşu</i>	
Programming Safe Robotics Systems: Challenges and Advances	103
<i>Ankush Desai, Shaz Qadeer, and Sanjit A. Seshia</i>	
Generating Component Interfaces by Integrating Static and Symbolic Analysis, Learning, and Runtime Monitoring	120
<i>Falk Howar, Dimitra Giannakopoulou, Malte Mues, and Jorge A. Navas</i>	
Evaluating Tools for Software Verification	
Evaluating Tools for Software Verification (Track Introduction)	139
<i>Markus Schordan, Dirk Beyer, and Stephen F. Siegel</i>	

Strategy Selection for Software Verification Based on Boolean Features: A Simple but Effective Approach	144
<i>Dirk Beyer and Matthias Dangl</i>	
Symbolic Execution and Deductive Verification Approaches to VerifyThis 2017 Challenges	160
<i>Ziqing Luo and Stephen F. Siegel</i>	
Runtime and Memory Evaluation of Data Race Detection Tools	179
<i>Pei-Hung Lin, Chunhua Liao, Markus Schordan, and Ian Karlin</i>	
In-Place vs. Copy-on-Write CEGAR Refinement for Block Summarization with Caching	197
<i>Dirk Beyer and Karlheinz Friedberger</i>	
Deductive Verification of Unmodified Linux Kernel Library Functions	216
<i>Denis Efremov, Mikhail Mandrykin, and Alexey Khoroshilov</i>	
Synthesizing Subtle Bugs with Known Witnesses	235
<i>Marc Jasper and Bernhard Steffen</i>	
Statistical Model Checking	
Statistical Model Checking the 2018 Edition!	261
<i>Kim Guldstrand Larsen and Axel Legay</i>	
Chasing Errors Using Biasing Automata	271
<i>Lei Bu, Doron Peled, Dashuan Shen, and Yael Tzirulnikov</i>	
On the Sequential Massart Algorithm for Statistical Model Checking.	287
<i>Cyrille Jegourel, Jun Sun, and Jin Song Dong</i>	
Quantitative Risk Assessment of Safety-Critical Systems via Guided Simulation for Rare Events.	305
<i>Stefan Puch, Martin Fränzle, and Sebastian Gerwinn</i>	
Monte Carlo Tree Search for Verifying Reachability in Markov Decision Processes	322
<i>Pranav Ashok, Tomáš Brázdil, Jan Křetínský, and Ondřej Slámečka</i>	
Lightweight Statistical Model Checking in Nondeterministic Continuous Time	336
<i>Pedro R. D’Argenio, Arnd Hartmanns, and Sean Sedwards</i>	
Statistical Model Checking of Incomplete Stochastic Systems	354
<i>Shiraj Arora, Axel Legay, Tania Richmond, and Louis-Marie Traonouez</i>	

Statistical Model Checking of a Moving Block Railway Signalling Scenario with UPPAAL SMC: Experience and Outlook 372
Davide Basile, Maurice H. ter Beek, and Vincenzo Ciancia

Mitigating Security Risks Through Attack Strategies Exploration 392
Braham Lotfi Mediouni, Ayoub Nouri, Marius Bozga, Axel Legay, and Saddek Bensalem

Statistical Model Checking of Processor Systems in Various Interrupt Scenarios 414
Josef Strnadel

RERS 2018

RERS 2018: CTL, LTL, and Reachability 433
Marc Jasper, Malte Mues, Maximilian Schlüter, Bernhard Steffen, and Falk Howar

Doctoral Symposium

Track Introduction – Doctoral Symposium 2018 451
Anna-Lena Lamprecht

Assuring Intelligent Ambient Assisted Living Solutions by Statistical Model Checking 457
Ashalatha Kunnappilly, Raluca Marinescu, and Cristina Seceleanu

Implementation of Privacy Calculus and Its Type Checking in Maude 477
Georgios V. Pitsiladis and Petros Stefaneas

Correction to: Assuring Intelligent Ambient Assisted Living Solutions by Statistical Model Checking C1
Ashalatha Kunnappilly, Raluca Marinescu, and Cristina Seceleanu

Author Index 495