

*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

Industrial Practice

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

*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 978-3-030-03426-9              ISBN 978-3-030-03427-6 (eBook)  
<https://doi.org/10.1007/978-3-030-03427-6>

Library of Congress Control Number: 2018960393

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

© Springer Nature Switzerland AG 2018

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.

November 2018

Tiziana Margaria  
Bernhard Steffen

# Organization

## Symposium Chair

Bernhard Steffen      TU Dortmund, Germany

## Program Chair

Tiziana Margaria      University of Limerick, Ireland

## 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 IV

## Runtime Verification from the Theory to the Industry Practice

RV-TheToP: Runtime Verification from Theory to the Industry Practice (Track Introduction) . . . . .	3
<i>Ezio Bartocci and Yliès Falcone</i>	
Opportunities and Challenges in Monitoring Cyber-Physical Systems Security. . . . .	9
<i>Borzoo Bonakdarpour, Jyotirmoy V. Deshmukh, and Miroslav Pajic</i>	
Migrating Monitors + ABE: A Suitable Combination for Secure IoT? . . . . .	19
<i>Gordon J. Pace, Pablo Picazo-Sanchez, and Gerardo Schneider</i>	
Capturing Inter-process Communication for Runtime Verification on Android. . . . .	25
<i>Alex Villazón, Haiyang Sun, and Walter Binder</i>	
Considering Academia-Industry Projects Meta-characteristics in Runtime Verification Design . . . . .	32
<i>Christian Colombo and Gordon J. Pace</i>	
Flexible Monitor Deployment for Runtime Verification of Large Scale Software . . . . .	42
<i>Teng Zhang, Gregory Eakman, Insup Lee, and Oleg Sokolsky</i>	
Increasing the Reusability of Enforcers with Lifecycle Events. . . . .	51
<i>Oliviero Riganelli, Daniela Micucci, and Leonardo Mariani</i>	
BDDs on the Run . . . . .	58
<i>Klaus Havelund and Doron Peled</i>	
Verifying Real-World Software with Contracts for Concurrency . . . . .	70
<i>João M. Lourenço</i>	

## Formal Methods in Industrial Practice - Bridging the Gap

Formal Methods in Industrial Practice - Bridging the Gap (Track Summary) . . . . .	77
<i>Michael Felderer, Dilian Gurov, Marieke Huisman, Björn Lisper, and Rupert Schlick</i>	

<b>Model-Based Testing for Avionic Systems Proven Benefits and Further Challenges . . . . .</b>	<b>82</b>
<i>Jan Peleska, Jörg Brauer, and Wen-ling Huang</i>	
<b>Test Case Generation with PATHCRAWLER/LTEST: How to Automate an Industrial Testing Process . . . . .</b>	<b>104</b>
<i>Sébastien Bardin, Nikolai Kosmatov, Bruno Marre, David Mentré, and Nicky Williams</i>	
<b>Pitfalls in Applying Model Learning to Industrial Legacy Software . . . . .</b>	<b>121</b>
<i>Omar al Duhaiby, Arjan Mooij, Hans van Wezep, and Jan Friso Groote</i>	
<b>Formal Verification in Automotive Industry: Enablers and Obstacles . . . . .</b>	<b>139</b>
<i>Mattias Nyberg, Dilian Gurov, Christian Lidström, Andreas Rasmusson, and Jonas Westman</i>	
<b>Scalability of Deductive Verification Depends on Method Call Treatment . . .</b>	<b>159</b>
<i>Alexander Knüppel, Thomas Thüm, Carsten Padylla, and Ina Schaefer</i>	
<b>Java Automated Deductive Verification in Practice: Lessons from Industrial Proof-Based Projects . . . . .</b>	<b>176</b>
<i>David R. Cok</i>	
<b>Security Filters for IoT Domain Isolation . . . . .</b>	<b>194</b>
<i>Dominique Bolignano and Florence Plateau</i>	
<b>20 Years of UPPAAL Enabled Industrial Model-Based Validation and Beyond . . . . .</b>	<b>212</b>
<i>Kim G. Larsen, Florian Lorber, and Brian Nielsen</i>	
<b>Verification of Operating System Monolithic Kernels Without Extensions . . .</b>	<b>230</b>
<i>Evgeny Novikov and Ilja Zakharov</i>	
<b>A Proposal of an Example and Experiments Repository to Foster Industrial Adoption of Formal Methods . . . . .</b>	<b>249</b>
<i>Rupert Schlick, Michael Felderer, Istvan Majzik, Roberto Nardone, Alexander Raschke, Colin Snook, and Valeria Vittorini</i>	
<b>Reliable Smart Contracts: State-of-the-art, Applications, Challenges and Future Directions</b>	
<b>Reliable Smart Contracts: State-of-the-Art, Applications, Challenges and Future Directions . . . . .</b>	<b>275</b>
<i>César Sánchez, Gerardo Schneider, and Martin Leucker</i>	
<b>Smart Contracts and Opportunities for Formal Methods . . . . .</b>	<b>280</b>
<i>Andrew Miller, Zhicheng Cai, and Somesh Jha</i>	

Contracts over Smart Contracts: Recovering from Violations Dynamically . . .	300
<i>Christian Colombo, Joshua Ellul, and Gordon J. Pace</i>	
Security Analysis of Smart Contracts in Datalog . . . . .	316
<i>Petar Tsankov</i>	
Temporal Properties of Smart Contracts . . . . .	323
<i>Ilya Sergey, Amrit Kumar, and Aquinas Hobor</i>	
Temporal Aspects of Smart Contracts for Financial Derivatives . . . . .	339
<i>Christopher D. Clack and Gabriel Vanca</i>	
Marlowe: Financial Contracts on Blockchain . . . . .	356
<i>Pablo Lamela Seijas and Simon Thompson</i>	
SMT-Based Verification of Solidity Smart Contracts . . . . .	376
<i>Leonardo Alt and Christian Reitwiessner</i>	
Blockchains as Kripke Models: An Analysis of Atomic Cross-Chain Swap. . . . .	389
<i>Yoichi Hirai</i>	
A Language-Independent Approach to Smart Contract Verification . . . . .	405
<i>Xiaohong Chen, Daejun Park, and Grigore Roşu</i>	
Towards Adding Variety to Simplicity. . . . .	414
<i>Nachiappan Valliappan, Solène Miriaz, Elisabet Lobo Vesga, and Alejandro Russo</i>	
Fun with Bitcoin Smart Contracts . . . . .	432
<i>Massimo Bartoletti, Tiziana Cimoli, and Roberto Zunino</i>	
Computing Exact Worst-Case Gas Consumption for Smart Contracts. . . . .	450
<i>Matteo Marescotti, Martin Blicha, Antti E. J. Hyvärinen, Sepideh Asadi, and Natasha Sharygina</i>	

## Industrial Day

Digital Transformation Trends: Industry 4.0, Automation, and AI: Industrial Track at ISO LA 2018 . . . . .	469
<i>Axel Hessenkämper, Falk Howar, and Andreas Rausch</i>	
A Methodology for Combinatory Process Synthesis: Process Variability in Clinical Pathways . . . . .	472
<i>Tristan Schäfer, Frederik Möller, Anja Burmann, Yevgen Pikus, Norbert Weissenberg, Marcus Hintze, and Jakob Rehof</i>	

Automatic Composition of Rough Solution Possibilities in the Target  
Planning of Factory Planning Projects by Means of Combinatory Logic. . . . . 487  
*Jan Winkels, Julian Graefenstein, Tristan Schäfer, David Scholz,  
Jakob Rehof, and Michael Henke*

GOLD: Global Organization aLignment and Decision - Towards  
the Hierarchical Integration of Heterogeneous Business Models . . . . . 504  
*Barbara Steffen and Steve Boßelmann*

**Author Index** . . . . . 529