

Founding Editors

Gerhard Goos

Karlsruhe Institute of Technology, Karlsruhe, Germany

Juris Hartmanis

Cornell University, Ithaca, NY, USA

Editorial Board Members

Elisa Bertino

Purdue University, West Lafayette, IN, USA

Wen Gao

Peking University, Beijing, China

Bernhard Steffen 

TU Dortmund University, Dortmund, Germany

Gerhard Woeginger 

RWTH Aachen, Aachen, Germany

Moti Yung

Columbia University, New York, NY, USA

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

Applications

9th International Symposium
on Leveraging Applications of Formal Methods, ISoLA 2020
Rhodes, Greece, October 20–30, 2020
Proceedings, Part III

Editors

Tiziana Margaria 
University of Limerick and Lero
Limerick, Ireland

Bernhard Steffen 
TU Dortmund
Dortmund, Germany

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-030-61466-9 ISBN 978-3-030-61467-6 (eBook)
<https://doi.org/10.1007/978-3-030-61467-6>

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

© Springer Nature Switzerland AG 2020

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, expressed 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

Introduction

It is our responsibility, as general and program chairs, to welcome the participants to the 9th International Symposium on Leveraging Applications of Formal Methods, Verification and Validation (ISoLA), planned to take place in Rhodes, Greece, during October 20–30, 2020, endorsed by the European Association of Software Science and Technology (EASST).

This year’s event follows the tradition of its symposia forerunners held in Paphos, Cyprus (2004 and 2006), Chalkidiki, Greece (2008), Crete, Greece (2010 and 2012), Corfu, Greece (2014 and 2016), and most recently in Limassol, Cyprus (2018), and the series of ISoLA workshops in Greenbelt, USA (2005), Poitiers, France (2007), Potsdam, Germany (2009), Vienna, Austria (2011), and Palo Alto, USA (2013).

Considering that this year’s situation is unique and unlike any previous one due to the ongoing COVID-19 pandemic, and that ISoLA’s symposium touch and feel is much unlike most conventional, paper-based conferences, after much soul searching we are faced with a true dilemma. “Virtualizing” the event, as many conferences have done, violates the true spirit of the symposium, which is rooted in the gathering of communities and the discussions within and across the various communities materialized in the special tracks and satellite events. Keeping with the physical meeting and holding it in a reduced form (as many may not be able to or feel comfortable with travel) under strict social distancing rules may also end up not being feasible. At the time of writing there is a resurgence of cases in several countries, many nations are compiling “green lists” of countries with which they entertain free travel relations, and these lists are updated – most frequently shortened – at short notice, with severe consequence for the travelers. Many governments and universities are again strengthening the travel restrictions for their employees, and many of us would anyway apply caution due to our own specific individual situation.

To be able to react as flexibly as possible to this situation, we decided to split ISoLA 2020 into two parts, one this year and one in October 2021, with the track organizers deciding when their track will take place. So far both dates have promoters, but it may still happen that, in the end, the entire event needs to move. All accepted papers are published in time, but some tracks will present their papers at the 2021 event.

As in the previous editions, ISoLA 2020 provides 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 one side, and users in engineering and in other disciplines on the other side. 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 consists of a collection of special tracks devoted to the following hot and emerging topics:

- Reliable Smart Contracts: State-of-the-art, Applications, Challenges and Future Directions
(Organizers: Gordon Pace, César Sánchez, Gerardo Schneider)
- Engineering of Digital Twins for Cyber-Physical Systems
(Organizers: John Fitzgerald, Pieter Gorm Larsen, Tiziana Margaria, Jim Woodcock)
- Verification and Validation of Concurrent and Distributed Systems
(Organizers: Cristina Seceleanu, Marieke Huisman)
- Modularity and (De-)composition in Verification
(Organizers: Reiner Hähnle, Eduard Kamburjan, Dilian Gurov)
- Software Verification Tools
(Organizers: Markus Schordan, Dirk Beyer, Irena Boyanova)
- X-by-Construction: Correctness meets Probability
(Organizers: Maurice H. ter Beek, Loek Cleophas, Axel Legay, Ina Schaefer, Bruce W. Watson)
- Rigorous Engineering of Collective Adaptive Systems
(Organizers: Rocco De Nicola, Stefan Jähnichen, Martin Wirsing)
- Automated Verification of Embedded Control Software
(Organizers: Dilian Gurov, Paula Herber, Ina Schaefer)
- Automating Software Re-Engineering
(Organizers: Serge Demeyer, Reiner Hähnle, Heiko Mantel)
- 30 years of Statistical Model Checking!
(Organizers: Kim G. Larsen, Axel Legay)
- From Verification to Explanation
(Organizers: Holger Herrmanns, Christel Baier)
- Formal methods for DIStributed COmputing in future RAILway systems (DisCo-Rail 2020)
(Organizers: Alessandro Fantechi, Stefania Gnesi, Anne Haxthausen)
- Programming: What is Next?
(Organizers: Klaus Havelund, Bernhard Steffen)

With the embedded events:

- RERS: Challenge on Rigorous Examination of Reactive Systems (Falk Howar, Markus Schordan, Bernhard Steffen)
- Doctoral Symposium and Poster Session (A. L. Lamprecht)
- Industrial Day (Falk Howar, Johannes Neubauer, Andreas Rausch)

Colocated with the ISoLA symposium is:

- STRESS 2020 – 5th International School on Tool-based Rigorous Engineering of Software Systems (J. Hatcliff, T. Margaria, Robby, B. Steffen)

Altogether the ISoLA 2020 proceedings comprises four volumes, Part 1: Verification Principles, Part 2: Engineering Principles, Part 3: Applications, and Part 4: Tools, Trends, and Tutorials, which also covers the associated events.

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, and the EasyConferences team for their continuous and precious support during the entire two-year period preceding the events, and Springer for being, as usual, a very reliable partner for 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 editorial system 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 University and the University of Limerick.

We wish you, as an ISoLA participant, a wonderful experience at this edition, and for you, reading the proceedings at a later occasion, valuable new insights that hopefully contribute to your research and its uptake.

August 2020

Tiziana Margaria
Bernhard Steffen

Organization

Symposium Chair

Tiziana Margaria

University of Limerick and Lero, Ireland

PC Chair

Bernhard Steffen

TU Dortmund University, Germany

PC Members

Christel Baier

Technische Universität Dresden, Germany

Maurice ter Beek

ISTI-CNR, Italy

Dirk Beyer

LMU Munich, Germany

Irena Bojanova

NIST, USA

Loek Cleophas

Eindhoven University of Technology, The Netherlands

Rocco De Nicola

IMT Lucca, Italy

Serge Demeyer

Universiteit Antwerpen, Belgium

Alessandro Fantechi

University of Florence, Italy

John Fitzgerald

Newcastle University, UK

Stefania Gnesi

CNR, Italy

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

Anne E. Haxthausen

Technical University of Denmark, Denmark

Paula Herber

University of Münster, Germany

Holger Hermanns

Saarland University, Germany

Falk Howar

Dortmund University of Technology and

Fraunhofer ISST, Germany

Marieke Huisman

University of Twente, The Netherlands

Reiner Hähnle

Technische Universität Darmstadt, Germany

Stefan Jähnichen

TU Berlin, Germany

Eduard Kamburjan

Technische Universität Darmstadt, Germany

Anna-Lena Lamprecht

Utrecht University, The Netherlands

Peter Gorm Larsen

Aarhus University, Denmark

Axel Legay

Université Catholique de Louvain, Belgium

Heiko Mantel

Technische Universität Darmstadt, Germany

Tiziana Margaria

University of Limerick and Lero, Ireland

Johannes Neubauer

Materna, Germany

Gordon Pace

University of Malta, Malta

Cesar Sanchez

IMDEA Software Institute, Madrid, Spain

Ina Schaefer	TU Braunschweig, Germany
Gerardo Schneider	University of Gothenburg, Sweden
Markus Schordan	Lawrence Livermore National Laboratory, USA
Cristina Seceleanu	Mälardalen University, Sweden
Bernhard Steffen	TU Dortmund University, Germany
Bruce Watson	Stellenbosch University, South Africa
Martin Wirsing	Ludwig-Maximilians-Universität München, Germany
James Woodcock	University of York, UK

Reviewers

Aho, Pekka	Hungar, Hardi
Aichernig, Bernhard	Inverso, Omar
Backeman, Peter	Iosti, Simon
Baranov, Eduard	Jacobs, Bart
Basile, Davide	Jaeger, Manfred
Beckert, Bernhard	Jensen, Peter
Bensalem, Saddek	Johnsen, Einar Broch
Bettini, Lorenzo	Jongmans, Sung-Shik
Beyer, Dirk	Jähnichen, Stefan
Bourr, Khalid	Kanav, Sudeep
Bubel, Richard	Konnov, Igor
Bures, Tomas	Kosak, Oliver
Casadei, Roberto	Kosmatov, Nikolai
Castiglioni, Valentina	Kretinsky, Jan
Ciatto, Giovanni	Könighofer, Bettina
Cimatti, Alessandro	Lanese, Ivan
Damiani, Ferruccio	Lecomte, Thierry
Di Marzo Serugendo, Giovanna	Lluch Lafuente, Alberto
Duong, Tan	Loreti, Michele
Filliâtre, Jean-Christophe	Maggi, Alessandro
Fränzle, Martin	Mariani, Stefano
Gabor, Thomas	Mazzanti, Franco
Gadducci, Fabio	Morichetta, Andrea
Galletta, Letterio	Nyberg, Mattias
Geisler, Signe	Omicini, Andrea
Gerostathopoulos, Ilias	Orlov, Dmitry
Guanciale, Roberto	Pacovsky, Jan
Heinrich, Robert	Parsai, Ali
Hillston, Jane	Peled, Doron
Hnetynka, Petr	Piho, Paul
Hoffmann, Alwin	Pugliese, Rosario

Pun, Violet Ka I
Reisig, Wolfgang
Schlingloff, Holger
Seifermann, Stephan
Soulat, Romain
Steinhöfel, Dominic
Stolz, Volker
Sürmeli, Jan
Tiezzi, Francesco
Tini, Simone
Tognazzi, Stefano
Tribastone, Mirco

Trubiani, Catia
Tuosto, Emilio
Ulbrich, Mattias
Vandin, Andrea
Vercammen, Sten
Viroli, Mirko
Wadler, Philip
Wanninger, Constantin
Weidenbach, Christoph
Wirsing, Martin
Zambonelli, Franco

Contents – Part III

Reliable Smart Contracts: State-of-the-art, Applications, Challenges and Future Directions

Reliable Smart Contracts	3
<i>Gordon J. Pace, César Sánchez, and Gerardo Schneider</i>	
Functional Verification of Smart Contracts via Strong Data Integrity	9
<i>Wolfgang Ahrendt and Richard Bubel</i>	
Bitcoin Covenants Unchained	25
<i>Massimo Bartoletti, Stefano Lande, and Roberto Zunino</i>	
Specifying Framing Conditions for Smart Contracts.	43
<i>Bernhard Beckert and Jonas Schiffel</i>	
Making Tezos Smart Contracts More Reliable with Coq	60
<i>Bruno Bernardo, Raphaël Cauderlier, Guillaume Claret, Arvid Jakobsson, Basile Pesin, and Julien Tesson</i>	
UTxO- vs Account-Based Smart Contract Blockchain Programming Paradigms	73
<i>Lars Brünjes and Murdoch J. Gabbay</i>	
Native Custom Tokens in the Extended UTXO Model.	89
<i>Manuel M. T. Chakravarty, James Chapman, Kenneth MacKenzie, Orestis Melkonian, Jann Müller, Michael Peyton Jones, Polina Vinogradova, and Philip Wadler</i>	
UTXO _{ma} : UTXO with Multi-asset Support.	112
<i>Manuel M. T. Chakravarty, James Chapman, Kenneth MacKenzie, Orestis Melkonian, Jann Müller, Michael Peyton Jones, Polina Vinogradova, Philip Wadler, and Joachim Zahnentferner</i>	
Towards Configurable and Efficient Runtime Verification of Blockchain Based Smart Contracts at the Virtual Machine Level	131
<i>Joshua Ellul</i>	
Compiling Quantitative Type Theory to Michelson for Compile-Time Verification and Run-time Efficiency in Juvix.	146
<i>Christopher Goes</i>	
Efficient Static Analysis of Marlowe Contracts	161
<i>Pablo Lamela Seijas, David Smith, and Simon Thompson</i>	

Accurate Smart Contract Verification Through Direct Modelling	178
<i>Matteo Marescotti, Rodrigo Otoni, Leonardo Alt, Patrick Eugster, Antti E. J. Hyvärinen, and Natasha Sharygina</i>	
Smart Derivatives: On-Chain Forwards for Digital Assets	195
<i>Alfonso D. D. M. Rius and Eamonn Gashier</i>	
The Good, The Bad and The Ugly: Pitfalls and Best Practices in Automated Sound Static Analysis of Ethereum Smart Contracts	212
<i>Clara Schneidewind, Markus Scherer, and Matteo Maffei</i>	
Automated Verification of Embedded Control Software	
Automated Verification of Embedded Control Software: Track Introduction.	235
<i>Dilian Gurov, Paula Herber, and Ina Schaefer</i>	
A Model-Based Approach to the Design, Verification and Deployment of Railway Interlocking System	240
<i>Arturo Amendola, Anna Becchi, Roberto Cavada, Alessandro Cimatti, Alberto Griggio, Giuseppe Scaglione, Angelo Susi, Alberto Tacchella, and Matteo Tessi</i>	
Guess What I’m Doing!: Rendering Formal Verification Methods Ripe for the Era of Interacting Intelligent Systems	255
<i>Martin Fränzle and Paul Kröger</i>	
On the Industrial Application of Critical Software Verification with VerCors.	273
<i>Marieke Huisman and Raúl E. Monti</i>	
A Concept of Scenario Space Exploration with Criticality Coverage Guarantees: Extended Abstract	293
<i>Hardi Hungar</i>	
Towards Automated Service-Oriented Verification of Embedded Control Software Modeled in Simulink	307
<i>Timm Liebrenz, Paula Herber, and Sabine Glesner</i>	
Verifying Safety Properties of Robotic Plans Operating in Real-World Environments via Logic-Based Environment Modeling	326
<i>Tim Meywerk, Marcel Walter, Vladimir Herdt, Jan Kleinekathöfer, Daniel Große, and Rolf Drechsler</i>	
Formally Proving Compositionality in Industrial Systems with Informal Specifications	348
<i>Mattias Nyberg, Jonas Westman, and Dilian Gurov</i>	

Specification, Synthesis and Validation of Strategies for Collaborative Embedded Systems	366
<i>Bernd-Holger Schlingloff</i>	
Formal methods for DIStributed COmputing in future RAILway systems	
Formal Methods for Distributed Computing in Future Railway Systems.	389
<i>Alessandro Fantechi, Stefania Gnesi, and Anne E. Haxthausen</i>	
Ensuring Safety with System Level Formal Modelling.	393
<i>Thierry Lecomte, Mathieu Comptier, Julien Molinero, and Denis Sabatier</i>	
A Modular Design Framework to Assess Intelligent Trains.	404
<i>Simon Collart-Dutilleul and Philippe Bon</i>	
Formal Modelling and Verification of a Distributed Railway Interlocking System Using UPPAAL.	415
<i>Per Lange Laursen, Van Anh Thi Trinh, and Anne E. Haxthausen</i>	
New Distribution Paradigms for Railway Interlocking	434
<i>Jan Peleska</i>	
Model Checking a Distributed Interlocking System Using k -induction with RT-Tester	449
<i>Signe Geisler and Anne E. Haxthausen</i>	
Designing a Demonstrator of Formal Methods for Railways Infrastructure Managers	467
<i>Davide Basile, Maurice H. ter Beek, Alessandro Fantechi, Alessio Ferrari, Stefania Gnesi, Laura Masullo, Franco Mazzanti, Andrea Piattino, and Daniele Trentini</i>	
Author Index	487