Lecture Notes in Computer Science 12476

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

Verification Principles

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

Springer

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 978-3-030-61361-7 ISBN 978-3-030-61362-4 (eBook)
https://doi.org/10.1007/978-3-030-61362-4

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

© Springer Nature Switzerland AG 2020
Chapters 8, 9, and 26 are licensed under the terms of the Creative Commons Attribution 4.0 International License (http://creativecommons.org/licenses/by/4.0/). For further details see license information in the chapters.
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 Sànchez, 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 (DisCoRail 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
Aichernig, Bernhard
Backeman, Peter
Baranov, Eduard
Basile, Davide
Beckert, Bernhard
Bensalem, Saddek
Bettini, Lorenzo
Beyer, Dirk
Bourr, Khalid
Bubel, Richard
Bures, Tomas
Casadei, Roberto
Castiglioni, Valentina
Ciatto, Giovanni
Cimatti, Alessandro
Damiani, Ferruccio
Di Marzo Serugendo, Giovanna
Duong, Tan
Filliâtre, Jean-Christophe
Fränzle, Martin
Gabor, Thomas
Gadducci, Fabio
Galletta, Letterio
Geisler, Signe
Gerostathopoulos, Ilias
Guanciale, Roberto
Heinrich, Robert
Hillston, Jane
Hnetynka, Petr
Hoffmann, Alwin
Hungar, Hardi
Inverso, Omar
Iosti, Simon
Jacobs, Bart
Jaeger, Manfred
Jensen, Peter
Johnsen, Einar Broch
Jongmans, Sung-Shik
Jähnichen, Stefan
Kanav, Sudeep
Konnov, Igor
Kosak, Oliver
Kosmatov, Nikolai
Kretinsky, Jan
Könighofer, Bettina
Lanese, Ivan
Lecomte, Thierry
Lluch Lafuente, Alberto
Loreti, Michele
Maggi, Alessandro
Mariani, Stefano
Mazzanti, Franco
Morichetta, Andrea
Nyberg, Mattias
Omicini, Andrea
Orlov, Dmitry
Pacovsky, Jan
Parsai, Ali
Peled, Doron
Piho, Paul
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 I

Modularity and (De-)Composition in Verification

Who Carries the Burden of Modularity? Introduction to ISoLA 2020 Track on *Modularity and (De-)composition in Verification* 3
Dilian Gurov, Reiner Hähnle, and Eduard Kamburjan

On Testing Message-Passing Components 22
Alex Coto, Roberto Guanciale, and Emilio Tuosto

Composing Communicating Systems, Synchronously. 39
Franco Barbanera, Ivan Lanese, and Emilio Tuosto

Modular Verification of JML Contracts Using Bounded Model Checking. . . . 60
Bernhard Beckert, Michael Kirsten, Jonas Klamroth, and Mattias Ulbrich

On Slicing Software Product Line Signatures 81
Ferruccio Damiani, Michael Lienhardt, and Luca Paolini

Assumption-Commitment Types for Resource Management in Virtually Timed Ambients 103
Einar Broch Johnsen, Martin Steffen, and Johanna Beate Stumpf

Abstraction and Genericity in Why3 122
Jean-Christophe Filliâtre and Andrei Paskevich

Verification Artifacts in Cooperative Verification: Survey and Unifying Component Framework 143
Dirk Beyer and Heike Wehrheim

An Interface Theory for Program Verification. 168
Dirk Beyer and Sudeep Kanav

Scaling Correctness-by-Construction 187
Alexander Knüppel, Tobias Runge, and Ina Schaefer

X-by-Construction: Correctness Meets Probability

X-by-Construction: Correctness Meets Probability. 211
Maurice H. ter Beek, Loek Cleophas, Axel Legay, Ina Schaefer, and Bruce W. Watson

Correctness by Construction for Probabilistic Programs 216
Annabelle McIver and Carroll Morgan

Components in Probabilistic Systems: Suitable by Construction 240
Christel Baier, Clemens Dubslaff, Holger Hermanns, Michaela Klauck, Sascha Klüppelholz, and Maximilian A. Köhl

Behavioral Specification Theories: An Algebraic Taxonomy. 262
Uli Fahrenberg and Axel Legay

Approximating Euclidean by Imprecise Markov Decision Processes 275
Manfred Jaeger, Giorgio Bacci, Giovanni Bacci, Kim Guldstrand Larsen, and Peter Gjøl Jensen

Shield Synthesis for Reinforcement Learning 290
Bettina Könighofer, Florian Lorber, Nils Jansen, and Roderick Bloem

Inferring Performance from Code: A Review 307
Emilio Incerto, Annalisa Napolitano, and Mirco Tribastone

30 Years of Statistical Model Checking!

30 Years of Statistical Model Checking 325
Kim G. Larsen and Axel Legay

Statistical Model Checking: Black or White? 331
Pranav Ashok, Przemysław Daca, Jan Křetínský, and Maximilian Weininger

Probabilistic Mission Planning and Analysis for Multi-agent Systems 350
Rong Gu, Eduard Enoiu, Cristina Seceleanu, and Kristina Lundqvist

30 Years of Simulation-Based Quantitative Analysis Tools: A Comparison Experiment Between Möbius and Uppaal SMC. 368
Davide Basile, Maurice H. ter Beek, Felicita Di Giandomenico, Alessandro Fantechi, Stefania Gnesi, and Giorgio O. Spagnolo

Fluid Model-Checking in UPPAAL for Covid-19 385
Peter G. Jensen, Kenneth Y. Jørgensen, Kim G. Larsen, Marius Mikučionis, Marco Muñiz, and Danny B. Poulsen

Improving Secure and Robust Patient Service Delivery 404
Eduard Baranov, Thomas Given-Wilson, and Axel Legay

Verification and Validation of Concurrent and Distributed Systems

Verification and Validation of Concurrent and Distributed Systems (Track Summary) 421
Marieke Huisman and Cristina Seceleanu

Step-Wise Development of Provably Correct Actor Systems 426
Bernhard K. Aichernig and Benedikt Maderbacher

Violation Witnesses and Result Validation for Multi-Threaded Programs: Implementation and Evaluation with CPAchecker 449
Dirk Beyer and Karlheinz Friedberger

Tendermint Blockchain Synchronization: Formal Specification and Model Checking 471
Sean Braithwaite, Ethan Buchman, Igor Konnov, Zarko Milosevic, Ilina Stoilkovska, Josef Widder, and Anca Zamfir

Safe Sessions of Channel Actions in Clojure: A Tour of the Discourje Project. 489
Ruben Hamers and Sung-Shik Jongmans

Modular Verification of Liveness Properties of the I/O Behavior of Imperative Programs 509
Bart Jacobs

Formal Verification of an Industrial Distributed Algorithm: An Experience Report 525
Nikolai Kosmatov, Delphine Longuet, and Romain Soulat

Deploying TESTAR to Enable Remote Testing in an Industrial CI Pipeline: A Case-Based Evaluation 543
Fernando Pastor Ricós, Pekka Aho, Tanja Vos, Ismael Torres Boigues, Ernesto Calás Blasco, and Héctor Martínez Martínez

A Formal Model of the Kubernetes Container Framework 558
Gianluca Turin, Andrea Borgarelli, Simone Donetti, Einar Broch Johnsen, Silvia Lizeth Tapia Tarifa, and Ferruccio Damiani

Author Index 579

Contents – Part II

Automating Software Re-Engineering

Automating Software Re-engineering: Introduction to the ISoLA 2020 Track . . . 3
Serge Demeyer, Reiner Hähnle, and Heiko Mantel

Formal Verification of Developer Tests: A Research Agenda Inspired by Mutation Testing . . . 9
Serge Demeyer, Ali Parsai, Sten Vercammen, Brent van Bladel, and Mehrdad Abdi

Modular Regression Verification for Reactive Systems . . . 25
Alexander Weigl, Mattias Ulbrich, and Daniel Lentzsch

Finding Idioms in Source Code Using Subtree Counting Techniques . . . 44
Dmitry Orlov

Parametric Timed Bisimulation . . . 55
Malte Lochau, Lars Luthmann, Hendrik Göttmann, and Isabelle Bacher

A Unifying Framework for Dynamic Monitoring and a Taxonomy of Optimizations . . . 72
Marie-Christine Jakobs and Heiko Mantel

Thirty-Seven Years of Relational Hoare Logic: Remarks on Its Principles and History . . . 93
David A. Naumann

Safer Parallelization . . . 117
Reiner Hähnle, Asmae Heydari Tabar, Arya Mazaheri, Mohammad Norouzi, Dominic Steinhöfel, and Felix Wolf

Refactoring and Active Object Languages . . . 138
Volker Stolz, Violet Ka I Pun, and Rohit Gheyi

Rigorous Engineering of Collective Adaptive Systems

Rigorous Engineering of Collective Adaptive Systems Introduction to the 3rd Track Edition . . . 161
Martin Wirsing, Rocco De Nicola, and Stefan Jähnichen

Composition of Component Models - A Key to Construct Big Systems . . . 171
Wolfgang Reisig

Degrees of Autonomy in Coordinating Collectives of Self-Driving Vehicles 189
Stefano Mariani and Franco Zambonelli

Engineering Semantic Self-composition of Services Through Tuple-Based Coordination. . . . 205
Ashley Caselli, Giovanni Ciatto, Giovanna Di Marzo Serugendo, and Andrea Omicini

A Dynamic Logic for Systems with Predicate-Based Communication 224
Rolf Hennicker and Martin Wirsing

Abstractions for Collective Adaptive Systems 243
Omar Inverso, Catia Trubiani, and Emilio Tuosto

Verifying AbC Specifications via Emulation. . . . 261
Rocco De Nicola, Tan Duong, and Omar Inverso

Adaptive Security Policies 280
Flemming Nielson, René Rydhof Hansen, and Hanne Riis Nielson

Capturing Dynamicity and Uncertainty in Security and Trust via Situational Patterns 295
Tomas Bures, Petr Hnetynka, Robert Heinrich, Stephan Seifermann, and Maximilian Walter

Guaranteeing Type Consistency in Collective Adaptive Systems 311
Jonas Schürmann, Tim Tegeler, and Bernhard Steffen

Epistemic Logic in Ensemble Specification. . . . 329
Jan Sürmeli

FScaFi : A Core Calculus for Collective Adaptive Systems Programming . . . 344
Roberto Casadei, Mirko Viroli, Giorgio Audrito, and Ferruccio Damiani

Writing Robotics Applications with X-Klaim 361
Lorenzo Bettini, Khalid Bourr, Rosario Pugliese, and Francesco Tiezzi

Measuring Adaptability and Reliability of Large Scale Systems 380
Valentina Castiglioni, Michele Loreti, and Simone Tini

Centrality-Preserving Exact Reductions of Multi-Layer Networks 397
Tatjana Petrov and Stefano Tognazzi

Towards Dynamic Dependable Systems Through Evidence-Based Continuous Certification 416
Rasha Faqeh, Christof Fetzer, Holger Hermanns, Jörg Hoffmann, Michaela Klauck, Maximilian A. Köhl, Marcel Steinmetz, and Christoph Weidenbach

Forming Ensembles at Runtime: A Machine Learning Approach 440
Tomáš Bureš, Ilias Gerostathopoulos, Petr Hnětynka, and Jan Pacovský

Synthesizing Control for a System with Black Box Environment, Based on Deep Learning 457
Simon Iosti, Doron Peled, Khen Aharon, Saddek Bensalem, and Yoav Goldberg

A Formal Model for Reasoning About the Ideal Fitness in Evolutionary Processes 473
Thomas Gabor and Claudia Linnhoff-Popien

A Case Study of Policy Synthesis for Swarm Robotics 491
Paul Piho and Jane Hillston

Maple-Swarm: Programming Collective Behavior for Ensembles by Extending HTN-Planning. 507
Oliver Kosak, Lukas Huhn, Felix Bohn, Constantin Wanninger, Alwin Hoffmann, and Wolfgang Reif

Swarm and Collective Capabilities for Multipotent Robot Ensembles. 525
Oliver Kosak, Felix Bohn, Lennart Eing, Dennis Rall, Constantin Wanninger, Alwin Hoffmann, and Wolfgang Reif

Author Index 541

Contents – Part III

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

Reliable Smart Contracts 3
Gordon J. Pace, César Sánchez, and Gerardo Schneider

Functional Verification of Smart Contracts via Strong Data Integrity 9
Wolfgang Ahrendt and Richard Bubel

Bitcoin Covenants Unchained 25
Massimo Bartoletti, Stefano Lande, and Roberto Zunino

Specifying Framing Conditions for Smart Contracts. 43
Bernhard Beckert and Jonas Schiffl

Making Tezos Smart Contracts More Reliable with Coq 60
Bruno Bernardo, Raphaël Cauderlier, Guillaume Claret, Arvid Jakobsson, Basile Pesin, and Julien Tesson

UTxO- vs Account-Based Smart Contract Blockchain Programming Paradigms 73
Lars Brünjes and Murdoch J. Gabbay

Native Custom Tokens in the Extended UTXO Model. 89
Manuel M. T. Chakravarty, James Chapman, Kenneth MacKenzie, Orestis Melkonian, Jann Müller, Michael Peyton Jones, Polina Vinogradova, and Philip Wadler

UTXO$_{\mathrm{ma}}$: UTXO with Multi-asset Support. 112
Manuel M. T. Chakravarty, James Chapman, Kenneth MacKenzie, Orestis Melkonian, Jann Müller, Michael Peyton Jones, Polina Vinogradova, Philip Wadler, and Joachim Zahnentferner

Towards Configurable and Efficient Runtime Verification of Blockchain Based Smart Contracts at the Virtual Machine Level 131
Joshua Ellul

Compiling Quantitative Type Theory to Michelson for Compile-Time Verification and Run-time Efficiency in Juvix. 146
Christopher Goes

Efficient Static Analysis of Marlowe Contracts 161
Pablo Lamela Seijas, David Smith, and Simon Thompson

Accurate Smart Contract Verification Through Direct Modelling 178
Matteo Marescotti, Rodrigo Otoni, Leonardo Alt, Patrick Eugster, Antti E. J. Hyvärinen, and Natasha Sharygina

Smart Derivatives: On-Chain Forwards for Digital Assets 195
Alfonso D. D. M. Rius and Eamonn Gashier

The Good, The Bad and The Ugly: Pitfalls and Best Practices in Automated Sound Static Analysis of Ethereum Smart Contracts 212
Clara Schneidewind, Markus Scherer, and Matteo Maffei

Automated Verification of Embedded Control Software

Automated Verification of Embedded Control Software: Track Introduction 235
Dilian Gurov, Paula Herber, and Ina Schaefer

A Model-Based Approach to the Design, Verification and Deployment of Railway Interlocking System 240
Arturo Amendola, Anna Becchi, Roberto Cavada, Alessandro Cimatti, Alberto Griggio, Giuseppe Scaglione, Angelo Susi, Alberto Tacchella, and Matteo Tessi

Guess What I'm Doing!: Rendering Formal Verification Methods Ripe for the Era of Interacting Intelligent Systems 255
Martin Fränzle and Paul Kröger

On the Industrial Application of Critical Software Verification with VerCors 273
Marieke Huisman and Raúl E. Monti

A Concept of Scenario Space Exploration with Criticality Coverage Guarantees: Extended Abstract 293
Hardi Hungar

Towards Automated Service-Oriented Verification of Embedded Control Software Modeled in Simulink 307
Timm Liebrenz, Paula Herber, and Sabine Glesner

Verifying Safety Properties of Robotic Plans Operating in Real-World Environments via Logic-Based Environment Modeling 326
Tim Meywerk, Marcel Walter, Vladimir Herdt, Jan Kleinekathöfer, Daniel Große, and Rolf Drechsler

Formally Proving Compositionality in Industrial Systems with Informal Specifications 348
Mattias Nyberg, Jonas Westman, and Dilian Gurov

Specification, Synthesis and Validation of Strategies for Collaborative Embedded Systems 366
Bernd-Holger Schlingloff

Formal methods for DIStributed COmputing in future RAILway systems

Formal Methods for Distributed Computing in Future Railway Systems. 389
Alessandro Fantechi, Stefania Gnesi, and Anne E. Haxthausen

Ensuring Safety with System Level Formal Modelling. 393
Thierry Lecomte, Mathieu Comptier, Julien Molinero, and Denis Sabatier

A Modular Design Framework to Assess Intelligent Trains. 404
Simon Collart-Dutilleul and Philippe Bon

Formal Modelling and Verification of a Distributed Railway Interlocking System Using UPPAAL. 415
Per Lange Laursen, Van Anh Thi Trinh, and Anne E. Haxthausen

New Distribution Paradigms for Railway Interlocking 434
Jan Peleska

Model Checking a Distributed Interlocking System Using *k*-induction with RT-Tester 449
Signe Geisler and Anne E. Haxthausen

Designing a Demonstrator of Formal Methods for Railways Infrastructure Managers 467
Davide Basile, Maurice H. ter Beek, Alessandro Fantechi, Alessio Ferrari, Stefania Gnesi, Laura Masullo, Franco Mazzanti, Andrea Piattino, and Daniele Trentini

Author Index 487