

## 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 subseries at <http://www.springer.com/series/7407>


Tiziana Margaria · Bernhard Steffen (Eds.)

# Leveraging Applications of Formal Methods, Verification and Validation

10th International Symposium  
on Leveraging Applications of Formal Methods, ISO/LA 2021  
Rhodes, Greece, October 17–29, 2021  
Proceedings

### *Editors*

Tiziana Margaria   
University of Limerick  
Limerick, Ireland

Bernhard Steffen   
TU Dortmund  
Dortmund, Germany

Lero  
Limerick, Ireland

ISSN 0302-9743                      ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-030-89158-9              ISBN 978-3-030-89159-6 (eBook)  
<https://doi.org/10.1007/978-3-030-89159-6>

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

© Springer Nature Switzerland AG 2021

Chapters “DSLs and Middleware Platforms in a Model-Driven Development Approach for Secure Predictive Maintenance Systems in Smart Factories” and “The Interoperability Challenge: Building a Model-driven Digital Thread Platform for CPS” 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

As Symposium and Program Chairs we would like to welcome you to the proceedings of ISO<sub>LA</sub> 2021, the 10th International Symposium on Leveraging Applications of Formal Methods, Verification and Validation which was planned to take place in Rhodes (Greece) during October 17–29, 2021, and endorsed by EASST, the European Association of Software Science and Technology.

This year's event was very special due to the very special circumstances. It comprised most of the contributions that were submitted to ISO<sub>LA</sub> 2020, only a few of which were presented last year in a remote fashion. ISO<sub>LA</sub> was planned to take place in October 2021 in a hybrid fashion, now comprising also the contributions contained in this volume. Only one track was postponed for yet another year, and we hoped very much to experience the other tracks in Rhodes.

As in the previous editions, ISO<sub>LA</sub> 2021 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, since 2004 the ISO<sub>LA</sub> series of events has served 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, ISO<sub>LA</sub> 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 ISO<sub>LA</sub> 2021 consisted of a collection of special tracks devoted to the following hot and emerging topics:

- 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 Seculeanu, 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)

- 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 Hermanns, 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)

It also included two embedded events:

- Doctoral Symposium and Poster Session (A.-L. Lamprecht)
- Industrial Day (Falk Howar, Johannes Neubauer, Andreas Rausch)

Co-located with ISO LA 2021 was:

- [STRESS 2021 – 5th International School on Tool-based Rigorous Engineering of Software Systems](#) (J. Hatcliff, T. Margaria, Robby, B. Steffen)

Altogether ISO LA 2021 comprised contributions from the proceedings originally foreseen for ISO LA 2020 collected in four volumes, Part 1: Verification Principles, Part 2: Engineering Principles, Part 3: Applications, and Part 4: Tools and Trends, and the content of these proceedings which also cover contributions of 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 Easy Conferences team for their continuous precious support during the entire two-year period preceding the events, and Springer-Verlag for being, as usual, a very reliable partner for the proceedings production. Finally, we are grateful to Christos Therapontos for his continuous support for the Web site 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 organizations 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.

We hope that you, as an ISO LA participant, had a wonderful experience at this edition, and that those of you reading the proceedings at a later date gain valuable new insights that hopefully contribute to your research and its uptake.

Tiziana Margaria  
Bernhard Steffen

# Organization

## Symposium Chair

Margaria, Tiziana

University of Limerick and Lero, Ireland

## Program Committee Chair

Steffen, Bernhard

TU Dortmund, Germany

## Program Committee

Beyer, Dirk

LMU Munich, Germany

Bojanova, Irena

National Institute of Standards and Technology, USA

Fantechi, Alessandro

Università degli Studi di Firenze, Italy

Gnesi, Stefania

ISTI-CNR, Italy

Hatcliff, John

Kansas State University, USA

Havelund, Klaus

Jet Propulsion Laboratory, USA

Howar, Falk

TU Dortmund, Germany

Margaria, Tiziana

University of Limerick and Lero, Ireland

Robby

Kansas State University, USA

Schordan, Markus

Lawrence Livermore National Laboratories, USA

Steffen, Bernhard

TU Dortmund, Germany

Wirsing, Martin

LMU Munich, Germany

# Contents

## 6th International School on Tool-Based Rigorous Engineering of Software Systems

An Introduction to Graphical Modeling of CI/CD Workflows with Rig . . . . .	3
<i>Tim Tegeler, Sebastian Teumert, Jonas Schürmann, Alexander Bainczyk, Daniel Busch, and Bernhard Steffen</i>	
Pyrus: An Online Modeling Environment for No-Code Data-Analytics Service Composition . . . . .	18
<i>Philip Zweihoff and Bernhard Steffen</i>	
Integrating External Services in DIME. . . . .	41
<i>Hafiz Ahmad Awais Chaudhary and Tiziana Margaria</i>	
Asking Why. . . . .	55
<i>Barbara Steffen and Bernhard Steffen</i>	

## Industrial Track

Formal Methods for a Digital Industry: Industrial Day at ISoLA 2021 . . . . .	71
<i>Falk Howar, Hardi Hungar, and Andreas Rausch</i>	
Agile Business Engineering: From Transformation Towards Continuous Innovation . . . . .	77
<i>Barbara Steffen, Falk Howar, Tim Tegeler, and Bernhard Steffen</i>	
Towards Living Canvases . . . . .	95
<i>Barbara Steffen, Frederik Möller, Alex Rotgang, Stephen Ryan, and Tiziana Margaria</i>	
Use Cases for Simulation in the Development of Automated Driving Systems . . . . .	117
<i>Hardi Hungar</i>	
Simulation-Based Elicitation of Accuracy Requirements for the Environmental Perception of Autonomous Vehicles. . . . .	129
<i>Robin Philipp, Hedan Qian, Lukas Hartjen, Fabian Schuldt, and Falk Howar</i>	
DSLs and Middleware Platforms in a Model-Driven Development Approach for Secure Predictive Maintenance Systems in Smart Factories. . . .	146
<i>Jobish John, Amrita Ghosal, Tiziana Margaria, and Dirk Pesch</i>	



From Requirements to Executable Rules: An Ensemble of Domain-Specific Languages for Programming Cyber-Physical Systems in Warehouse Logistics . . . . .	162
<i>Malte Mauritz and Moritz Roidl</i>	
Mining Data Quality Rules for Data Migrations: A Case Study on Material Master Data . . . . .	178
<i>Marcel Altendeitering</i>	
<b>Programming: What is Next</b>	
Programming - What is Next? . . . . .	195
<i>Klaus Havelund and Bernhard Steffen</i>	
Low-Code Is Often High-Code, So We Must Design Low-Code Platforms to Enable Proper Software Engineering . . . . .	202
<i>Timothy C. Lethbridge</i>	
Time for All Programs, Not Just Real-Time Programs . . . . .	213
<i>Edward A. Lee and Marten Lohstroh</i>	
Integrated Modeling and Development of Component-Based Embedded Software in Scala . . . . .	233
<i>Klaus Havelund and Robert Bocchino</i>	
Slang: The Sireum Programming Language . . . . .	253
<i>Robby and John Hatcliff</i>	
HAMR: An AADL Multi-platform Code Generation Toolset . . . . .	274
<i>John Hatcliff, Jason Belt, Robby, and Todd Carpenter</i>	
Fundamental Constructs in Programming Languages . . . . .	296
<i>Peter D. Mosses</i>	
Introducing Dynamical Systems and Chaos Early in Computer Science and Software Engineering Education Can Help Advance Theory and Practice of Software Development and Computing . . . . .	322
<i>David Harel and Assaf Marron</i>	
GATE: Gradual Effect Types . . . . .	335
<i>Philip Wadler</i>	
Fixing Classification: A Viewpoint-Based Approach . . . . .	346
<i>Bran Selić and Alfonso Pierantonio</i>	
The Future of Programming and Modelling: A Vision . . . . .	357
<i>Perdita Stevens</i>	

<b>Towards Model-Based Intent-Driven Adaptive Software. . . . .</b>	<b>378</b>
<i>Daniel Balasubramanian, Alessandro Coglio, Abhishek Dubey, and Gabor Karsai</i>	
<b>The Interoperability Challenge: Building a Model-Driven Digital Thread Platform for CPS . . . . .</b>	<b>393</b>
<i>Tiziana Margaria, Hafiz Ahmad Awais Chaudhary, Ivan Guevara, Stephen Ryan, and Alexander Schieweck</i>	
<b>Programming vs. That Thing Subject Matter Experts Do . . . . .</b>	<b>414</b>
<i>Markus Voelter</i>	
<b>Aligned, Purpose-Driven Cooperation: The Future Way of System Development . . . . .</b>	<b>426</b>
<i>Philip Zweihoff, Tim Tegeler, Jonas Schürmann, Alexander Bainczyk, and Bernhard Steffen</i>	
<b>Software Verification Tools</b>	
<b>sVerify: Verifying Smart Contracts Through Lazy Annotation and Learning . . . . .</b>	<b>453</b>
<i>Bo Gao, Ling Shi, Jiaying Li, Jialiang Chang, Jun Sun, and Zijiang Yang</i>	
<b>Rigorous Engineering of Collective Adaptive Systems</b>	
<b>Verifying Temporal Properties of Stigmergic Collective Systems Using CADP . . . . .</b>	<b>473</b>
<i>Luca Di Stefano and Frédéric Lang</i>	
<b>Formal Methods for DIStributed COmputing in Future RAILway Systems</b>	
<b>RAILS: Roadmaps for AI integration in the rail Sector. . . . .</b>	<b>493</b>
<i>Francesco Flammini and Valeria Vittorini</i>	
<b>A Journey Through Software Model Checking of Interlocking Programs . . . .</b>	<b>495</b>
<i>Simon Chadwick, Phillip James, Faron Moller, Markus Roggenbach, and Thomas Werner</i>	
<b>Supporting the Development of Hybrid ERTMS/ETCS Level 3 with Formal Modelling, Analysis and Simulation . . . . .</b>	<b>498</b>
<i>Maarten Bartholomeus, Rick Erkens, Bas Luttik, and Tim Willemse</i>	

Formal Methods in Railway Signalling Infrastructure  
Standardisation Processes . . . . . 500  
    *Mark Bouwman, Bas Luttik, Arend Rensink, Mariëlle Stoelinga,  
    and Djurre van der Wal*

**Author Index . . . . . 503**