

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

Moti Yung 

Columbia University, New York, NY, USA

More information about this series at <https://link.springer.com/bookseries/558>


Jan Friso Groote · Marieke Huisman (Eds.)

Formal Methods for Industrial Critical Systems

27th International Conference, FMICS 2022
Warsaw, Poland, September 14–15, 2022
Proceedings

Editors

Jan Friso Groote 
Eindhoven University of Technology
Eindhoven, The Netherlands

Marieke Huisman 
University of Twente
Enschede, The Netherlands

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-031-15007-4 ISBN 978-3-031-15008-1 (eBook)
<https://doi.org/10.1007/978-3-031-15008-1>

© The Editor(s) (if applicable) and The Author(s), under exclusive license
to Springer Nature Switzerland AG 2022

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

Preface

The International Conference on Formal Methods in Industrial Critical Systems (FMICS), organized by ERCIM, is the key conference at the intersection of industrial applications and formal methods. The aim of the FMICS series is to provide a forum for researchers who are interested in the development and application of formal methods in industry. FMICS brings together scientists and engineers who are active in the area of formal methods and interested in exchanging their experiences in the industrial usage of these methods. FMICS also strives to promote research and development for the improvement of formal methods and tools for industrial applications.

This volume contains the papers presented at the 27th International Conference on Formal Methods in Industrial Critical Systems (FMICS 2022), which was held during September 14–15, 2022. The symposium took place in the beautiful capital of Poland, Warsaw, but could also be attended online. The conference was organized under the umbrella of CONFEST, alongside with the 33rd International Conference on Concurrency Theory (CONCUR 2022), the 19th International Conference on Quantitative Evaluation of Systems (QEST 2022), and the 20th International Conference on Formal Modeling and Analysis of Timed Systems (FORMATS 2022).

FMICS 2022 received 22 paper submissions. We selected a total of 13 papers for presentation during the conference and inclusion in these proceedings, resulting in an overall acceptance rate of 59%.

The submissions were reviewed by an international Program Committee (PC) of 28 members from a mix of universities, industry, and research institutes. All submissions went through a rigorous single-blind review process overseen by the Program Committee Chairs. Each submission received three review reports and was actively and thoroughly discussed by the PC.

The program of CONFEST 2022 included two FMICS invited keynotes. One by Sven Schewe from Liverpool University about reinforcement learning with guarantees, and one by Bas Luttik from Eindhoven University of Technology about railway innovations via formal modeling and verification.

We are grateful to all involved in FMICS 2022. We thank the authors for submitting and presenting their work at FMICS 2022 and the PC members and sub-reviewers for their accurate and timely reviewing. We also thank the invited speakers, session chairs, and attendees, all of whom contributed to making the conference a success. We are also grateful to the providers of the EasyChair system, which was used to manage the submissions, to Springer for sponsoring the Best Paper Award and for publishing the proceedings, and to the Steering Committee of FMICS for their trust and support. We thank the General Chair of CONFEST, Sławek Lasota, for providing the logistics that enabled and facilitated the organization of FMICS 2022.

July 2022

Jan Friso Groote
Marieke Huisman

Organization

Program Committee

Erika Ábrahám	RWTH Aachen University, Germany
Maurice ter Beek	ISTI-CNR, Italy
Simon Bliudze	Inria, France
Rafael C. Cardoso	University of Aberdeen, UK
Milan Česka	Brno University of Technology, Czech Republic
Hubert Garavel	Inria, France
Jan Friso Groote (Chair)	Eindhoven University of Technology, The Netherlands
Ernst Moritz Hahn	University of Twente, The Netherlands
Paula Herber	University of Münster, Germany
Marieke Huisman (Chair)	University of Twente, The Netherlands
Peter Höfner	Australian National University, Australia
Nikolai Kosmatov	CEA List, Université Paris-Saclay and Thales, France
Alfons Laarman	Leiden University, The Netherlands
Peter Gorm Larsen	Aarhus University, Denmark
István Majzik	Budapest University of Technology and Economics, Hungary
Rosemary Monahan	Maynooth University, Ireland
Thomas Neele	Eindhoven University of Technology, The Netherlands
Wytse Oortwijn	TNO-ESI, The Netherlands
Paweł Parys	University of Warsaw, Poland
Wojciech Penczek	Institute of Computer Science, Polish Academy of Sciences, Poland
Jaco van de Pol	Aarhus University, Denmark
Marco Roveri	University of Trento, Italy
Kristin Yvonne Rozier	Iowa State University, USA
Cristina Seceleanu	Mälardalen University, Sweden
Martina Seidl	Johannes Kepler University Linz, Austria
Jiri Srba	Aalborg University, Denmark
Alexander J. Summers	University of British Columbia, Canada
Ashutosh Trivedi	University of Colorado Boulder, USA
Elena Troubitsyna	KTH, Sweden
Naijun Zhan	Institute of Software, Chinese Academy of Sciences, China

Additional Reviewers

Backeman, Peter

Franken, Tom

Gora, Paweł

Grosen, Thomas Møller

Iwanicki, Konrad

Jin, Xiangyu

Kurkowski, Mirosław

Longuet, Delphine

Oda, Tomohiro

Schubert, Aleksy

Sidoruk, Teofil

Szekeres, Dániel

Wang, Qiang

Xu, Runqing

Contents

Invited Keynote Talks

- Reinforcement Learning with Guarantees that Hold for Ever 3
*Ernst Moritz Hahn, Mateo Perez, Sven Schewe, Fabio Somenzi,
Ashutosh Trivedi, and Dominik Wojtczak*
- Supporting Railway Innovations with Formal Modelling and Verification 8
Bas Luttik

Certification

- Formal Monotony Analysis of Neural Networks with Mixed Inputs:
An Asset for Certification 15
*Guillaume Vidot, Mélanie Ducoffe, Christophe Gabreau, Ileana Ober,
and Iulian Ober*
- Generating Domain-Specific Interactive Validation Documents 32
Fabian Vu, Christopher Happe, and Michael Leuschel
- Deductive Verification of Smart Contracts with Dafny 50
Franck Cassez, Joanne Fuller, and Horacio Mijail Antón Quiles

Industrial Use Cases

- Towards Reusable Formal Models for Custom Real-Time Operating
Systems 69
Julius Adelt, Julian Gebker, and Paula Herber
- Formal Verification of an Industrial UML-like Model using mCRL2 86
Anna Stramaglia and Jeroen J. A. Keiren
- Chemical Case Studies in KeYmaera X 103
Rose Bohrer
- Analysing Capacity Bottlenecks in Rail Infrastructure by Episode Mining 121
*Philipp Berger, Wiebke Lenze, Thomas Noll, Simon Schotten,
Thorsten Büker, Mario Fietze, and Bastian Kogel*

Testing and Monitoring

Test Suite Augmentation for Reconfigurable PLC Software in the Internet
of Production 137
Marco Grochowski, Marcus Völker, and Stefan Kowalewski

Monitoring of Spatio-Temporal Properties with Nonlinear SAT Solvers 155
*André de Matos Pedro, Tomás Silva, Tiago Sequeira, João Lourenço,
João Costa Seco, and Carla Ferreira*

Model-Based Testing of Internet of Things Protocols 172
Xavier Manuel van Dommelen, Machiel van der Bijl, and Andy Pimentel

Methodology

Formally Verifying Decompositions of Stochastic Specifications 193
Anton Hampus and Mattias Nyberg

Verification of Behavior Trees using Linear Constrained Horn Clauses 211
*Thomas Henn, Marcus Völker, Stefan Kowalewski, Minh Trinh,
Oliver Petrovic, and Christian Brecher*

A Multi-level Methodology for Behavioral Comparison
of Software-Intensive Systems 226
Dennis Hendriks, Arjan van der Meer, and Wytse Oortwijn

Author Index 245