Lecture Notes in Computer Science **14300**

Founding Editors

Gerhard Goos
Juris Hartmanis

Editorial Board Members

Elisa Bertino, USA
Wen Gao, China
Bernhard Steffen, Germany
Moti Yung, USA

Formal Methods

Subline of Lecture Notes in Computer Science

Subline Series Editors

Ana Cavalcanti, *University of York, UK*
Marie-Claude Gaudel, *Université de Paris-Sud, France*

Subline Advisory Board

Manfred Broy, *TU Munich, Germany*
Annabelle McIver, *Macquarie University, Sydney, NSW, Australia*
Peter Müller, *ETH Zurich, Switzerland*
Erik de Vink, *Eindhoven University of Technology, The Netherlands*
Pamela Zave, *AT&T Laboratories Research, Bedminster, NJ, USA*

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

Paula Herber · Anton Wijs
Editors

iFM 2023

18th International Conference, iFM 2023
Leiden, The Netherlands, November 13–15, 2023
Proceedings

Springer

Editors
Paula Herber
Embedded Systems Group
University of Münster
Münster, Germany

Anton Wijs
Eindhoven University of Technology
Eindhoven, The Netherlands

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-031-47704-1 ISBN 978-3-031-47705-8 (eBook)
https://doi.org/10.1007/978-3-031-47705-8

© The Editor(s) (if applicable) and The Author(s), under exclusive license
to Springer Nature Switzerland AG 2024

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

Paper in this product is recyclable.

Preface

This volume contains the papers presented at the 18th International Conference on integrated Formal Methods (iFM 2023), held in the charming city of Leiden, The Netherlands, and hosted by the Leiden Institute of Advanced Computer Science of Leiden University. These proceedings also contain three papers selected by the Program Committee of the PhD Symposium (PhD-iFM 2023), chaired by Crystal Chang Din and Gidon Ernst.

In recent years, we have witnessed a proliferation of approaches that integrate several modeling, verification, and simulation techniques, facilitating more versatile and efficient analysis of software-intensive systems. These approaches provide powerful support for the analysis of different functional and non-functional properties of the systems, and the complex interaction of components of different natures, as well as validation of diverse aspects of system behavior. The iFM conference series is a forum for discussing recent research advances in the development of integrated approaches to formal modeling and analysis. The conference series covers all aspects of the design of integrated techniques, including language design, verification and validation, automated tool support, and the use of such techniques in software engineering practice.

The iFM 2023 conference solicited high-quality papers reporting research results and/or experience reports related to the overall theme of formal methods integration. The Program Committee (PC) received a total of 51 paper submissions from authors in 17 different countries: 43 regular papers and 8 short papers. All submissions were rigorously reviewed by three PC members, with the help of many external reviewers, after which the reviewers had a short but intense discussion. The decision to accept or reject a submission was based on both the review reports with their scores and the outcomes of these in-depth discussions.

Ultimately, the PC of iFM 2023 selected 18 papers for presentation during the conference and inclusion in these proceedings: 16 regular papers and 2 short papers. This amounts to an overall acceptance rate of 35.3% (37% for regular papers and 25% for short papers). The PC of PhD-iFM 2023 received 12 submissions and selected 7 submissions for presentation at the symposium and 3 of those submissions for inclusion in these proceedings.

This edition of iFM continued the use of the EAPLS artifact badging scheme, which was introduced at iFM 2022, to credit tool developers and stimulate reproducibility of the reported results. The Artifact Evaluation Committee, chaired by Anna-Lena Lamprecht and Muhammad Osama, received 8 submissions and intensively tested the quality of the artifacts. All artifacts achieved the available and the functional badges, while 6 artifacts additionally were awarded the reusable badge.

The iFM 2023 conference featured keynotes by the following speakers:

- Erika Ábrahám (RWTH Aachen University, Germany);
- Barbara Jobstmann (EPFL and Cadence Design Systems, Switzerland);
- K. Rustan M. Leino (Amazon Web Services, USA).

The first speaker was an invited speaker for both iFM 2023 and the colocated Fifth Workshop on Formal Methods for Autonomous Systems. We heartily thank these invited speakers for accepting our invitation and sharing their research results and views with the iFM 2023 audience.

We thank everybody involved in iFM 2023. First of all, all PC members and external reviewers for their in-depth and timely reviewing, all authors for submitting their work, and all attendees for participating. We also thank the chairs and committees for the Artifact Evaluation and the PhD Symposium, listed on the following pages, and the excellent local organization team, including the Publicity Chair Alfons Laarman and the General Chair Marcello M. Bonsangue.

We are very grateful to the organizations that sponsored iFM 2023, namely the Leiden Institute of Advanced Computer Science, Springer, and the European Association for Programming Languages and Systems (EAPLS).

Finally, we thank Springer for publishing these proceedings in their FM subline, and we gratefully acknowledge the support from EasyChair in assisting us in managing the complete process from submissions to the proceedings.

We hope you enjoyed the conference!

September 2023

Paula Herber
Anton Wijs

Organization

General Chair

Marcello M. Bonsangue	Leiden University, The Netherlands

Program Committee Chairs

Paula Herber	University of Münster, Germany
Anton Wijs	Eindhoven University of Technology, The Netherlands

Publicity Chair

Alfons Laarman	Leiden University, The Netherlands

Artifact Evaluation Committee Chairs

Anna-Lena Lamprecht	University of Potsdam, Germany
Muhammad Osama	Eindhoven University of Technology, The Netherlands

PhD Symposium Chairs

Crystal Chang Din	University of Bergen, Norway
Gidon Ernst	Ludwig Maximilian University of Munich, Germany

Steering Committee

Erika Ábrahám	RWTH Aachen University, Germany
Wolfgang Ahrendt	Chalmers University of Technology, Sweden
Ferruccio Damiani	University of Turin, Italy
John Derrick	University of Sheffield, UK
Carlo A. Furia	Università della Svizzera italiana, Switzerland
Marieke Huisman	University of Twente, The Netherlands
Einar Broch Johnsen	University of Oslo, Norway
Luigia Petre	Åbo Akademi University, Finland
Nadia Polikarpova	University of California, USA
Steve Schneider	University of Surrey, UK
Emil Sekerinski	McMaster University, Canada
Silvia Lizeth Tapia Tarifa	University of Oslo, Norway
Helen Treharne	University of Surrey, UK
Heike Wehrheim	University of Oldenburg, Germany
Kirsten Winter	University of Queensland, Australia

Program Committee

Wolfgang Ahrendt	Chalmers University of Technology, Sweden
Maurice ter Beek	ISTI-CNR, Italy
Petra van den Bos	University of Twente, The Netherlands
Alessandro Cimatti	Fondazione Bruno Kessler, Italy
Pedro R. D'Argenio	Universidad Nacional de Córdoba, Argentina
Richard DeFrancisco	Augusta University, USA
John Derrick	University of Sheffield, UK
Claire Dross	AdaCore, France
Karine Even-Mendoza	King's College London, UK
Marie Farrell	University of Manchester, UK
Carlo A. Furia	Università della Svizzera Italiana, Italy
Dilian Gurov	KTH Royal Institute of Technology, Sweden
Marieke Huisman	University of Twente, The Netherlands
Einar Broch Johnsen	University of Oslo, Norway
Sebastian Junges	Radboud University, The Netherlands
Nikolai Kosmatov	CEA List, France
Alfons Laarman	Leiden University, The Netherlands
Martin Leucker	University of Lübeck, Germany
Rosemary Monahan	Maynooth University, Ireland
Thomas Neele	Eindhoven University of Technology, The Netherlands
Wytse Oortwijn	TNO, The Netherlands
Jun Pang	University of Luxembourg, Luxembourg
Luigia Petre	Åbo Akademi University, Finland
Giles Reger	Amazon Web Services and University of Manchester, UK
Anne Remke	University of Münster, Germany
David Šafránek	Masaryk University, Czech Republic
Thomas Santen	Formal Assurance, Germany
Ina Schäfer	Karlsruhe Institute of Technology, Germany
Ana Sokolova	University of Salzburg, Austria
Silvia Lizeth Tapia Tarifa	University of Oslo, Norway
Heike Wehrheim	University of Oldenburg, Germany
Kirsten Winter	University of Queensland, Australia
Naijun Zhan	Institute of Software, Chinese Academy of Sciences, China

Artifact Evaluation Committee

Sharar Ahmadi	University of Surrey, UK
Davide Basile	ISTI-CNR, Italy
César Cornejo	Universidad Nacional de Rio Cuarto, Argentina
Mathias Fleury	University of Freiburg, Germany
Mario Frank	University of Potsdam, Germany
Lars B. van den Haak	Eindhoven University of Technology, The Netherlands

Emilio Incerto	IMT School for Advanced Studies Lucca, Italy
Maurice Laveaux	Eindhoven University of Technology, The Netherlands
Yong Li	Institute of Software, Chinese Academy of Sciences, China
Anik Momtaz	Michigan State University, USA
Andres Noetzli	Cubist, Inc., USA
Danilo Pianini	University of Bologna, Italy
Cedric Richter	Carl von Ossietzky University of Oldenburg, Germany
Mouhammad Sakr	University of Luxembourg, Luxembourg
Dimitrios Thanos	Leiden University, The Netherlands

PhD Symposium Program Committee

Elvira Albert	Complutense University of Madrid, Spain
Eduard Kamburjan	University of Oslo, Norway
Ondrej Lengal	Brno University of Information Technology, Czech Republic
Anna Lukina	Technical University of Delft, The Netherlands
Andrei Paskevich	Paris-Saclay University, France
Chris Poskitt	Singapore Management University, Singapore
José Proença	CISTER Lab, ISEP, Portugal
Elvinia Riccobene	Università degli Studi di Milano, Italy
Dominic Steinhöfel	CISPA Helmholtz Center for Information Security, Germany

Additional Reviewers

Yehia Abd Alrahman
Jesper Amilon
Luís Soares Barbosa
Lara Bargmann
Davide Basile
Lukas Birkemeyer
Sandrine Blazy
Giovanna Broccia
Zhenbang Chen
Tim Coopmans
Joanna Delicaris
Ramiro Demasi
Luca Di Stefano
Adel Djoudi
Catherine Dubois
Tom Franken
Alistair Finn Hackett
Jan Haltermann
Nils Jansen
Hannes Kallwies
Eduard Kamburjan
Karam Kharraz
Paul Kobialka
Thierry Lecomte
Christian Lidström
Frédéric Loulergue
Guillaume Melquiond
Mathis Niehage
Federico Olmedo
Anurudh Peduri
Cedric Richter
Tobias Runge

Martin Sachenbacher
Rudolf Schlatte
Samuel Teuber
Nicola Thoben
Daniel Thoma
Marck van der Vegt
Shuling Wang
Xiong Xu
Lina Ye
Hengjun Zhao

Sponsors

Leiden Institute of Advanced Computer Science (LIACS)

European Association for Programming Languages and Systems (EAPLS)

Springer

Abstract of Invited Talks

Formal Signoff Flows

Barbara Jobstmann

EPFL and Cadence Design Systems, Switzerland
barbara.jobstmann@epfl.ch

Abstract. Verification sign-off flows aims to answer the question of when to stop the verification effort, i.e., when the design is good enough for tape-out (manufacturing). Classical functional verification sign-off flows are based on simulation coverage metrics, which allow one to track the performed verification effort. With the rise of formal verification in industry, formal verification sign-off flows are becoming more and more critical. In this talk, we will first discuss coverage models and metrics used in formal verification in the industry. These metrics allow analysis of a verification setup from two different angles: (1) From a controllability angle, to answer questions like does the verification setup exercise all parts of the design? Did I over-constrain my design? (2) From the observability angle, to know if the set of checks is sufficient to catch potential faults in the design. To be meaningful, the metrics need to be tailored to a design. Therefore, we will next discuss methods to ensure coverage is measured in the context of design-specific scenarios. Finally, we will discuss dedicated techniques like bound aggregation and bug hunting to increase the coverage numbers.

Industrial Experience with a Verification-Aware Programming Language

K. Rustan M. Leino

Amazon Web Services, USA
leino@amazon.com

Abstract. The programming language Dafny was designed to support specifications and formal verification in a modern software-engineering setting. As a language, it blends imperative and functional features with specifications and proof authoring. The Dafny ecosystem includes not just compilers, but also, conspicuously, an automated program verifier. Following a decade of use in teaching and in research projects, the language and its verifier now also have several years of industrial use. In this talk, I reflect on some of the lessons learned from working with engineers to write and maintain verified software and how this has impacted the language and its tooling.

Contents

Hardware and Memory Verification

Verification and Learning

Temporal Logics

Autonomous Systems