Formal Methods

LNCS 13550

Bernd-Holger Schlingloff
Ming Chai (Eds.)

Software Engineering and Formal Methods

20th International Conference, SEFM 2022
Berlin, Germany, September 26–30, 2022
Proceedings

Springer

Lecture Notes in Computer Science 13550

Formal Methods

Subline of Lectures Notes in Computer Science

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

Bernd-Holger Schlingloff ·
Ming Chai (Eds.)

Software Engineering and Formal Methods

20th International Conference, SEFM 2022
Berlin, Germany, September 26–30, 2022
Proceedings

Springer

Editors

Bernd-Holger Schlingloff
Humboldt-Universität zu Berlin
Berlin, Germany

Ming Chai
Beijing Jiaotong University
Beijing, China

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-031-17107-9 ISBN 978-3-031-17108-6 (eBook)
https://doi.org/10.1007/978-3-031-17108-6

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

This volume contains the papers accepted for SEFM 2022, the 20th International Conference on Software Engineering and Formal Methods, held in Berlin, Germany, during September 28–30, 2022.

The SEFM conference series aims to bring together researchers and practitioners from academia, industry, and government to advance the state of the art in formal methods, to facilitate their uptake in the software industry, and to encourage their integration within practical software engineering methods and tools. This year marks the 20th anniversary of the series. Within these 20 years, the field has matured and extended focus: whereas in the 1st edition, which was held in 2003 in Brisbane, topics like verification, testing, object-oriented modeling, and integration of formal and informal methods prevailed, today additional topics like verification of machine learning, program synthesis from formal specifications, and correctness of cyber-physical and multi-agent systems have been added to the range. To reflect this extension, special emphasis was placed on the topic of "Software Engineering and Formal Methods for Intelligent and Learning Systems" at SEFM 2022.

SEFM 2022 was jointly organized by the Institute of Computer Science of the Humboldt University of Berlin (Germany) and the School of Electronic and Information Engineering of Beijing Jiaotong University (China). We also kindly acknowledge the support of Fraunhofer FOKUS, the Fraunhofer Institute for Open Communication Systems, Berlin. Following the online editions of SEFM in 2020 and 2021, it was the general opinion that we should have a physical face-to-face meeting again. Nevertheless, talks were streamed to an open website to allow online participation of a worldwide audience.

There were three invited talks at SEFM 2022: Uwe Nestmann (Technische Universität Berlin, Germany) reported on "Distributed process calculi with local states"; Mariëlle Stoelinga (Radboud University Nijmegen and University of Twente, The Netherlands) spoke on "Maintenance meets model checking: predictive maintenance via fault trees and formal methods"; and Alessio Lomuscio (Imperial College London, UK) gave a talk titled "Towards verifying neural-symbolic multi-agent systems". The abstracts of these talks are contained in this volume; we thank all three invited speakers for their insights.

Following the call for papers, there were 68 announced submissions, of which six were retracted or not submitted in time. The remaining 62 submissions were each reviewed independently by three reviewers, and this was followed by an online discussion amongst the reviewers. Based on the reviewing results, the Program Committee selected 19 full papers and three tool papers for presentation at the conference and publication in this volume. The editors thank the members of the Program Committee and the additional reviewers for their reviews and discussions. We also thank all authors for their submissions, whether accepted or not, and hope that they will keep contributing to future editions of this conference series. All SEFM submissions have to be original, unpublished, and not submitted concurrently for publication elsewhere.

Associated with the main SEFM 2022 conference was a SEFM summer school and six workshops: AI4EA 2022, FMAS 2022, F-IDE 2022, ASYDE 2022, CIFMA 2022, and CoSim-CPS 2022. We thank all organizers of the associated events for contributing to the success of SEFM. The proceedings of these events will appear in a separate LNCS volume.

Furthermore, we thank Antonio Cerone for his guidance in the organization, and the team at Springer for their support of SEFM 2022 and these proceedings. We also gratefully acknowledge Andrei Voronkov and the University of Manchester for the EasyChair system, which was used to handle the submission and review processes, and we wish the new EasyChair registration services and the whole EasyChair team success. Finally, we thank GFaI (Gesellschaft zur Förderung angewandter Informatik e.V.) for providing rooms and materials, the support team from Beijing Jiaotong University (Haoyuan Liu, Haoxiang Su, Dong Xie, and Qi Wang) for their help in editing the proceeding, and the support team from the Humboldt University of Berlin (Marc Carwehl, Eric Faust, Luisa Gerlach, Galina Greil, Philipp Jass, Sami Kharma, and Merlin von Wartburg) for their help in organizing SEFM 2022.

August 2022

Bernd-Holger Schlingloff
Ming Chai

Organization

Program Committee Chairs

Bernd-Holger Schlingloff	Fraunhofer FOKUS and Humboldt University of Berlin, Germany
Ming Chai	Beijing Jiaotong University, China

Program Committee

Jiri Barnat	Masaryk University, Czech Republic
Dirk Beyer	LMU München, Germany
Radu Calinescu	University of York, UK
María-Emilia Cambronero	University of Castilla-La Mancha, Spain
Ana Cavalcanti	University of York, UK
Alessandro Cimatti	Fondazione Bruno Kessler, Italy
Gabriel Ciobanu	Romanian Academy, Iasi, Romania
Corina Cirstea	University of Southampton, UK
Antonio Filieri	Imperial College London, UK
Mario Gleirscher	University of Bremen, Germany
Marie-Christine Jakobs	TU Darmstadt, Germany
Raluca Lefticaru	University of Bradford, UK
Antónia Lopes	Universidade de Lisboa, Portugal
Tiziana Margaria	University of Limerick – Lero, Ireland
Paolo Masci	National Institute of Aerospace, USA
Claudio Menghi	McMaster University, Canada
Rocco De Nicola	IMT School for Advanced Studies Lucca, Italy
Hans de Nivelle	Nazarbayev University, Kazakhstan
Peter Ölveczky	University of Oslo, Norway
Gordon Pace	University of Malta, Malta
Corina Pasareanu	Carnegie Mellon University, NASA, and KBR, USA
Violet Ka I Pun	Western Norway University of Applied Sciences, Norway
Markus Roggenbach	Swansea University, UK
Gwen Salaün	University of Grenoble Alpes, France
Augusto Sampaio	Federal University of Pernambuco, Brazil
Ina Schaefer	Karlsruhe Institute of Technology, Germany
Gerardo Schneider	Chalmers University of Technology and University of Gothenburg, Sweden
Marjan Sirjani	Malardalen University, Sweden
Elena Troubitsyna	KTH Royal Institute of Technology, Sweden
Graeme Smith	University of Queensland, Australia
Silvia Lizeth Tapia Tarifa	University of Oslo, Norway

Marina Waldén	Abo Akademi University, Finland
Heike Wehrheim	University of Oldenburg, Germany
Gianluigi Zavattaro	University of Bologna, Italy

List of Additional Reviewers

Filipe Arruda
Anna Becchi
Lukas Birkemeyer
Tabea Bordis
Marco Bozzano
Gabriele Costa
Dana Dghaym
Neil Evans
Xinwei Fang
Marco Feliu Gabaldon
Letterio Galletta
Sinem Getir Yaman
Alberto Griggio
George Hagen
Jan Haltermann
William Hughes
Calum Imrie
Omar Inverso
Eduard Kamburjan
Alexander Kittelmann
Christoph König
Frédéric Lang
Michael Lienhardt
Enrico Lipparini
Mariano Moscato
Cláudia Nalon
Felix Pauck
Ehsan Poorhadi
Cedric Richter
Lionel Rieg
Cleyton Rodrigues
Rudolf Schlatte
Arnab Sharma
Fedor Shmarov
Colin Snook
Marielle Stoelinga
Matteo Tadiello
Francesco Tiezzi
Catia Trubiani
Gricel Vazquez

Organizing Committee

Bernd-Holger Schlingloff	Fraunhofer FOKUS and Humboldt University of Berlin, Germany
Ming Chai	Beijing Jiaotong University, China

Steering Committee

Radu Calinescu	University of York, UK
Antonio Cerone	Nazarbayev University, Kazakhstan
Rocco De Nicola	IMT School for Advanced Studies Lucca, Italy
Gwen Salaün	University of Grenoble Alpes, France
Marjan Sirjani	Mälardalen University, Sweden

Webmaster

Ming Chai	Beijing Jiaotong University, China

Invited Talks

Distributed Process Calculi with Local States

Uwe Nestmann

Process calculi are popular for several reasons: (1) they precisely capture concurrent computation models via the syntax and semantics of minimalistic languages; (2) they are equipped with rich algebraic theories that build upon behavioural equivalences, often with precise logical counterparts; and (3) they support powerful action-based proof techniques. While these advantages of process calculi are good for many concurrent applications, the reasoning about distributed algorithms often requires analyses in a state-based style, e.g., using (global) invariants. Thus, we study extensions of process calculi with explicit support for distribution, where processes dispose of a private memory component representing their own explicit local state. In the talk, I addressed the motivation behind distributed process calculi with local states as well as the engineering principles when developing the design and theory of such calculi.

Maintenance Meets Model Checking—Predictive Maintenance via Fault Trees and Formal Methods

Mariëlle Stoelinga

Proper maintenance is crucial to keep our trains, power plants and robots up and running. Since maintenance is also expensive, effective maintenance is a typical optimization problem, where one balances costs against system performance (in terms of availability, reliability, and remaining useful lifetime).

Predictive maintenance is a promising technique that aims at predicting failures more accurately, so that just-in-time maintenance can be performed, doing maintenance exactly when and where needed. Thus, predictive maintenance promises higher availability and fewer failures at lower costs. In this talk, I advocated a combination of model-driven (esp. fault trees) and data analytical techniques to get more insight in the costs versus performance of maintenance strategies. I showed the results of several case studies from railroad engineering, namely rail track (with Arcadis), and HVAC (heating, ventilation, and air conditioning; with Dutch railroads).

Towards Verifying Neural-Symbolic Multi-Agent Systems

Alessio Lomuscio

A challenge in the deployment of multi-agent systems (MAS) remains the inherent difficulty of predicting with confidence their run-time behaviour. Over the past twenty years, increasingly scalable verification methods, including model checking and parameterised verification, have enabled the validation of several classes of MAS against AI-based specifications, and several MAS applications in services, robotics, security, and beyond.

Yet, a new class of agents is emerging in applications. Differently from traditional MAS, which are typically directly programmed (and less often purely neural), they combine both connectionist and symbolic aspects. We will refer to these as neural-symbolic MAS. These agents include a neural layer, often implementing a perception function, and symbolic or control-based layers, typically realising decision making and planning. Implementations of neural-symbolic agents permeate many present and forthcoming AI applications, including autonomous vehicles and robotics. Due to the neural layer, as well as their heterogeneity, verifying the behaviours of neural-symbolic MAS is particularly challenging. Yet, I argued that, given the safety-critical applications they are used in, methods and tools to address their formal verification should be developed.

In this talk I shared some of the contributions on this topic developed at the Verification of Autonomous Systems Lab at Imperial College London. I began by describing traditional approaches for the verification of symbolic MAS, and parameterised verification to address arbitrary collections of agents such as swarms. I then summarised our present efforts on verification of neural perception systems, including MILP-based approaches, linear relaxations, and symbolic interval propagation, introduce our resulting toolkits, Venus and Verinet, and exemplified their use.

This lead to existing methods for closed-loop, neural-symbolic MAS. In this context, I shared existing results that enable us to perform reachability analysis, and verify systems against bounded temporal specifications and Alternating Temporal Logic (ATL).

I concluded by highlighting some of the many challenges that lie ahead.

Contents

Software Verification

Program Analysis

Verifier Technology

Formal Methods for Intelligent and Learning Systems

Specification and Contracts

Program Synthesis

Temporal Logic

Runtime Methods