Lecture Notes in Computer Science 9762

Commenced Publication in 1973
Founding and Former Series Editors:
Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

More information about this series at http://www.springer.com/series/7408

Bernhard K. Aichernig · Carlo A. Furia (Eds.)

Tests and Proofs

10th International Conference, TAP 2016
Held as Part of STAF 2016
Vienna, Austria, July 5–7, 2016
Proceedings

Springer

Editors
Bernhard K. Aichernig
Graz University of Technology
Graz
Austria

Carlo A. Furia
Chalmers University of Technology
Göteborg
Sweden

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-41134-7 ISBN 978-3-319-41135-4 (eBook)
DOI 10.1007/978-3-319-41135-4

Library of Congress Control Number: 2016942015

LNCS Sublibrary: SL2 – Programming and Software Engineering

Printed on acid-free paper

This Springer imprint is published by Springer Nature
The registered company is Springer International Publishing AG Switzerland

Foreword

Software Technologies: Applications and Foundations (STAF) is a federation of leading conferences on software technologies. It provides a loose umbrella organization with a Steering Committee that ensures continuity. The STAF federated event takes place annually. The participating conferences may vary from year to year, but all focus on foundational and practical advances in software technology. The conferences address all aspects of software technology, from object-oriented design, testing, mathematical approaches to modeling and verification, transformation, model-driven engineering, aspect-oriented techniques, and tools.

STAF 2016 took place at TU Wien, Austria, during July 4–8, 2016, and hosted the five conferences ECMFA 2016, ICGT 2016, ICMT 2016, SEFM 2016, and TAP 2016, the transformation tool contest TTC 2016, eight workshops, a doctoral symposium, and a projects showcase event. STAF 2016 featured eight internationally renowned keynote speakers, and welcomed participants from around the world.

The STAF 2016 Organizing Committee thanks (a) all participants for submitting to and attending the event, (b) the program chairs and Steering Committee members of the individual conferences and satellite events for their hard work, (c) the keynote speakers for their thoughtful, insightful, and inspiring talks, and (d) TU Wien, the city of Vienna, and all sponsors for their support. A special thank you goes to the members of the Business Informatics Group, coping with all the foreseen and unforeseen work (as usual ☺)!

July 2016 Gerti Kappel

Preface

The TAP conference promotes research in verification and formal methods that targets the interplay of proofs and testing: the advancement of techniques of each kind and their combination, with the ultimate goal of improving software and system dependability. This volume contains the proceedings of TAP 2016, which marks a decade of TAP conferences since the first edition in 2007. As in the three previous editions, TAP 2016 was part of STAF (Software Technologies: Applications and Foundations), a federation of leading conferences in software technology.

TAP 2016 took place in Vienna during July 5–7, 2016. The Program Committee (PC) received 19 paper submissions, each reviewed by three PC members. After two weeks of lively discussion and careful deliberation, we selected 11 contributions (eight regular papers, one tool demonstration paper, and two short papers) for inclusion in this proceedings volume and presentation at the conference. The combination of topics highlights how testing and proving are increasingly seen as complementary rather than mutually exclusive techniques, and confirms TAP's commitment to bringing together researchers and practitioners from both areas of verification.

The program of TAP was nicely completed by a keynote talk by Kim G. Larsen (Aalborg University, Denmark) and an industrial keynote talk by Klaus Reichl (Thales, Austria), whose content is also documented in this volume. We would like to thank both invited speakers for contributing exciting presentations from the different perspective of academic research and industrial practice.

We also thank the PC members and the additional reviewers for their timely and thorough reviewing work, and for contributing to an animated and informed discussion. Their names are listed on the following pages. The EasyChair system provided flawless technical support to the process.

The organization of STAF made for a successful and enjoyable conference in a wonderful location. We thank all the organizers, and in particular the general chair, Gerti Kappel, and the organization chair, Tanja Mayerhofer, for their hard work, and TU Wien for hosting us. Thanks also to Richard Schumi from TU Graz for managing TAP's website.

July 2016

Bernhard K. Aichernig
Carlo A. Furia

Organization

Program Committee

Bernhard K. Aichernig	TU Graz, Austria
Jasmin C. Blanchette	Inria Nancy and LORIA, France
Achim D. Brucker	University of Sheffield, UK
Catherine Dubois	ENSIEE-CEDRIC, France
Gordon Fraser	University of Sheffield, UK
Carlo A. Furia	Chalmers University of Technology, Sweden
Juan Pablo Galeotti	University of Buenos Aires, Argentina
Angelo Gargantini	University of Bergamo, Italy
Alain Giorgetti	LIFC, University of Franche-Comte, France
Christoph Gladisch	BOSCH, Germany
Martin Gogolla	University of Bremen, Germany
Arnaud Gotlieb	SIMULA Research Laboratory, Norway
Ashutosh Gupta	TIFR, India
Marieke Huisman	University of Twente, The Netherlands
Reiner Hähnle	Technical University of Darmstadt, Germany
Bart Jacobs	Katholieke Universiteit Leuven, Belgium
Nikolai Kosmatov	CEA LIST, France
Laura Kovacs	Chalmers University of Technology, Sweden
Shaoying Liu	Hosei University, Japan
Panagiotis Manolios	Northeastern University, USA
Karl Meinke	Royal Institute of Technology (KTH), Sweden
Brian Nielsen	Aalborg University, Denmark
Nadia Polikarpova	MIT CSAIL, USA
Andrew Reynolds	University of Iowa, USA
Augusto Sampaio	Federal University of Pernambuco, Brazil
Martina Seidl	Johannes Kepler University Linz, Austria
Jun Sun	Singapore University of Technology and Design, Singapore
Nikolai Tillmann	Microsoft Research, USA
T.H. Tse	The University of Hong Kong, SAR China
Margus Veanes	Microsoft Research, USA
Burkhart Wolff	University of Paris-Sud, France

Additional Reviewers

Bubel, Richard
Christakis, Maria
Fleury, Mathias
Hoelscher, Karsten
Hübner, Felix
Kumar, Ramana
Scheurer, Dominic

Abstracts of Invited Contributions

From Testing and Verification to Performance Analysis and Synthesis of Cyber-Physical Systems

Kim G. Larsen

Department of Computer Science
Aalborg University, Aalborg, Denmark
kgl@cs.aau.dk

Abstract. Timed automata and games, priced timed automata and energy automata have emerged as useful formalisms for modeling real-time and energy-aware systems as found in several embedded and cyber-physical systems. In this talk we will survey how the various components of the UPPAAL tool-suite over a 20 year period have been developed to support various types of analysis of these formalisms.

This includes the classical usage of UPPAAL as an efficient model checker of hard real time constraints of timed automata models, but also the branch UPPAAL TRON which has been extensively used to perform on-and off-line conformance testing of real-time systems with respect to timed automata specifications.

More ambitiously, UPPAAL TIGA allow for automatic synthesis of strategies – and subsequent executable control programs – for safety and reachability objectives. Most recently the branch UPPAAL SMC offers a highly scalable statistical model checking engine supporting performance analysis of stochastic hybrid automata, and the branch UPPAAL-STRATEGO supports synthesis (using machine learning) and evaluation of near-optimal strategies for stochastic priced timed games. The keynote will review the various branches of UPPAAL and indicate their concerted applications to a range of real-time and cyber-physical examples.

Using Formal Methods for Verification and Validation in Railway

Klaus Reichl, Tomas Fischer, and Peter Tummeltshammer

Thales Austria GmbH, Handelskai 92, 1200 Vienna, Austria
{klaus.reichl,tomas.fischer,
peter.tummeltshammer}@thalesgroup.com

Abstract. A very promising and efficient method of showing the correctness of a complex system is using formal methods on a model of that system. To this end there exist plentiful methods and tools for easing the mathematically burdensome process of refinement and proofs, as well as the computationally complex task of model checking.

While in todays industrial applications formal methods are mostly used for verification (i.e. for showing that the system model fulfills properties such as completeness and consistency) we propose to use these methods for validation as well (i.e. correspondence of the model with the customer needs).

In this paper we show the applicability as well as the limitations of this approach for feature driven development towards continuous verification and validation. As an example we present a model of a railway interlocking system written in Event-B.

The model can be instantiated and animated, which in combination with model checking and formal proofs demonstrates the usefulness of the approach.

The resulting model can be used again to automatically generate test cases which are suitable to show the correspondence of the implementation and the model, given that the model supports a sufficient level of detail.

Contents

Short Contributions