Maurice H. ter Beek · Stefania Gnesi
Alexander Knapp (Eds.)

LNCS 9933

Critical Systems: Formal Methods and Automated Verification

Joint 21st International Workshop on Formal Methods for Industrial Critical Systems and 16th International Workshop on Automated Verification of Critical Systems, FMICS-AVoCS 2016

Pisa, Italy, September 26–28, 2016, Proceedings

FMICS

AVOCS

Springer

Lecture Notes in Computer Science 9933

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

Maurice H. ter Beek · Stefania Gnesi
Alexander Knapp (Eds.)

Critical Systems: Formal Methods and Automated Verification

Joint 21st International Workshop
on Formal Methods for Industrial Critical Systems and
16th International Workshop
on Automated Verification of Critical Systems, FMICS-AVoCS 2016
Pisa, Italy, September 26–28, 2016
Proceedings

Springer

Editors
Maurice H. ter Beek
ISTI-CNR
Pisa
Italy

Alexander Knapp
Universität Augsburg
Augsburg
Germany

Stefania Gnesi
ISTI-CNR
Pisa
Italy

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-45942-4 ISBN 978-3-319-45943-1 (eBook)
DOI 10.1007/978-3-319-45943-1

Library of Congress Control Number: 2016950740

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
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Preface

This volume contains the papers presented at the International Workshop on Formal Methods for Industrial Critical Systems and Automated Verification of Critical Systems (FMICS-AVoCS), which was held in Pisa, Italy, September 26–28, 2016. FMICS-AVoCS 2016 combines the 21st International Workshop on Formal Methods for Industrial Critical Systems and the 16th International Workshop on Automated Verification of Critical Systems.

The aim of the FMICS workshop series is to provide a forum for researchers who are interested in the development and application of formal methods in industry. In particular, FMICS brings together scientists and engineers that are active in the area of formal methods and interested in exchanging their experiences in the industrial usage of these methods. The FMICS workshop series also strives to promote research and development for the improvement of formal methods and tools for industrial applications.

The aim of the AVoCS workshop series is to contribute to the interaction and exchange of ideas among members of the international research community on tools and techniques for the verification of critical systems. The subject is to be interpreted broadly and inclusively. It covers all aspects of automated verification, including model checking, theorem proving, SAT/SMT constraint solving, abstract interpretation, and refinement pertaining to various types of critical systems that need to meet stringent dependability requirements (safety-critical, business-critical, performance-critical, etc.).

The topics of interest include, but are not limited to:

- Design, specification, refinement, code generation, and testing of critical systems based on formal methods
- Methods, techniques, and tools to support automated analysis, certification, debugging, learning, optimization, and transformation of critical systems, in particular distributed, real-time systems, and embedded systems
- Automated verification (model checking, theorem proving, SAT/SMT constraint solving, abstract interpretation, etc.) of critical systems
- Verification and validation methods that address shortcomings of existing methods with respect to their industrial applicability (e.g., scalability and usability issues)
- Tools for the development of formal design descriptions
- Case studies and experience reports on industrial applications of formal methods, focusing on lessons learned or identification of new research directions
- Impact of the adoption of formal methods on the development process and associated costs
- Application of formal methods in standardization and industrial forums

This year we received 24 submissions. Each of these submissions went through a rigorous review process in which each paper was reviewed by at least three researchers from a strong Program Committee of international reputation. We selected 11 full papers and 4 short papers for presentation during the workshop and inclusion in these proceedings. The workshop also featured keynotes by Thomas Arts (QuviQ AB, Gothenburg, Sweden), Silvia Mazzini (Intecs SpA, Pisa, Italy), and Jan Peleska (Universität Bremen, Germany). We hereby thank the invited speakers for having accepted our invitation.

We are very grateful to our sponsors, the European Research Consortium for Informatics and Mathematics (ERCIM), Formal Methods Europe (FME), and Springer International Publishing AG. We thank Alfred Hofmann (Vice-President Publishing) and the Editorial staff of Springer for publishing these proceedings. We also thank Tiziana Margaria (University of Limerick & LERO, the Irish Software Research Center, Ireland), the coordinator of the ERCIM working group FMICS, and the other board members, as well as the steering committee of AVoCS, all listed below, for their continuous support during the organization of FMICS-AVoCS. We acknowledge the support of EasyChair for assisting us in managing the complete process from submission to these proceedings.

Finally, we would like to thank the Program Committee members and the external reviewers, listed below, for their accurate and timely reviewing, all authors for their submissions, and all attendees of the workshop for their participation.

July 2016

Maurice ter Beek
Stefania Gnesi
Alexander Knapp

Organization

General Chair

Maurice H. ter Beek	ISTI–CNR, Pisa, Italy

Program Committee Co-chairs

Stefania Gnesi	ISTI–CNR, Pisa, Italy
Alexander Knapp	Universität Augsburg, Germany

Program Committee

Maria Alpuente	Universitat Politècnica de Valéncia, Spain
Jiri Barnat	Masarykova Univerzita, Czech Republic
Michael Dierkes	Rockwell Collins, Blagnac, France
Cindy Eisner	IBM Research, Haifa, Israel
Alessandro Fantechi	Università di Firenze, Italy
Francesco Flammini	Ansaldo STS, Naples, Italy
María del Mar Gallardo	Universidad de Málaga, Spain
Michael Goldsmith	University of Oxford, UK
Gudmund Grov	Heriot-Watt University, UK
Matthias Güdemann	Diffblue Ltd., Oxford, UK
Marieke Huisman	Universiteit Twente, The Netherlands
Gerwin Klein	NICTA and University of New South Wales, Australia
Peter Gorm Larsen	Aarhus Universitet, Denmark
Thierry Lecomte	ClearSy, Aix-en-Provence, France
Tiziana Margaria	University of Limerick and LERO, Ireland
Radu Mateescu	Inria Grenoble Rhône-Alpes, France
David Mentré	Mitsubishi Electric R&D Centre Europe, Rennes, France
Stephan Merz	Inria Nancy and LORIA, France
Manuel Núñez	Universidad Complutense de Madrid, Spain
Peter Ölveczky	Universitetet i Oslo, Norway
Charles Pecheur	Université Catholique de Louvain, Belgium
Marielle Petit-Doche	Systerel, Aix-en-Provence, France
Ralf Pinger	Siemens AG, Braunschweig, Germany
Jaco van de Pol	Universiteit Twente, The Netherlands
Markus Roggenbach	Swansea University, UK
Matteo Rossi	Politecnico di Milano, Italy
Marco Roveri	FBK-irst, Trento, Italy

Thomas Santen	Microsoft Research Advanced Technology Labs Europe, Aachen, Germany
Bernhard Steffen	Universität Dortmund, Germany
Jun Sun	University of Technology and Design, Singapore
Helen Treharne	University of Surrey, UK

Additional Reviewers

Joël Allred
Jaroslav Bendík
Marco Bozzano
Ning Gee
Stefan Hallerstede
Laura Panizo
Enno Ruijters
Alberto Salmerón
Julia Sapiña
Wendelin Serwe

FMICS WG Board Members

Álvaro Arenas	IE Business School, Madrid, Spain
Luboš Brim	Masarykova Univerzita, Czech Republic
Alessandro Fantechi	Università di Firenze, Italy
Hubert Garavel	Inria Grenoble Rhône-Alpes, France
Stefania Gnesi	ISTI–CNR, Pisa, Italy
Diego Latella	ISTI–CNR, Pisa, Italy
Tiziana Margaria	University of Limerick and LERO, Ireland
Radu Mateescu	Inria Grenoble Rhône-Alpes, France
Pedro Merino	Universidad de Málaga, Spain
Jaco van de Pol	Universiteit Twente, The Netherlands

AVoCS Steering Committee

Michael Goldsmith	University of Oxford, UK
Stephan Merz	Inria Nancy and LORIA, France
Markus Roggenbach	Swansea University, UK

Sponsors

ERCIM
European Research Consortium
for Informatics and Mathematics

FORMAL METHODS EUROPE

Springer

Abstracts of the Invited Talks

Lessons Learned in a Journey Toward Correct-by-Construction Model-Based Development

Laura Baracchi[1], Silvia Mazzini[1], Stefano Puri[1],
and Tullio Vardanega[2]

[1] Intecs SpA, Pisa, Italy
{laura.baracchi,silvia.mazzini,stefano.puri}@intecs.it
[2] Università di Padova, Italy
tullio.vardanega@math.unipd.it

Abstract. In our view, an effective correct-by-construction (CbyC) approach, geared to making it extremely difficult to introduce errors in the software development process, would have two main ingredients: one, the adoption of model-driven engineering (MDE) to manipulate malleable and yet powerful abstractions; the other, rigor at each development step, to enable (possibly automated) formal reasoning or analysis of the correctness of the step, and (possibly automated) derivation, whenever possible, of correct base input for the subsequent step.

We advocate that using models in most of the development steps, supported by adequate MDE techniques and tooling (far more productive today than in the early age of CbyC), makes it easier to define correct requirements, to design a system that meets the requirements, and to develop an implementation that preserves the desired correctness properties. We discuss lessons learned in the attempt to apply the long-known principles of CbyC first promoted by Dijkstra, to modern model-based development practices. We recall the intent and scrutinize the outcomes of a string of research projects that focused explicitly on the pursuit of CbyC by means of model-driven methods and technologies. The lessons learned show that when CbyC extends from the algorithmic and functional dimension to extra-functional concerns, some of the strength of original CbyC concept and its pull dilute. One of the possible causes of that phenomenon, is that — in some situation — the assertive style of algorithm refinement gives way to more tentative exploration of an unknown solution space where the known truths are insuffcient to steer the development.

Keywords: Model-based development · Model transformation · Correctness by construction · Formal methods · Contract refinement

Model-based Testing Strategies and Their (In)dependence on Syntactic Model Representations

Jan Peleska[1,2] and Wen-ling Huang[2]

[1] Verified Systems International GmbH, Bremen, Germany
[2] Department of Mathematics and Computer Science,
University of Bremen, Bremen, Germany
{jp,huang}@cs.uni-bremen.de

Abstract. Model-based testing (MBT) in its most advanced form allows for automated test case identification, test data calculation, and test procedure generation from reference models describing the expected behaviour of the system under test (SUT). If the underlying algorithms for test case identification operate only on the syntactic representation of test models, however, the resulting test strength depends on the syntactic representation as well. This observation is true, even if syntactically differing models are behaviourally equivalent. In this paper, we present a systematic approach to elaborating test case selection strategies that only depend on the behavioural semantics of test models, but are invariant under syntactic transformations preserving the semantics. The benefits of these strategies are discussed, and practical generation algorithms are presented.

Keywords: Model-based testing · Equivalence class partition testing · Kripke structures · Complete testing theories

Random Testing of Formal Properties for Industrial Critical Systems

Thomas Arts

Quviq AB, Gothenburg, Sweden
thomas.arts@quviq.com

Abstract. QuickCheck is a tool that can automatically generate test cases for software systems. These tests are generated from manually specified formal properties or models that the system is supposed to conform to. The set of possible tests for such systems is practically infinite. QuickCheck uses a random selection strategy for generating test cases. Compared to other selection strategies, QuickCheck can very quickly generate tests and more time is spent on testing than on carefully selecting tests; this works best in situations where test execution can be performed in seconds rather than days.

The result is a light-weight method for finding software faults in industrial critical systems in the domain of telecommunication, automotive, database systems, financial systems and medical devices. Compared to many formal methods, this kind of light-weight formal testing is very cost effective for finding faults.

However, if no faults are found, the obvious question is: "how well is the software tested?". We present some results based on measuring coverage. Code coverage is a poor measure for correctness, as will be confirmed for line coverage through MC/DC coverage.

As an alternative we look at requirement coverage and generate test suites that cover all requirements. This again results in very poor fault detection. Even after improving the notion of "covering requirements", we see that random testing detects more faults than carefully constructed tests that cover all requirements.

By giving the user control over defining and measuring what has been tested, we can increase the confidence in the models underlying the test generation. Nevertheless, more research is needed to find satisfactory criteria for sufficient testing.

Contents

Invited Talk

Automated Verification Techniques

Model-Based System Analysis

Applications and Case Studies