Lecture Notes in Computer Science **10469**

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

Formal Methods

Subline of Lectures Notes in Computer Science

More information about this series at http://www.springer.com/series/7407

Alessandro Cimatti · Marjan Sirjani (Eds.)

Software Engineering and Formal Methods

15th International Conference, SEFM 2017
Trento, Italy, September 4–8, 2017
Proceedings

Springer

Editors
Alessandro Cimatti
University of Trento
Trento
Italy

Marjan Sirjani
Mälardalen University
Västerås
Sweden

ISSN 0302-9743 ISSN 1611-3349 (electronic)
Lecture Notes in Computer Science
ISBN 978-3-319-66196-4 ISBN 978-3-319-66197-1 (eBook)
DOI 10.1007/978-3-319-66197-1

Library of Congress Control Number: 2017949511

LNCS Sublibrary: SL1 – Theoretical Computer Science and General Issues

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 SEFM 2017, the 15th International Conference on Software Engineering and Formal Methods, held on September 4–8 in Trento, Italy. SEFM 2017 was organized and hosted by the Fondazione Bruno Kessler (FBK), Trento, Italy.

The SEFM conference aims to bring together leading 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. The topics of interest for submission included the following aspects of software engineering and formal methods:

- New frontiers in software architecture: self-adaptive, service-oriented, and cloud computing systems; component-based, object-based, and multi-agent systems; real-time, hybrid, and embedded systems; reconfigurable systems
- Software verification and testing: model checking and theorem proving; verification and validation; probabilistic verification and synthesis; testing
- Software development methods: requirement analysis, modeling, specification, and design; light-weight and scalable formal methods
- Application and technology transfer: case studies, best practices, and experience reports; tool integration
- Security and safety: security and mobility; safety-critical, fault-tolerant, and secure systems; software certification
- Design principles: domain-specific languages, type theory, abstraction, and refinement

SEFM 2017 hosted six workshops:

- FAACS – Formal Approaches for Advanced Computing Systems
- MSE – Microservices: Science and Engineering
- POTENTIAL – Technology Transfer in Software Engineering and Formal Methods
- DataMod – From Data to Models and Back
- CoSim-CPS – Formal Co-Simulation of Cyber-Physical Systems
- FOCLASA – Foundations of Coordination Languages and Self-Adaptive Systems

SEFM 2017 solicited full research papers describing original research results, case studies and tools, and short papers on new ideas and work-in-progress, describing new approaches, techniques and/or tools that are not fully validated yet. We received 102 submissions (88 full and 14 short) from 36 different countries. Each submission was reviewed by at least four Program Committee members. We accepted 22 regular papers, with an acceptance rate of 25%. We also accepted 6 short papers on new ideas and work-in-progress. The program also included three remarkable invited talks:

- Marsha Chechik, from the University of Toronto, Canada, presented "Software Safety and Security, Assurance Cases and Model Management".
- Jeff Kramer, from Imperial College London, UK, presented "The Challenge of Change".
- Alberto Sangiovanni-Vincentelli, from the University of California, Berkeley, USA, presented "A Formal Contract-Based Design Methodology for Cyber-Physical Systems".

Our first words of thanks go to the Program Committee members and to the external reviewers, who carried out thorough and careful reviews and enabled the assembly of this high-quality work. We thank the authors for their submissions, and for their collaboration in further improving their papers. A special word of thanks goes to our invited speakers, Marsha Chechick, Jeff Kramer and Alberto Sangiovanni-Vincentelli, for accepting our invitation and for their very stimulating contributions. We also thank the workshop chairs, Antonio Cerone and Marco Roveri, and the organizers of the workshops: Paolo Arcaini, Marina Mongiello, Elvinia Riccobene and Patrizia Scandurra (FAACS); Marcello M. Bersani, Antonio Bucchiarone, Luca Ferrucci, Manuel Mazzara, Fabrizio Montesi and Nicola Dragoni (MSE); Roberto Confalonieri and Andrea Janes (POTENTIAL); Paolo Milazzo, Vashti Galpin and Andre Teixeira (DataMod); Cinzia Bernardeschi, Paolo Masci and Peter Gorm Larsen (CoSim-CPS); Carlos Canal and Gwen Salaün (FOCLASA). Many thanks to Alberto Griggio (publicity chair) and Gianni Zampedri (web master). A special word of thanks goes to Annalisa Armani and to all the other members of the Ufficio Eventi of FBK, who largely contributed to the success of this event. We also thank the developers and maintainers of the EasyChair conference management system, which was of great help in handling paper submission, reviewing, discussion, and the assembly of the proceedings. Finally, we are most grateful to Hossein Hojjat, who provided invaluable help in the preparation of the conference proceedings.

July 2017

Alessandro Cimatti
Marjan Sirjani

Organization

Program Committee

Wolfgang Ahrendt	Chalmers University of Technology, Sweden
Farhad Arbab	CWI and Leiden University, Netherlands
Luis Barbosa	Universidade do Minho, Portugal
Antonia Bertolino	ISTI-CNR, Italy
Dirk Beyer	LMU Munich, Germany
Jonathan Bowen	London South Bank University, UK
Mario Bravetti	University of Bologna, Italy
Ana Cavalcanti	University of York, UK
Alessandro Cimatti	FBK, Italy
Paul Curzon	Queen Mary University of London, UK
Hung Dang Van	UET, Vietnam National University, Hanoi
Jim Davies	University of Oxford, UK
Rocco De Nicola	IMT - School for Advanced Studies Lucca, Italy
Patricia Derler	National Instruments, USA
John Derrick	Unversity of Sheffield, UK
Anke Dittmar	University of Rostock, Germany
George Eleftherakis	The University of Sheffield International Faculty, CITY College, Greece
José Luiz Fiadeiro	Royal Holloway, University of London, UK
Wan Fokkink	Vrije Universiteit Amsterdam, Netherlands
Adrian Francalanza	University of Malta, Malta
Hubert Garavel	Inria Rhône-Alpes/CONVECS, France
Dimitra Giannakopoulou	NASA Ames, USA
Stefania Gnesi	ISTA-CNR, Italy
Klaus Havelund	Jet Propulsion Laboratory, California Institute of Technology, USA
Rob Hierons	Brunel University London, UK
Hossein Hojjat	Rochester Institute of Technology, USA
Michaela Huhn	Ostfalia, Germany
Einar Broch Johnsen	University of Oslo, Norway
Gabriel Juhas	Slovak University of Technology, Bratislava, Slovakia
Jens Knoop	TU Wien, Austria
Paddy Krishnan	Oracle, Australia
Eva Kühn	TU Wien, Austria
Kung-Kiu Lau	The University of Manchester, UK
Sergio Mover	University of Colorado Boulder, USA
Viet Yen Nguyen	Hypefactors, Denmark
Fernando Orejas	UPC, Barcellona, Spain

Corina Pasareanu	CMU/NASA Ames Research Center, USA
Marinella Petrocchi	IIT-CNR, Italy
Anna Philippou	University of Cyprus, Cyprus
Sanjiva Prasad	Indian Institute of Technology, India
Geguang Pu	East China Normal University, China
Leila Ribeiro	UFRGS, Federal University of Rio Grande do Sul, Brazil
Bernhard Rumpe	RWTH Aachen University, Germany
Gwen Salaün	Grenoble INP - Inria - LIG, France
Augusto Sampaio	Federal University of Pernambuco, Brazil
Vesna Sesum-Cavic	TU Wien, Austria
Marjan Sirjani	Malardalen University, Sweden
Graeme Smith	University of Queensland, Australia
Bernhard Steffen	University of Dortmund, Germany
Markus Stumptner	University of South Australia, Australia
Francesco Tiezzi	Università di Camerino, Italy
Danny Weyns	Linnaeus University, Sweden

Additional Reviewers

Achilleos, Antonis
Adam, Kai
Attard, Duncan
Åman Pohjola, Johannes
Banach, Richard
Barbon, Gianluca
Basile, Davide
Bertram, Vincent
Blanchette, Jasmin Christian
Bliudze, Simon
Bolognesi, Tommaso
Bride, Hadrien
Bubel, Richard
Butting, Arvid
Carvalho, Gustavo
Cassar, Ian
Chen, Yuting
Chimento, Jesus Mauricio
Colvin, Robert
Cooper, Gregory
Crass, Stefan
Cresci, Stefano
Dangl, Matthias
De Angelis, Francesco
Del Vigna, Fabio
Din, Crystal Chang
Dokter, Kasper
Dongol, Brijesh
Eikermann, Robert
Ertl, M. Anton
Fazzolari, Michela
Fedyukovich, Grigory
Fornari, Fabrizio
Friedberger, Karlheinz
Grech, Neville
Green, Ryan
Greifenberg, Timo
Grossmann, Georg
Guo, Jian
Howar, Falk
Inverso, Omar
Jebali, Fatma
K.R., Raghavendra
Kappé, Tobias
Kautz, Oliver
Kourtis, Georgios
Krall, Andreas
Kusmenko, Evgeny
Lang, Frédéric
Lazovik, Alexander
Lemberger, Thomas
Li, Jianwen

Loreti, Michele
Lu, Yi
Luiz Leite Jr., Fabio
Madeira, Alexandre
Maggi, Alessandro
Margheri, Andrea
Marsso, Lina
Martins, Francisco
Matteucci, Ilaria
Mauro, Jacopo
Mavridou, Anastasia
Mayer, Wolfgang
Mazzanti, Franco
Messinger, Anita
Miao, Weikai
Morichetta, Andrea
Mota, Alexandre
Muzi, Chiara
Nelson, Tim
Olesen, Mads Chr.
Oliveira, Marcel Vinicius Medeiros
Owens, Scott
Ozeer, Umar
Pinisetty, Srinivas
Planer, Martin
Polini, Andrea
Proenca, Jose
Pun, Ka I
Puntigam, Franz
Pérez, Jorge A.
Qiang, Wang
Raco, Deni
Radschek, Sophie Therese
Razavi, Joseph
Re, Barbara
Riely, James
Robillard, Simon
Rossi, Lorenzo
Rossi, Matteo
Rüthing, Oliver
Saracino, Andrea
Saraiva, João
Schlatte, Rudolf
Schoepe, Daniel
Seceleanu, Cristina
Selway, Matt
Serwe, Wendelin
Tapia Tarifa, Silvia Lizeth
Tesei, Luca
Tognazzi, Stefano
Trivedi, Ashutosh
Tutu, Ionut
Vandin, Andrea
von Wenckstern, Michael
Vorobyov, Kostyantyn
Voß, Jan-Niklas
Weber, Jean-Francois
Wehrheim, Heike
Welch, James
Wendler, Philipp
Winter, Kirsten

Invited Talks

The Challenge of Change

Jeff Kramer

Department of Computing, Imperial College London, London, UK
j.kramer@imperial.ac.uk

Abstract. One of the grand challenges of our time is the provision of self-managing adaptive systems. In the extreme, these are required to handle unexpected and unplanned changes that occur at run-time. These unexpected changes can be in any or all of the following: the environment in which the system operates, the capabilities of the system, or in the requirements and goals that the system should achieve. Although ad hoc techniques can be used for specific circumstances, what we need are rigorous, comprehensive, and pragmatic approaches to deal with the challenges that operational run-time change presents. Formal models, appropriate for the aspects of concern, are essential to support dynamic (semi-) automatic reasoning about change. Furthermore, these models need to be available at runtime and should themselves be amenable to modification. These models@runtime are needed for aspects such as domain modelling and model revision, software configuration and reconfiguration, requirements goals and goal revision and planning and plan revision. The foundation necessary to support these models@runtime is a sound software architecture. This talk will elaborate on this vision and propose a software architecture to support run-time change and adaptation.

Software Safety and Security, Assurance Cases and Model Management

Marsha Chechik

Department of Computer Science, University of Toronto,
Toronto, ON, M5S2E4, Canada
chechik@cs.toronto.edu

Abstract. From financial services platforms to social networks to vehicle control, software has come to mediate many activities of daily life. Governing bodies and standards organizations have responded to this trend by creating regulations and standards to address issues such as safety, security and privacy. In this environment, the compliance of software development to standards and regulations has emerged as a key requirement; yet, software compliance is a costly and complex goal to achieve. For example, one estimate of the cost of compliance in the US to the Sarbanes-Oxley Act (SOX) is $8B per year [1]. Regulatory compliance creates software development complexity in various ways. An organization may have to comply with multiple standards due to multiple jurisdictions or to address different aspects of the software, and these may overlap and conflict with each other. Evidence of compliance must be collected, managed and linked to an *assurance case* that contains the claims and arguments for compliance. When software evolves, compliance must be reassessed, which can delay the release of changes. Finally, maintaining families of related software products (product lines) multiplies the effort even further.

Standards, development artifacts and compliance evidence can all be expressed as *models*. The field of Model Management [2] has emerged to address another software development complexity problem – the proliferation of software models in model-driven software development [3]. Model management focuses on a high-level view in which entire models and their relationships (i.e., mappings between models) can be manipulated using specialized operators to achieve useful outcomes.

In this talk, we look at the connection between compliance and modeling to reduce compliance complexity and cost, as well as to facilitate reuse and evolution, with a special focus on automotive software development [4, 5].

Acknowledgements

Joint work with Sahar Kokaly, Rick Salay, Tom Maibaum, Mark Lawford, Alessio DiSandro, Nick Fung.

References

1. Carney, W.J.: The costs of being public after sarbanes-oxley: the irony of going private. Emory LJ **55**, 141 (2006)
2. Bernstein, P.A.: Applying model management to classical meta data problems. In: Proceedings of the CIDR 2003, vol. 2003, pp. 209–220 (2003)
3. Beydeda, S., Book, M., Gruhn, V., et al.: Model-Driven Software Development. vol. 15, Springer, Heidelberg (2005)
4. Kokaly, S., Salay, R., Chechik, M., Lawford, M., Maibaum, T.: Safety case impact assessment in automotive software systems: an improved model-based approach. In: Proceedings of the SafeComp 2017 (2017)
5. Kokaly, S., Salay, R., Cassano, V., Maibaum, T., Chechik, M.: A model management approach for assurance case reuse due to system evolution. In: Proceedings of the MoDELS 2016, pp.196–206 (2016)

A Formal Contract-Based Design Methodology for CyberPhysical Systems

Alberto Sangiovanni-Vincentelli

Department of Electrical Engineering and Computer Sciences,
University of California, Berkeley
alberto@berkeley.edu

Abstract. In cyber-physical systems (CPS) computing, networking and control (typically regarded as the "cyber" part of the system) are tightly intertwined with mechanical, electrical, thermal, chemical or biological processes (the "physical" part). The increasing sophistication and heterogeneity of these systems requires radical changes in the way sense-and-control platforms are designed to regulate them. In this presentation, I introduce a design methodology whereby platform-based design is combined with assume-guarantee contracts to formalize the design process and enable realization of CPS architectures and control software in a hierarchical and compositional manner.

Contents