

*Commenced Publication in 1973*

Founding and Former Series Editors:

Gerhard Goos, Juris Hartmanis, and Jan van Leeuwen

## Editorial Board

David Hutchison

*Lancaster University, Lancaster, UK*

Takeo Kanade

*Carnegie Mellon University, Pittsburgh, PA, USA*

Josef Kittler

*University of Surrey, Guildford, UK*

Jon M. Kleinberg

*Cornell University, Ithaca, NY, USA*

Friedemann Mattern

*ETH Zurich, Zurich, Switzerland*

John C. Mitchell

*Stanford University, Stanford, CA, USA*

Moni Naor

*Weizmann Institute of Science, Rehovot, Israel*

C. Pandu Rangan

*Indian Institute of Technology Madras, Chennai, India*

Bernhard Steffen

*TU Dortmund University, Dortmund, Germany*

Demetri Terzopoulos

*University of California, Los Angeles, CA, USA*

Doug Tygar

*University of California, Berkeley, CA, USA*

Gerhard Weikum

*Max Planck Institute for Informatics, Saarbrücken, Germany*

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


Kyungmin Bae · Peter Csaba Ölveczky (Eds.)

# Formal Aspects of Component Software

15th International Conference, FACS 2018  
Pohang, South Korea, October 10–12, 2018  
Proceedings

*Editors*

Kyungmin Bae   
Pohang University of Science  
and Technology  
Pohang  
South Korea

Peter Csaba Ölveczky   
University of Oslo  
Oslo, Norway

ISSN 0302-9743 ISSN 1611-3349 (electronic)  
Lecture Notes in Computer Science  
ISBN 978-3-030-02145-0 ISBN 978-3-030-02146-7 (eBook)  
<https://doi.org/10.1007/978-3-030-02146-7>

Library of Congress Control Number: 2018957278

LNCS Sublibrary: SL2 – Programming and Software Engineering

© Springer Nature Switzerland AG 2018

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, express 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 proceedings of the 15th International Conference on Formal Aspects of Component Software (FACS 2018), held at Pohang University of Science and Technology (POSTECH), Korea, during October 10–12, 2018.

Component-based software development proposes sound engineering principles and techniques to cope with the complexity of present-day software systems. However, many challenging conceptual and technological issues remain in component-based software development theory and practice. Furthermore, the advent of service-oriented and cloud computing, cyber-physical systems, and the Internet of Things has brought to the fore new dimensions, such as quality of service and robustness to withstand faults, which require revisiting established concepts and developing new ones.

The FACS series of events addresses the application of formal methods in all aspects of software components and services. Formal methods have provided foundations for component-based software through research on mathematical models for components, composition and adaptation, and rigorous approaches to verification, deployment, testing, and certification.

FACS 2018 received 32 regular and tool paper submissions. All but four submissions were reviewed by at least three reviewers. Based on the reviews and extensive discussions, the program committee decided to accept 12 regular papers and two tool papers. This volume contains those 14 papers, an invited paper by Edward A. Lee, and an abstract of an invited talk by Grigore Rosu.

Many colleagues and friends contributed to FACS 2018. We thank Edward A. Lee and Grigore Rosu for accepting our invitations to give invited talks, and the authors who submitted their work to FACS 2018. We are grateful to the members of the program committee for providing timely and insightful reviews as well as for their involvement in the post-reviewing discussions. We also thank the members of the FACS steering committee for their useful suggestions. Finally, we thank Saron Kim and Moonhyeon Jung for their assistance in organizing FACS 2018, and acknowledge financial support from the Brain Korea 21 Plus program and the POSTECH Basic Science Research Institute.

August 2018

Kyungmin Bae  
Peter Csaba Ölveczky

# Organization

## Program Chairs

Kyungmin Bae  
Peter Csaba Ölveczky

Pohang University of Science and Technology, Korea  
University of Oslo, Norway

## Steering Committee

Farhad Arbab  
Luís Barbosa  
José Luiz Fiadeiro  
Ramtin Khosravi  
Olga Kouchnarenko  
Zhiming Liu  
Markus Lumpe  
Eric Madelaine (Chair)

CWI and Leiden University, The Netherlands  
INESC TEC and University of Minho, Portugal  
Royal Holloway, University of London, UK  
University of Tehran, Iran  
FEMTO-ST and University of Franche-Comté, France  
Southwest University, China  
Swinburne University of Technology, Australia  
Inria and University of Côte d'Azur, Sophia Antipolis,  
France

Peter Csaba Ölveczky  
José Proença

University of Oslo, Norway  
University of Minho, Portugal

## Program Committee

Farhad Arbab  
Cyrille Artho  
Kyungmin Bae  
Luís Barbosa  
Simon Bliudze  
Roberto Bruni  
Zhenbang Chen  
Yunja Choi  
José Luiz Fiadeiro  
Xudong He  
Sung-Shik Jongmans  
Yunho Kim  
Olga Kouchnarenko  
Ivan Lanese  
Axel Legay  
Shaoying Liu  
Zhiming Liu  
Markus Lumpe  
Eric Madelaine

CWI and Leiden University, The Netherlands  
KTH Royal Institute of Technology, Sweden  
Pohang University of Science and Technology, Korea  
INESC TEC and University of Minho, Portugal  
Inria Lille, France  
University of Pisa, Italy  
National University of Defense Technology, China  
Kyungpook National University, Korea  
Royal Holloway, University of London, UK  
Florida International University, USA  
The Open University, The Netherlands  
KAIST, Korea  
FEMTO-ST and University of Franche-Comté, France  
University of Bologna/Inria, Italy  
Inria Rennes, France  
Hosei University, Japan  
Southwest University, China  
Swinburne University of Technology, Australia  
Inria and University of Côte d'Azur, Sophia Antipolis,  
France

|                      |  |
|----------------------|--|
| Hernán Melgratti     | University of Buenos Aires, Argentina  |
| José Meseguer        | University of Illinois at Urbana-Champaign, USA  |
| Kazuhiro Ogata       | JAIST, Japan   |
| Peter Csaba Ölveczky | University of Oslo, Norway   |
| Catuscia Palamidessi | Inria, France  |
| José Proença         | University of Minho, Portugal  |
| Gwen Salaün          | University of Grenoble Alpes, France   |
| Francesco Santini    | University of Perugia, Italy   |
| Meng Sun             | Peking University, China   |
| Antonio Vallecillo   | University of Málaga, Spain  |
| Dániel Varró         | McGill University, Canada, and Budapest University<br>of Technology and Economics, Hungary |
| Shoji Yuen           | Nagoya University, Japan   |
| Min Zhang            | East China Normal University, China  |

## **Additional Reviewers**

|                      |                      |
|----------------------|----------------------|
| Chen, Xin            | Krishna, Ajay        |
| Chirita, Claudia     | Li, Yi               |
| Chouali, Samir       | Liu, Bo              |
| Cristescu, Ioana     | Masson, Pierre-Alain |
| Dadeau, Frederic     | Quilbeuf, Jean       |
| Koutsoukos, Giorgios | Zhang, Xiyue         |

# Formal Design, Implementation and Verification of Blockchain Languages (Abstract of Invited Paper)

Grigore Rosu<sup>1,2</sup>

<sup>1</sup> University of Illinois at Urbana-Champaign, USA  
grosu@illinois.edu  
<http://fsl.cs.illinois.edu/grosu>

<sup>2</sup> Runtime Verification, Inc., USA  
[grigore.rosu@runtimeverification.com](mailto:grigore.rosu@runtimeverification.com)

**Abstract.** Many of the recent cryptocurrency bugs and exploits are due to flaws or weaknesses of the underlying blockchain programming languages or virtual machines. The usual post-mortem approach to formal language semantics and verification, where the language is firstly implemented and used in production for many years before a need for formal semantics and verification tools naturally arises, simply does not work anymore. New blockchain languages or virtual machines are proposed at an alarming rate, followed by new versions of them every few weeks, together with programs (or smart contracts) in these languages that are responsible for financial transactions of potentially significant value. Formal analysis and verification tools are therefore needed immediately for such languages and virtual machines. We present recent academic and commercial results in developing blockchain languages and virtual machines that come directly equipped with formal analysis and verification tools. The main idea is to generate all these automatically, correct-by-construction from a formal specification. We demonstrate the feasibility of the proposed approach by applying it to two blockchains, Ethereum and Cardano.

**Keywords:** Formal verification · Formal semantics · Blockchain

## Links

Runtime Verification, Inc:

- <http://runtimeverification.com>

Smart contract verification approach and verified contracts:

- <https://runtimeverification.com/smartcontract/>
- <https://github.com/runtimeverification/verified-smart-contracts>



Formally specified, automatically generated virtual machines for the blockchain:

- EVM: <https://github.com/runtimeverification/evm-semantic>
- IELE: <https://github.com/runtimeverification/iele-semantic>

# Contents

## Invited Paper

|   |   |
|---|---|
| What Good are Models? . . . . .         | 3 |
| <i>Edward A. Lee and Marjan Sirjani</i> |   |

## Regular Papers

|  |     |
|--|-----|
| Building Correct SDN Components from a Global Event-B Formal Model. . .                            | 35  |
| <i>J. Christian Attiogbé</i>   |     |
| Event-B Formalization of a Variability-Aware Component Model<br>Patterns Framework. . . . .        | 54  |
| <i>Jean-Paul Bodeveix, Arnaud Dieumegard, and Mamoun Filali</i>                                    |     |
| A Logical Characterization of Differential Privacy via Behavioral Metrics . . .                    | 75  |
| <i>Valentina Castiglioni, Konstantinos Chatzikokolakis,<br/>and Catuscia Palamidessi</i>           |     |
| Incremental Computation of Synthesis Rules for Free-Choice Petri Nets . . . .                      | 97  |
| <i>Prabhakar M. Dixit, H. M. W. Verbeek, and Wil M. P. van der Aalst</i>                           |     |
| Programming Dynamic Reconfigurable Systems . . . . .   | 118 |
| <i>Rim El Ballouli, Saddek Bensalem, Marius Bozga, and Joseph Sifakis</i>                          |     |
| Automating Verification of State Machines with Reactive Designs<br>and Isabelle/UTP. . . . .       | 137 |
| <i>Simon Foster, James Baxter, Ana Cavalcanti, Alvaro Miyazawa,<br/>and Jim Woodcock</i>           |     |
| Using Coloured Petri Nets for Resource Analysis of Active Objects . . . . .                        | 156 |
| <i>Anastasia Gkolfi, Einar Broch Johnsen, Lars Michael Kristensen,<br/>and Ingrid Chieh Yu</i>     |     |
| Adaptive Formal Framework for WMN Routing Protocols . . . . .                                      | 175 |
| <i>Mojgan Kamali and Ansgar Fehnker</i>  |     |
| <b>IsaK-Static:</b> A Complete Static Semantics of $\mathbb{K}$ . . . . .                          | 196 |
| <i>Liyi Li and Elsa L. Gunter</i>  |     |
| Solving Parameterised Boolean Equation Systems with Infinite Data<br>Through Quotienting . . . . . | 216 |
| <i>Thomas Neele, Tim A. C. Willemse, and Jan Friso Groote</i>                                      |     |

|   |     |
|---|-----|
| Actors with Coroutine Support in Java. . . . .                            | 237 |
| <i>Vlad Serbanescu, Frank de Boer, and Mohammad Mahdi Jaghoori</i>        |     |
| Dynamic Cut-Off Algorithm for Parameterised Refinement Checking . . . . . | 256 |
| <i>Antti Siirtola and Keijo Heljanko</i>                                  |     |

**Tool Papers**

|  |     |
|--|-----|
| FACTUM Studio: A Tool for the Axiomatic Specification and Verification<br>of Architectural Design Patterns . . . . . | 279 |
| <i>Diego Marmosler and Habtom Kahsay Gidey</i>   |     |
| The SLco Framework for Verified, Model-Driven Construction of<br>Component Software . . . . .                        | 288 |
| <i>Sander de Putter, Anton Wijs, and Dan Zhang</i>   |     |
| <b>Author Index</b> . . . . .  | 297 |