# Contents

## Invited Presentations

Resource Analysis: From Sequential to Concurrent and Distributed Programs ................................................................. 3  
*Elvira Albert, Puri Arenas, Jesús Correas, Samir Genaim, Miguel Gómez-Zamalloa, Enrique Martín-Martin, Germán Pueblán Puebla, and Guillermo Román-Díez*

AVACS: Automatic Verification and Analysis of Complex Systems Highlights and Lessons Learned ................................................. 18  
*Werner Damm*

## Main Track

Automated Circular Assume-Guarantee Reasoning ...................... 23  
*Karam Abd Elkader, Orna Grumberg, Corina S. Pásáreanu, and Sharon Shoham*

Towards Formal Verification of Orchestration Computations Using the K Framework ................................................................. 40  
*Musab A. AlTurki and Omar Alzuhaibi*

Narrowing Operators on Template Abstract Domains ................... 57  
*Gianluca Amato, Simone Di Nardo Di Maio, Maria Chiara Meo, and Francesca Scozzari*

Detection of Design Flaws in the Android Permission Protocol Through Bounded Verification ......................................................... 73  
*Hamid Bagheri, Eunsuk Kang, Sam Malek, and Daniel Jackson*

Privacy by Design in Practice: Reasoning about Privacy Properties of Biometric System Architectures ........................................... 90  
*Julien Bringer, Hervé Chabanne, Daniel Le Métayer, and Roch Lescuyer*

A Specification Language for Static and Runtime Verification of Data and Control Properties ......................................................... 108  
*Wolfgang Ahrendt, Jesús Mauricio Chimento, Gordon J. Pace, and Gerardo Schneider*

Certificates for Parameterized Model Checking ............................ 126  
*Sylvain Conchon, Alain Mebsout, and Fatiha Zaïdi*
Safety, Liveness and Run-Time Refinement for Modular Process-Aware Information Systems with Dynamic Sub Processes ........................................ 143
Søren Debois, Thomas Hildebrandt, and Tijs Slaats

Verifying Opacity of a Transactional Mutex Lock ............................ 161
John Derrick, Brijesh Dongol, Gerhard Schellhorn, Oleg Travkin, and Heike Wehrheim

A Framework for Correctness Criteria on Weak Memory Models .... 178
John Derrick and Graeme Smith

Semantics-Preserving Simplification of Real-World Firewall Rule Sets ... 195
Cornelius Diekmann, Lars Hupel, and Georg Carle

Parameter Synthesis Through Temporal Logic Specifications .......... 213
Thao Dang, Tommaso Dreossi, and Carla Piazza

Trace-Length Independent Runtime Monitoring of Quantitative Policies in LTL ................................................................. 231
Xiaoning Du, Yang Liu, and Alwen Tiu

Probabilistic Bisimulation for Realistic Schedulers ......................... 248
Christian Eisentraut, Jens Chr. Godskesen, Holger Hermanns, Lei Song, and Lijun Zhang

QPMC: A Model Checker for Quantum Programs and Protocols ...... 265
Yuan Feng, Ernst Moritz Hahn, Andrea Turrini, and Lijun Zhang

Automated Verification of RPC Stub Code ................................. 273
Matthew Fernandez, June Andronick, Gerwin Klein, and Ihor Kuz

Property-Driven Fence Insertion Using Reorder Bounded Model Checking ................................................................. 291
Saurabh Joshi and Daniel Kroening

Verifying the Safety of a Flight-Critical System ............................ 308
Guillaume Brat, David Bushnell, Misty Davies, Dimitra Giannakopoulou, Falk Howar, and Temesghen Kahsai

Proving Safety with Trace Automata and Bounded Model Checking .... 325
Daniel Kroening, Matt Lewis, and Georg Weissenbacher

Verifying Parameterized Timed Security Protocols ....................... 342
Li Li, Jun Sun, Yang Liu, and Jin Song Dong

Abstraction of Elementary Hybrid Systems by Variable Transformation ................................................................. 360
Jiang Liu, Naijun Zhan, Hengjun Zhao, and Liang Zou
<table>
<thead>
<tr>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Using Real-Time Maude to Model Check Energy Consumption</td>
<td>378</td>
</tr>
<tr>
<td>Shin Nakajima</td>
<td></td>
</tr>
<tr>
<td>Static Differential Program Analysis for Software-Defined Networks</td>
<td>395</td>
</tr>
<tr>
<td>Tim Nelson, Andrew D. Ferguson, and Shriram Krishnamurthi</td>
<td></td>
</tr>
<tr>
<td>A Fully Verified Container Library</td>
<td>414</td>
</tr>
<tr>
<td>Nadia Polikarpova, Julian Tschannen, and Carlo A. Furia</td>
<td></td>
</tr>
<tr>
<td>Counterexamples for Expected Rewards</td>
<td>435</td>
</tr>
<tr>
<td>Tim Quatmann, Nils Jansen, Christian Dehnert, Ralf Wimmer, Erika Ábrahám, Joost-Pieter Katoen, and Bernd Becker</td>
<td></td>
</tr>
<tr>
<td>The Semantics of Cardinality-Based Feature Models via Formal Languages</td>
<td>453</td>
</tr>
<tr>
<td>Aliakbar Safilian, Tom Maibaum, and Zinovy Diskin</td>
<td></td>
</tr>
<tr>
<td>Axiomatization of Typed First-Order Logic</td>
<td>470</td>
</tr>
<tr>
<td>Peter H. Schmitt and Mattias Ulbrich</td>
<td></td>
</tr>
<tr>
<td>Model-Based Problem Solving for University Timetable Validation and Improvement</td>
<td>487</td>
</tr>
<tr>
<td>David Schneider, Michael Leuschel, and Tobias Witt</td>
<td></td>
</tr>
<tr>
<td>Certified Reasoning with Infinity</td>
<td>496</td>
</tr>
<tr>
<td>Asankhaya Sharma, Shengyi Wang, Andreea Costea, Aquinas Hobor, Wei-Ngan Chin</td>
<td></td>
</tr>
<tr>
<td>Direct Formal Verification of Liveness Properties in Continuous and Hybrid Dynamical Systems</td>
<td>514</td>
</tr>
<tr>
<td>Andrew Sogokon and Paul B. Jackson</td>
<td></td>
</tr>
<tr>
<td>Rigorous Estimation of Floating-Point Round-off Errors with Symbolic Taylor Expansions</td>
<td>532</td>
</tr>
<tr>
<td>Alexey Solovyev, Charles Jacobsen, Zvonimir Rakamarić, Ganesh Gopalakrishnan</td>
<td></td>
</tr>
<tr>
<td>Static Optimal Scheduling for Synchronous Data Flow Graphs with Model Checking</td>
<td>551</td>
</tr>
<tr>
<td>Xue-Yang Zhu, Rongjie Yan, Yu-Lei Gu, Jian Zhang, Wenhui Zhang, Guangquan Zhang</td>
<td></td>
</tr>
</tbody>
</table>

**Industry Track**

Eliminating Static Analysis False Positives Using Loop Abstraction and Bounded Model Checking | 573  |
| Bharti Chindyalwar, Priyanka Darke, Anooj Chavda, Sagar Vaghani, Avriti Chauhan |      |
Autofunk: An Inference-Based Formal Model Generation Framework for Production Systems ........................................... 577

William Durand and Sébastien Salva

Software Development and Authentication for Arms Control Information Barriers ............................................ 581

Neil Evans

Analyzing the Restart Behavior of Industrial Control Applications .... 585

Stefan Hauck-Stattemann, Sebastian Biallas, Bastian Schlich,
Stefan Kowalewski, and Raoul Jetley

Case Study: Static Security Analysis of the Android Goldfish Kernel ... 589

Tao Liu and Ralf Huuck


Taro Kurita, Fuyuki Ishikawa, and Keijiro Araki

Formal Virtual Modelling and Data Verification for Supervision Systems ........................................................... 597

Thierry Lecomte

Using Simulink Design Verifier for Automatic Generation of Requirements-Based Tests ........................................... 601

Bruno Miranda, Henrique Masini, and Rodrigo Reis

Formalizing the Concept Phase of Product Development ............ 605

Matthijs Schuts and Jozef Hooman

Author Index .................................................. 609
FM 2015: Formal Methods
20th International Symposium, Oslo, Norway, June
24-26, 2015, Proceedings
Bjørner, N.; de Boer, F. (Eds.)
2015, XVI, 610 p. 156 illus., Softcover
ISBN: 978-3-319-19248-2