

# Contents

## Requirements and Architectures

Temporal Logic Framework for Performance Analysis of Architectures of Systems . . . . .	3
<i>Ariane Piel, Jean Bourrely, Stéphanie Lala, Sylvain Bertrand, and Romain Kervarc</i>	
On Implementing Real-Time Specification Patterns Using Observers . . . . .	19
<i>John D. Backes, Michael W. Whalen, Andrew Gacek, and John Komp</i>	
Contract-Based Verification of Complex Time-Dependent Behaviors in Avionic Systems . . . . .	34
<i>Devesh Bhatt, Arunabh Chattopadhyay, Wenchao Li, David Oglesby, Sam Owre, and Natarajan Shankar</i>	
ARSENAL: Automatic Requirements Specification Extraction from Natural Language . . . . .	41
<i>Shalini Ghosh, Daniel Elenius, Wenchao Li, Patrick Lincoln, Natarajan Shankar, and Wilfried Steiner</i>	

## Testing and Run-Time Enforcement

Assisted Coverage Closure . . . . .	49
<i>Adam Nellis, Pascal Kesseli, Philippa Ryan Conmy, Daniel Kroening, Peter Schrammel, and Michael Tautschnig</i>	
Synthesizing Runtime Enforcer of Safety Properties Under Burst Error . . . . .	65
<i>Meng Wu, Haibo Zeng, and Chao Wang</i>	
Compositional Runtime Enforcement . . . . .	82
<i>Srinivas Pinisetty and Stavros Tripakis</i>	
Improving an Industrial Test Generation Tool Using SMT Solver . . . . .	100
<i>Hao Ren, Devesh Bhatt, and Jan Hvozdozic</i>	
The comKorat Tool: Unified Combinatorial and Constraint-Based Generation of Structurally Complex Tests . . . . .	107
<i>Hua Zhong, Lingming Zhang, and Sarfraz Khurshid</i>	

## Code Generation and Synthesis

Automated Synthesis of Safe Autonomous Vehicle Control Under Perception Uncertainty . . . . .	117
<i>Susmit Jha and Vasumathi Raman</i>	
Obfuscator Synthesis for Privacy and Utility. . . . .	133
<i>Yi-Chin Wu, Vasumathi Raman, Stéphane Lafortune, and Sanjit A. Seshia</i>	
Code Generation Using a Formal Model of Reference Counting . . . . .	150
<i>Gaspard Férey and Natarajan Shankar</i>	
EventB2Java: A Code Generator for Event-B . . . . .	166
<i>Néstor Cataño and Victor Rivera</i>	

## Applications of Formal Methods

A Formally Verified Checker of the Safe Distance Traffic Rules for Autonomous Vehicles. . . . .	175
<i>Albert Rizaldi, Fabian Immler, and Matthias Althoff</i>	
Probabilistic Formal Verification of the SATS Concept of Operation. . . . .	191
<i>Muhammad Usama Sardar, Nida Afaq, Khaza Anuarul Hoque, Taylor T. Johnson, and Osman Hasan</i>	
Formal Translation of IEC 61131-3 Function Block Diagrams to PVS with Nuclear Application . . . . .	206
<i>Josh Newell, Linna Pang, David Tremaine, Alan Wasssyng, and Mark Lawford</i>	
Formal Analysis of Extended Well-Clear Boundaries for Unmanned Aircraft . . . . .	221
<i>César Muñoz and Anthony Narkawicz</i>	
Formal Validation and Verification Framework for Model-Based and Adaptive Control Systems . . . . .	227
<i>Sergio Guarro, Umit Ozguner, Tunc Aldemir, Matt Knudson, Arda Kurt, Michael Yau, Mohammad Hejase, and Steve Kwon</i>	

## Techniques for Automated Verification

Verifying Relative Safety, Accuracy, and Termination for Program Approximations . . . . .	237
<i>Shaobo He, Shuvendu K. Lahiri, and Zvonimir Rakamarić</i>	

Bandwidth and Wavefront Reduction for Static Variable Ordering in Symbolic Reachability Analysis . . . . .	255
<i>Jeroen Meijer and Jaco van de Pol</i>	

Gray-Box Learning of Serial Compositions of Mealy Machines . . . . .	272
<i>Andreas Abel and Jan Reineke</i>	

## **Theorem Proving and Proofs**

Specification and Proof of High-Level Functional Properties of Bit-Level Programs . . . . .	291
<i>Clément Fumex, Claire Dross, Jens Gerlach, and Claude Marché</i>	

Formal Verification of an Executable LTL Model Checker with Partial Order Reduction . . . . .	307
<i>Julian Brunner and Peter Lammich</i>	

A Modular Way to Reason About Iteration . . . . .	322
<i>Jean-Christophe Filliâtre and Mário Pereira</i>	

A Proof Infrastructure for Binary Programs . . . . .	337
<i>Ashlie B. Hocking, Benjamin D. Rodes, John C. Knight, Jack W. Davidson, and Clark L. Coleman</i>	

Hierarchical Verification of Quantum Circuits. . . . .	344
<i>Sidi Mohamed Beillahi, Mohamed Yousri Mahmoud, and Sofiène Tahar</i>	

## **Correctness and Certification**

Semantics for Locking Specifications. . . . .	355
<i>Michael D. Ernst, Damiano Macedonio, Massimo Merro, and Fausto Spoto</i>	

From Design Contracts to Component Requirements Verification . . . . .	373
<i>Jing Liu, John D. Backes, Darren Cofer, and Andrew Gacek</i>	

A Hybrid Architecture for Correct-by-Construction Hybrid Planning and Control . . . . .	388
<i>Robert P. Goldman, Daniel Bryce, Michael J.S. Pelican, David J. Musliner, and Kyungmin Bae</i>	

<b>Author Index</b> . . . . .	395
-------------------------------	-----

NASA Formal Methods

8th International Symposium, NFM 2016, Minneapolis,

MN, USA, June 7-9, 2016, Proceedings

Rayadurgam, S.; Tkachuk, O. (Eds.)

2016, XIX, 396 p. 129 illus., Softcover

ISBN: 978-3-319-40647-3