Contents

Requirements and Architectures

Temporal Logic Framework for Performance Analysis of Architectures of Systems .......................................................... 3
   Ariane Piel, Jean Bourrely, Stéphanie Lala, Sylvain Bertrand,
   and Romain Kervarc

On Implementing Real-Time Specification Patterns Using Observers .... 19
   John D. Backes, Michael W. Whalen, Andrew Gacek, and John Komp

Contract-Based Verification of Complex Time-Dependent Behaviors in Avionic Systems .............................................. 34
   Devesh Bhatt, Arunabh Chattopadhyay, Wenchao Li, David Oglesby,
   Sam Owre, and Natarajan Shankar

ARSENAL: Automatic Requirements Specification Extraction from Natural Language ................................................... 41
   Shalini Ghosh, Daniel Elenius, Wenchao Li, Patrick Lincoln,
   Natarajan Shankar, and Wilfried Steiner

Testing and Run-Time Enforcement

Assisted Coverage Closure ...................................................... 49
   Adam Nellis, Pascal Kesseli, Philippa Ryan Conmy, Daniel Kroening,
   Peter Schrammel, and Michael Tautschnig

Synthesizing Runtime Enforcer of Safety Properties Under Burst Error ..... 65
   Meng Wu, Haibo Zeng, and Chao Wang

Compositional Runtime Enforcement ........................................ 82
   Srinivas Pinisetty and Stavros Tripakis

Improving an Industrial Test Generation Tool Using SMT Solver ........ 100
   Hao Ren, Devesh Bhatt, and Jan Hvozdovic

The comKorat Tool: Unified Combinatorial and Constraint-Based Generation of Structurally Complex Tests ...................... 107
   Hua Zhong, Lingming Zhang, and Sarfraz Khurshid


**Code Generation and Synthesis**

Automated Synthesis of Safe Autonomous Vehicle Control Under Perception Uncertainty ........................................ 117

*Susmit Jha and Vasumathi Raman*

Obfuscator Synthesis for Privacy and Utility ........................................ 133

*Yi-Chin Wu, Vasumathi Raman, Stéphane Lafortune, and Sanjit A. Seshia*

Code Generation Using a Formal Model of Reference Counting ........... 150

*Gaspard Férey and Natarajan Shankar*

EventB2Java: A Code Generator for Event-B ................................. 166

*Néstor Cataño and Victor Rivera*

**Applications of Formal Methods**

A Formally Verified Checker of the Safe Distance Traffic Rules for Autonomous Vehicles ........................................ 175

*Albert Rizaldi, Fabian Immler, and Matthias Althoff*

Probabilistic Formal Verification of the SATS Concept of Operation ...... 191

*Muhammad Usama Sardar, Nida Afaq, Khaza Anuarul Hoque, Taylor T. Johnson, and Osman Hasan*

Formal Translation of IEC 61131-3 Function Block Diagrams to PVS with Nuclear Application ........................................ 206

*Josh Newell, Linna Pang, David Tremaine, Alan Wassyng, and Mark Lawford*

Formal Analysis of Extended Well-Clear Boundaries for Unmanned Aircraft .......................................................... 221

*César Muñoz and Anthony Narkawicz*

Formal Validation and Verification Framework for Model-Based and Adaptive Control Systems ................................. 227

*Sergio Guarro, Umit Ozguner, Tunc Aldemir, Matt Knudson, Arda Kurt, Michael Yau, Mohammad Hejase, and Steve Kwon*

**Techniques for Automated Verification**

Verifying Relative Safety, Accuracy, and Termination for Program Approximations ................................................... 237

*Shaobo He, Shuvendu K. Lahiri, and Zvonimir Rakamarić*
Bandwidth and Wavefront Reduction for Static Variable Ordering in Symbolic Reachability Analysis ........................................ 255  
  \textit{Jeroen Meijer and Jaco van de Pol}

Gray-Box Learning of Serial Compositions of Mealy Machines .......... 272  
  \textit{Andreas Abel and Jan Reineke}

\textbf{Theorem Proving and Proofs}

Specification and Proof of High-Level Functional Properties of Bit-Level Programs ......................................................... 291  
  \textit{Clément Fumex, Claire Dross, Jens Gerlach, and Claude Marché}

Formal Verification of an Executable LTL Model Checker with Partial Order Reduction .......................................................... 307  
  \textit{Julian Brunner and Peter Lammich}

A Modular Way to Reason About Iteration ....................................... 322  
  \textit{Jean-Christophe Filliâtre and Mário Pereira}

A Proof Infrastructure for Binary Programs ...................................... 337  
  \textit{Ashlie B. Hocking, Benjamin D. Rodes, John C. Knight, Jack W. Davidson, and Clark L. Coleman}

Hierarchical Verification of Quantum Circuits. ............................... 344  
  \textit{Sidi Mohamed Beillahi, Mohamed Yousri Mahmoud, and Sofiène Tahar}

\textbf{Correctness and Certification}

Semantics for Locking Specifications. ............................................ 355  
  \textit{Michael D. Ernst, Damiano Macedonio, Massimo Merro, and Fausto Spoto}

From Design Contracts to Component Requirements Verification ............ 373  
  \textit{Jing Liu, John D. Backes, Darren Cofer, and Andrew Gacek}

A Hybrid Architecture for Correct-by-Construction Hybrid Planning and Control ................................................................. 388  
  \textit{Robert P. Goldman, Daniel Bryce, Michael J.S. Pelican, David J. Musliner, and Kyungmin Bae}

\textbf{Author Index} ................................................................. 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