ISoLA 2006
Second International Symposium on Leveraging Applications of Formal Methods, Verification and Validation

Table of Contents

Preface
Reviewers

Invited Talks

Triumphs and Challenges for Model-Oriented Formal Methods: The VDM++ Experience (Abstract) ............................................................. 1
John S. Fitzgerald and Peter Gorm Larsen

Formal Security Analysis in Industry, at the Example of Electronic Distribution of Aircraft Software (EDS) .............................................................. 5
David van Oheimb

Certificates of Resource Usage on Mobile Telephones .......................................................... 6
Thomas Jensen

Program Safety via Programmer Safety ............................................................................. 8
Joseph Kiniry

The AUTOSAR Timing Model – Status and Challenges – .................................................. 9
Kai Richter

Analysis Techniques for Service Models .......................................................................... 11
Wolfgang Reisig, Dirk Fahland, Niels Lohmann, Peter Massuthe, Christian Stahl, Daniela Weinberg, Karsten Wolf, and Kathrin Kaschner

Keynote

Software Assurance Research Infusion: The NASA Experience ........................................... 18
Michael G. Hinchey, Thomas Pressburger, Martin S. Feather, Lawrence Markosian, and Wes Deadrick
Track on Formal Methods in Avionics and Aerospace Applications

Verifying LTL Properties on Hierarchical Systems: Application to Aircraft Autopilot ........................................... Mohammed Al Achhab, Ahmed Hammad, and Hassan Mountassir .......................................................... 28

  Yamine Ait-Ameur, Alexandre Cortier, Rmi Delmas, and Virginie Wiels

Reasoning about Airport Security Regulations Using the Focal Environment ................................................. 45
  David Delahaye, Jean-Frédéric Etienne, and Véronique Viguié Donzeau-Gouge

Track on Formal Specifications in Practice

Alexander Petrenko

Concurrent Testing of Java Components Using Java PathFinder ................................................................. 53
  Vadim Mutilin

The UniTESK Approach to Specification-Based Validation of Hardware Designs ........................................... 60
  Alexander Kamkin

Combining Logic and Algebraic Techniques for Program Verification in Theorema ........................................ 67
  Laura Kovács, Nikolaj Popov, and Tudor Jebelean

Automatic Test Generation for Model-Based Code Generators ....................................................................... 75
  Sergey V. Zelenov, Denis V. Silakov, Alexander K. Petrenko, Mirko Conrad, and Ines Fey

Retrenching the Purse: Hashing Injective CLEAR Codes, and Security Properties ......................................... 82
  Richard Banach, Michael Poppleton, Czeslaw Jeske, and Susan Stepney

Formal Modelling of Dynamic Coalitions, with an Application in Chemical Engineering ............................ 91
  Jeremy W. Bryans, John S. Fitzgerald, Cliff B. Jones, and Igor Mozolevsky

Poster Session

CARVER: A Slicing Tool for Communicating Automata Specifications ........................................................... 99
  Sébastien Labbé and Arnault Lapitre

Model-Based Development of Fault-Tolerant Embedded Software .......................................................... 103
  Christian Buckl, Alois Knoll, and Gerhard Schrott

A Formal Specification of a Programming Language: Design of Pit .......................................................... 111
  Leif Pedersen and Hassan Reza
Track on Safety and Security
Anindya Banerjee, Gilles Barthe, John Hatcliff, Joe Kiniry and Jens Krinke

Intransitive Noninterference in Dependence Graphs................................................................. 119
Christian Hammer, Jens Krinke, and Frank Noda

Formally Proved Anti-tearing Properties of Embedded C Code...................................................... 129
June Andronick

Kiasan: A Verification and Test-Case Generation Framework for Java Based
on Symbolic Execution.................................................................................................................. 137
Xianghua Deng, Robby, and John Hatcliff

Extending Source Code Generators for Evidence-Based Software Certification .............................. 138
Ewen Denney and Bernd Fischer

Track on Evolutionary Computing Applied to Engineering
Ibrahim Esat

Application of Bioinformatics in the Design of Gene Expression Microarrays.................................. 146
Sabah Khalid, Mohsin Khan, Ping Wang, Xiaohui Liu, and Su-Ling Li

A Novel Method for Obtaining Real Time Control Strategy Using GA for Dynamical
Systems Subjected to External Arbitrary Excitations...................................................................... 161
M. Saud and I. I. Esat

Real-Coded Quantum Inspired Evolution Algorithm Applied to Engineering
Optimization Problems .................................................................................................................. 169
F. S. Alfares and I. I. Esat

Track on Organic Computing
Wolfgang Reif

Safety and Dependability Analysis of Self-Adaptive Systems......................................................... 177
Matthias Güdemann, Frank Ortmeier, and Wolfgang Reif

Organic Computing – Addressing Complexity by Controlled Self-Organization.......................... 185
Jürgen Branke, Moez Mnif, Christian Müller-Schloer, Holger Prothmann,
Urban Richter, Fabian Rochner, and Hartmut Schmeck

Real-Time Property Verification in Organic Computing Systems.................................................. 192
Steffen Stein, Arne Hamann, and Rolf Ernst

Recognizing Traffic Jams with Hovering Data Clouds.................................................................... 198
Sándor P. Fekete, Christiane Schmidt, Axel Wegener, and Stefan Fischer
Track on Timing Analysis in the Industrial Development Process
Reinhard Wilhelm, Joern Schneider and Jean Souyris

Cost-Efficient Worst-Case Execution Time Analysis in Industrial Practice .......................................................... 204
Jan Staschulat, Jörn C. Braam, Rolf Ernst, Thomas Rambow, and Rainer Schlör Rainer Busch

Static WCET Analysis of Real-Time Task-Oriented Code in Vehicle Control Systems ........................................ 212
Daniel Sehlberg, Andreas Ermedahl, Jan Gustafsson, Björn Lisper, and Steffen Wiegartz

Towards an Integration of Low-Level Timing Analysis and Model-Based Code Generation ......................... 220
Christian Ferdinand, Reinhold Heckmann, Hans-Jörg Wolff, Christian Renz, Manabendra Gupta, and Oleg Parshin

Challenges of Timing Verification Tools in the Automotive Domain ............................................................. 227
Pascal Montag, Steffen Görzig, and Paul Levi

The Worst Case Execution Time Tool Challenge 2006 .................................................................................. 233
Jan Gustafsson

The Worst Case Execution Time Tool Challenge 2006: The External Test .................................................. 241
Lili Tan

Track on Formal Approaches to the Specification and Verification of Sensor Networks
Allice Miller and Paolo Ballarini

Model Checking Techniques for the Performance Analysis of Delay Tolerant Networks with On-off Behavior .......................................................... 249
Michele Garetto and Marco Gribaudo

Model Checking Medium Access Control for Sensor Networks ................................................................. 255
Paolo Ballarini and Alice Miller

Formal Techniques for the Analysis of Wireless Networks ........................................................................... 263
A. K. McIver and A. Fehnker

Modeling of Sensor Networks Using XRM ................................................................................................. 271
Akim Demaille, Sylvain Peyronnet, and Benoît Sigoure

"Towards a Trusted Compiler for a Query Language for Wireless Sensor Networks." ................................ 277

A Space and Time Requirements Logic for Sensor Networks ...................................................................... 283
Rachel Cardell-Oliver, Mark Reynolds, and Mark Kranz

Probabilistic Model Checking of Contention Resolution in the IEEE 802.15.4 Low-Rate Wireless Personal Area Network Protocol .......................................................... 290
Matthias Fruth
Track on Biologically-Inspired Computing
Michael G. Hinchey and Roy Sterritt

Formal Executable Models of Cell Signaling Primitives
Carolyn Talcott

Biological LC/MS Preprocessing and Analysis with jABC, jETI and xcms
Christian Kubczak, Tiziana Margaria, Arno Fritsch, and Bernhard Steffen

Track on Applications of Rigorous and Formal Methods to Service-Oriented Computing
Bernd Kramer, Schahram Dustdar, and Heiko Ludwig

Foundations for Web Services Orchestrations: Functional and QoS Aspects, Jointly
Sidney Rosario, Albert Benveniste, Stefan Haar, and Claude Jard

Service Based Enabling Service Availability in the MaTRICS: A Model-Driven Approach
Markus Bajohr, Tiziana Margaria, and Bernhard Steffen

Web Services for the Integration of XML-Based Content into Learning Platforms:
A Three-level Model
Reinhold Kröger, Ulrike Lucke, Markus Schmid, and Djamshid Tavangarian

Semi-automated Workflow Synthesis
Abilio Fernandes, Karin K. Breitman, Tatiana A. S. C. Vieira, Marco A. Casanova, and Antonio L. Furtado

Track on Highly Reliable Software: Theories, Methods, Tools and Experiences in China and South Africa
He Jifeng, Xuandong Li and Zhiming Liu

Context Awareness Systems Design and Reasoning
Jin Song Dong, Yuzhang Feng, Jing Sun, and Jun Sun

REDLIB for the Formal Verification of Embedded Systems
Farn Wang

Synthesis and Traceability of Scenario-Based Executable Models
Ankit Goel and Abhik Roychoudhury

Towards a Framework for Scalable Model Checking of Concurrent C Programs
Ji Wang, Xiaodong Yi, and Xuejun Yang

Patterns with Algebraic Properties in BPEL
Geguang Pu, Huibiao Zhu, Jifeng He, Zongyan Qiu, Hongli Yang, and Xiangpeng Zhao

Harnessing Theories for Tool Support
Zhiming Liu, Vladimir Mencl, Anders P. Ravn, and Lu Yang

Connecting Algebraic and Logical Descriptions of Concurrent Systems
Naijun Zhan
Improve Model Checking Efficiency Using Specific Knowledge about the System ........................................ 392

Jianhua Zhao, Bin Lei, Xuandong Li, and Guoliang Zheng

**Thematic Session on FMICS: Formal Methods for Industrial Critical Systems**

Pedro Merino

An SDL Implementation of the UMTS Radio Resource Control Protocol Oriented to Conformance Testing ................................................................. 397

José M. Álvarez, Pedro de la Cámara, Jesús Martínez, Pedro Merino, Francisco C. Pérez, and Victoria Morillo

The FMICS-jETI Platform: Status and Perspectives ........................................................................................................ 402

Tiziana Margaria, Christian Kubczak, Bernhard Steffen, and Stefan Naujokat

**Thematic Session on Validation and Verification in the Large**

Jens Knoop

Verification in the Large via Symbolic Approximation .................................................................................. 408

Peter T. Breuer and Simon Pickin

Implementing Influence Analysis Using Parameterised Boolean Equation Systems ................................... 416

María del Mar Gallardo, Christophe Joubert, and Pedro Merino

Formal Verification of Consistency in Model-Driven Development of Distributed Communicating Systems and Communication Protocols ........................................................................ 425

Dubravka Ilić, Elena Troubitsyna, Linas Laibinis, and Sari Leppänen

Comparative Analysis of Tools for Automated Software Re-engineering Purposes ..................................... 433

Christian Wagner, Tiziana Margaria, and Hans-Georg Pagendarm

**Session on System Modelling and Verification**

A Formal Behavioral Semantics for TestML .................................................................................................. 441

Jürgen Grossmann and Wolfgang Müller

An Automated Approach for Writing Alloy Specifications Using Instances ............................................. 449

Sarfraz Khurshid, Muhammad Zubair Malik, and Engin Uzuncaova

Noise Makers Need to Know Where to be Silent – Producing Schedules That Find Bugs ...................... 458

Yosi Ben-Asher, Yaniv Eytani, Eitan Farchi, and Shmuel Ur

[mc]square: A Model Checker for Microcontroller Code ............................................................................. 466

Bastian Schlich and Stefan Kowalewski

Author Index.