

Proceedings

ISoLA 2006

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

15-19 November 2006
Paphos, Cyprus

Sponsored by



ATHK
CYTA



Los Alamitos, California
Washington • Tokyo



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
<i>John S. Fitzgerald and Peter Gorm Larsen</i>	
Formal Security Analysis in Industry, at the Example of Electronic Distribution of Aircraft Software (EDS)	5
<i>David van Oheimb</i>	
Certificates of Resource Usage on Mobile Telephones	6
<i>Thomas Jensen</i>	
Program Safety via Programmer Safety	8
<i>Joseph Kiniry</i>	
The AUTOSAR Timing Model – Status and Challenges –	9
<i>Kai Richter</i>	
Analysis Techniques for Service Models	11
<i>Wolfgang Reisig, Dirk Fahland, Niels Lohmann, Peter Massuthe, Christian Stahl, Daniela Weinberg, Karsten Wolf, and Kathrin Kaschner</i>	

Keynote

Software Assurance Research Infusion: The NASA Experience	18
<i>Michael G. Hinchey, Thomas Pressburger, Martin S. Feather, Lawrence Markosian, and Wes Deadrick</i>	

Track on Formal Methods in Avionics and Aerospace Applications

Verifying LTL Properties on Hierarchical Systems: Application to Aircraft Autopilot	28
<i>Mohammed Al Achhab, Ahmed Hammad, and Hassan Mountassir</i>	
Formal Modelling of Avionics Systems. An Approach Based on Category Theory and the EXPRESS Modelling Language.....	36
<i>Yamine Ait-Ameur, Alexandre Cortier, Rmi Delmas, and Virginie Wiels</i>	
Reasoning about Airport Security Regulations Using the Focal Environment	45
<i>David Delahaye, Jean-Frédéric Étienne, and Véronique Viguié Donzeau-Gouge</i>	

Track on Formal Specifications in Practice Alexander Petrenko

Concurrent Testing of Java Components Using Java PathFinder.....	53
<i>Vadim Mutilin</i>	
The UniTESK Approach to Specification-Based Validation of Hardware Designs	60
<i>Alexander Kamkin</i>	
Combining Logic and Algebraic Techniques for Program Verification in <i>Theorema</i>	67
<i>Laura Kovács, Nikolaj Popov, and Tudor Jebelean</i>	
Automatic Test Generation for Model-Based Code Generators.....	75
<i>Sergey V. Zelenov, Denis V. Silakov, Alexander K. Petrenko, Mirko Conrad, and Ines Fey</i>	
Retrenching the Purse: Hashing Injective CLEAR Codes, and Security Properties	82
<i>Richard Banach, Michael Poppleton, Czeslaw Jeske, and Susan Stepney</i>	
Formal Modelling of Dynamic Coalitions, with an Application in Chemical Engineering	91
<i>Jeremy W. Bryans, John S. Fitzgerald, Cliff B. Jones, and Igor Mozolevsky</i>	

Poster Session

CARVER: A Slicing Tool for Communicating Automata Specifications.....	99
<i>Sébastien Labbé and Arnault Lapitre</i>	
Model-Based Development of Fault-Tolerant Embedded Software.....	103
<i>Christian Buckl, Alois Knoll, and Gerhard Schrott</i>	
A Formal Specification of a Programming Language: Design of Pit	111
<i>Leif Pedersen and Hassan Reza</i>	

Track on Safety and Security
Anindya Banerjee, Gilles Barthe, John Hatcliff, Joe Kiniry
and Jens Krinke

Intransitive Noninterference in Dependence Graphs.....	119
<i>Christian Hammer, Jens Krinke, and Frank Nodes</i>	
Formally Proved Anti-tearing Properties of Embedded C Code.....	129
<i>June Andronick</i>	
Kiasan: A Verification and Test-Case Generation Framework for Java Based on Symbolic Execution.....	137
<i>Xianghua Deng, Robby, and John Hatcliff</i>	
Extending Source Code Generators for Evidence-Based Software Certification	138
<i>Ewen Denney and Bernd Fischer</i>	

Track on Evolutionary Computing Applied to Engineering
Ibrahim Esat

Application of Bioinformatics in the Design of Gene Expression Microarrays.....	146
<i>Sabah Khalid, Mohsin Khan, Ping Wang, Xiaohui Liu, and Su-Ling Li</i>	
A Novel Method for Obtaining Real Time Control Strategy Using GA for Dynamical Systems Subjected to External Arbitrary Excitations.....	161
<i>M. Saud and I. I. Esat</i>	
Real-Coded Quantum Inspired Evolution Algorithm Applied to Engineering Optimization Problems	169
<i>F. S. Alfares and I. I. Esat</i>	

Track on Organic Computing
Wolfgang Reif

Safety and Dependability Analysis of Self-Adaptive Systems.....	177
<i>Matthias Gdemann, Frank Ortmeier, and Wolfgang Reif</i>	
Organic Computing – Addressing Complexity by Controlled Self-Organization.....	185
<i>Jrgen Branke, Moez Mnif, Christian Mller-Schloer, Holger Prothmann, Urban Richter, Fabian Rochner, and Hartmut Schmeck</i>	
Real-Time Property Verification in Organic Computing Systems	192
<i>Steffen Stein, Arne Hamann, and Rolf Ernst</i>	
Recognizing Traffic Jams with Hovering Data Clouds.....	198
<i>Sndor P. Fekete, Christiane Schmidt, Axel Wegener, and Stefan Fischer</i>	

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
<i>Jan Staschulat, Jörn C. Braam, Rolf Ernst, Thomas Rambow, and Rainer Schlör Rainer Busch</i>	
Static WCET Analysis of Real-Time Task-Oriented Code in Vehicle Control Systems	212
<i>Daniel Sehlberg, Andreas Ermedahl, Jan Gustafsson, Björn Lisper, and Steffen Wiegratz</i>	
Towards an Integration of Low-Level Timing Analysis and Model-Based Code Generation.....	220
<i>Christian Ferdinand, Reinhold Heckmann, Hans-Jörg Wolff, Christian Renz, Manabendra Gupta, and Oleg Parshin</i>	
Challenges of Timing Verification Tools in the Automotive Domain	227
<i>Pascal Montag, Steffen Görzig, and Paul Levi</i>	
The Worst Case Execution Time Tool Challenge 2006	233
<i>Jan Gustafsson</i>	
The Worst Case Execution Time Tool Challenge 2006: The External Test	241
<i>Lili Tan</i>	

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

Model Checking Techniques for the Performance Analysis of Delay Tolerant Networks with On-off Behavior	249
<i>Michele Garetto and Marco Gribaudo</i>	
Model Checking Medium Access Control for Sensor Networks.....	255
<i>Paolo Ballarini and Alice Miller</i>	
Formal Techniques for the Analysis of Wireless Networks	263
<i>A. K. McIver and A. Fehnker</i>	
Modeling of Sensor Networks Using XRM	271
<i>Akim Demaille, Sylvain Peyronnet, and Benoît Sigoure</i>	
“Towards a Trusted Compiler for a Query Language for Wireless Sensor Networks.”	277
<i>T. E. Daniel, S. N. I. Mount, R. M. Newman, and E. I. Gaura</i>	
A Space and Time Requirements Logic for Sensor Networks	283
<i>Rachel Cardell-Oliver, Mark Reynolds, and Mark Kranz</i>	
Probabilistic Model Checking of Contention Resolution in the IEEE 802.15.4 Low-Rate Wireless Personal Area Network Protocol.....	290
<i>Matthias Fruth</i>	

Track on Biologically-Inspired Computing **Michael G. Hinchey and Roy Sterritt**

Formal Executable Models of Cell Signaling Primitives.....	298
<i>Carolyn Talcott</i>	
Biological LC/MS Preprocessing and Analysis with jABC, jETI and xcms	303
<i>Christian Kubczak, Tiziana Margaria, Arno Fritsch, and Bernhard Steffen</i>	

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.....	309
<i>Sidney Rosario, Albert Benveniste, Stefan Haar, and Claude Jard</i>	
Service Based Enabling Service Availability in the MaTRICS: A Model-Driven Approach	317
<i>Markus Bajohr, Tiziana Margaria, and Bernhard Steffen</i>	
Web Services for the Integration of XML-Based Content into Learning Platforms: A Three-level Model	325
<i>Reinhold Kröger, Ulrike Lucke, Markus Schmid, and Djamshid Tavangarian</i>	
Semi-automated Workflow Synthesis	332
<i>Abilio Fernandes, Karin K. Breitman, Tatiana A. S. C. Vieira, Marco A. Casanova, and Antonio L. Furtado</i>	

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	335
<i>Jin Song Dong, Yuzhang Feng, Jing Sun, and Jun Sun</i>	
REDLIB for the Formal Verification of Embedded Systems	341
<i>Farn Wang</i>	
Synthesis and Traceability of Scenario-Based Executable Models.....	347
<i>Ankit Goel and Abhik Roychoudhury</i>	
Towards a Framework for Scalable Model Checking of Concurrent C Programs	355
<i>Ji Wang, Xiaodong Yi, and Xuejun Yang</i>	
Patterns with Algebraic Properties in BPELO	363
<i>Geguang Pu, Huibiao Zhu, Jifeng He, Zongyan Qiu, Hongli Yang, and Xiangpeng Zhao</i>	
Harnessing Theories for Tool Support	371
<i>Zhiming Liu, Vladimir Mencl, Anders P. Ravn, and Lu Yang</i>	
Connecting Algebraic and Logical Descriptions of Concurrent Systems.....	383
<i>Naijun Zhan</i>	

Improve Model Checking Efficiency Using Specific Knowledge about the System	392
<i>Jianhua Zhao, Bin Lei, Xuandong Li, and Guoliang Zheng</i>	

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
<i>José M. Álvarez, Pedro de la Cámara, Jesús Martínez, Pedro Merino, Francisco C. Pérez, and Victoria Morillo</i>	
The FMICS-jETI Platform: Status and Perspectives.....	402
<i>Tiziana Margaria, Christian Kubczak, Bernhard Steffen, and Stefan Naujokat</i>	

Thematic Session on Validation and Verification in the Large

Jens Knoop

Verification in the Large via Symbolic Approximation.....	408
<i>Peter T. Breuer and Simon Pickin</i>	
Implementing Influence Analysis Using Parameterised Boolean Equation Systems.....	416
<i>María del Mar Gallardo, Christophe Joubert, and Pedro Merino</i>	
Formal Verification of Consistency in Model-Driven Development of Distributed Communicating Systems and Communication Protocols.....	425
<i>Dubravka Ilić, Elena Troubitsyna, Linas Laibinis, and Sari Leppänen</i>	
Comparative Analysis of Tools for Automated Software Re-engineering Purposes	433
<i>Christian Wagner, Tiziana Margaria, and Hans-Georg Pagendam</i>	

Session on System Modelling and Verification

A Formal Behavioral Semantics for TestML.....	441
<i>Jürgen Grossmann and Wolfgang Müller</i>	
An Automated Approach for Writing Alloy Specifications Using Instances	449
<i>Sarfraz Khurshid, Muhammad Zubair Malik, and Engin Uzuncaova</i>	
Noise Makers Need to Know Where to be Silent – Producing Schedules That Find Bugs	458
<i>Yosi Ben-Asher, Yaniv Eytani, Eitan Farchi, and Shmuel Ur</i>	
[mc]square: A Model Checker for Microcontroller Code	466
<i>Bastian Schlich and Stefan Kowalewski</i>	

Author Index