Table of Contents

Invited Talk

The Embedded Systems Design Challenge .............................................. 1
  *Thomas A. Henzinger, Joseph Sifakis*

Interactive Verification

The Mondex Challenge: Machine Checked Proofs for an Electronic Purse ............................... 16
  *Gerhard Schellhorn, Holger Grandy, Dominik Haneberg, Wolfgang Reif*

Interactive Verification of Medical Guidelines .................................. 32
  *Jonathan Schmitt, Alwin Hoffmann, Michael Balser, Wolfgang Reif, Mar Marcos*

Certifying Airport Security Regulations Using the Focal Environment .......... 48
  *David Delahaye, Jean-Frédéric Étienne, Véronique Viguié Donzeau-Gouge*

Proving Safety Properties of an Aircraft Landing Protocol Using I/O Automata and the PVS Theorem Prover: A Case Study ......................... 64
  *Shinya Umeno, Nancy Lynch*

Invited Talk

Validating the Microsoft Hypervisor .............................................. 81
  *Ernie Cohen*

Formal Modelling of Systems

Interface Input/Output Automata .................................................. 82
  *Kim G. Larsen, Ulrik Nyman, Andrzej Wąsowski*

Properties of Behavioural Model Merging ..................................... 98
  *Greg Brunet, Marsha Chechik, Sebastian Uchitel*

Automatic Translation from Circus to Java .................................. 115
  *Angela Freitas, Ana Lucia Caneca Cavalcanti*

Quantitative Refinement and Model Checking for the Analysis of Probabilistic Systems .................. 131
  *Annabelle K. McIver*
Real Time

Modeling and Validating Distributed Embedded Real-Time Systems
with VDM++ ............................................. 147
   Marcel Verhoef, Peter Gorm Larsen, Jozef Hoorn

Towards Modularized Verification of Distributed Time-Triggered
Systems .................................................. 163
   Jewgenij Botaschanjan, Alexander Gruler, Alexander Harhurin,
   Leonid Kof, Maria Spichkova, David Trachtenherz

Industrial Experience

A Story About Formal Methods Adoption by a Railway Signaling
Manufacturer ............................................. 179
   Stefano Bacherini, Alessandro Fantechi, Matteo Tempestini,
   Niccolò Zingoni

Partially Introducing Formal Methods into Object-Oriented
Development: Case Studies Using a Metrics-Driven Approach ............ 190
   Yujun Zheng, Jinquan Wang, Kan Wang, Jinyun Xue

Specification and Refinement

Compositional Class Refinement in Object-Z .......................... 205
   Tim McComb, Graeme Smith

A Proposal for Records in Event-B .................................. 221
   Neil Evans, Michael Butler

Pointfree Factorization of Operation Refinement ......................... 236
   José Nuno Oliveira, César Jesus Rodrigues

A Formal Template Language Enabling Metaproof ........................ 252
   Nuno Amâlio, Susan Stepney, Fiona Polack

Programming Languages

Dynamic Frames: Support for Framing, Dependencies and Sharing
Without Restrictions (Best Paper) ................................... 268
   Ioannis T. Kassios

Type-Safe Two-Level Data Transformation ............................. 284
   Alcino Cunha, José Nuno Oliveira, Joost Visser
# Algebra

**Feature Algebra** .................................................. 300  
*Peter Höfner, Ridha Khedri, Bernhard Möller*

# Education

**Using Domain-Independent Problems for Introducing Formal Methods** .................................................. 316  
*Raymond Boute*

# Formal Modelling of Systems

**Compositional Binding in Network Domains** .................................................. 332  
*Pamela Zave*

**Formal Modeling of Communication Protocols by Graph Transformation** .................................................. 348  
*Zarrin Langari, Richard Trefler*

**Feature Specification and Static Analysis for Interaction Resolution** .................................................. 364  
*Marc Aiguier, Karim Berkani, Pascale Le Gall*

**A Fully General Operational Semantics for UML 2.0 Sequence Diagrams with Potential and Mandatory Choice** .................................................. 380  
*Mass Soldal Lund, Ketil Stølen*

# Formal Aspects of Java

**Towards Automatic Exception Safety Verification** .................................................. 396  
*Xin Li, H. James Hoover, Piotr Rudnicki*

**Efficient Failure Injection** .................................................. 412  
*Cyrille Valentin Artho, Armin Biere, Shinichi Honiden*

**Automated Boundary Test Generation from JML Specifications** .................................................. 428  
*Fabrice Bouquet, Frédéric Dadeau, Bruno Legeard*

**Formal Reasoning About Non-atomic JAVA CARD Methods in Dynamic Logic** .................................................. 444  
*Wojciech Mostowski*

# Programming Languages

**Formal Verification of a C Compiler Front-End** .................................................. 460  
*Sandrine Blazy, Zaynah Dargaye, Xavier Leroy*
A Memory Model Sensitive Checker for C#
   Thuan Quang Huynh, Abhik Roychoudhury

Changing Programs Correctly: Refactoring with Specifications
   Fabian Bannwart, Peter Müller

Mechanical Verification of Recursive Procedures Manipulating Pointers
Using Separation Logic
   Viorel Preoteasa

Model Checking

Model-Based Variable and Transition Orderings for Efficient Symbolic
Model Checking
   Wendy Johnston, Kirsten Winter, Lionel van den Berg,
   Paul Stooper, Peter Robinson

Exact and Approximate Strategies for Symmetry Reduction in Model
Checking
   Alastair F. Donaldson, Alice Miller

Monitoring Distributed Controllers: When an Efficient LTL Algorithm
on Sequences is Needed to Model-Check Traces
   Alexandre Genon, Thierry Massart, Cédric Meuter

PSL Model Checking and Run-Time Verification Via Testers
   Amir Pnueli, Aleksandr Zaks

Industry Day: Abstracts of Invited Talks

Formal Methods for Security: Lightweight Plug-In or New Engineering
Discipline
   Werner Stephan

in an Expanding Niche
   David von Oheimb

Connector-Based Software Development: Deriving Secure Protocols
   Dusko Pavlovic

Model-Based Security Engineering for Real
   Jan Jürjens

Cost Effective Software Engineering for Security
   D. Randolph Johnson

Formal Methods and Cryptography
   Michael Backes, Birgit Pfitzmann, Michael Waidner
Verified Software Grand Challenge .......................... 617
Jim Woodcock

Author Index ......................................................... 619