Proceedings

Fifth IEEE International Conference on Software Engineering and Formal Methods

SEFM 2007

London, England
10-14 September 2007

Sponsored by

Los Alamitos, California
Washington • Tokyo
# Table of Contents

**Fifth IEEE International Conference on Software Engineering and Formal Methods**

**SEFM 2007**

<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Preface</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Committees</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Reviewers</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Keynote Talk</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Specializing in Software Engineering</td>
<td></td>
<td>3</td>
</tr>
<tr>
<td>Michael Jackson, The Open University</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SE 1</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verification of C Programs Using Automated Reasoning</td>
<td></td>
<td>7</td>
</tr>
<tr>
<td>David Crocker and Judith Carlton</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Problem Oriented Software Engineering: A Design-Theoretic Framework for Software Engineering</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>Jon G. Hall, Lucia Rapanotti, and Michael Jackson</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Formalising Design Patterns in Predicate Logic</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>Ian Bayley and Hong Zhu</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Mondex/VSI Challenge</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Retrenchment and the Atomicity Pattern</td>
<td></td>
<td>29</td>
</tr>
<tr>
<td>Richard Banach, Czeslaw Jeske, Anthony Hall, and Susan Stepney</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verifying the Mondex Case Study</td>
<td></td>
<td>39</td>
</tr>
<tr>
<td>Peter H. Schmitt and Isabel Tonin</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Applications</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Model-Driven Architecture for Cancer research</td>
<td></td>
<td>51</td>
</tr>
<tr>
<td>Radu Calinescu, Steve Harris, Jeremy Gibbons, Jim Davies, Igor Toujilov, and Sylvia B. Nagl</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modeling and Verification of TTCAN Startup Protocol Using Synchronous Calendar</td>
<td>61</td>
<td></td>
</tr>
<tr>
<td>Indranil Saha, Suman Roy, and Kuntal Chakraborty</td>
<td></td>
<td></td>
</tr>
<tr>
<td>How to Test Program Generators? A Case Study Using flex</td>
<td>72</td>
<td></td>
</tr>
<tr>
<td>Prahladavaradan Sampath, A.C. Rajeev, K.C. Shashidhar, and S. Ramesh</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

v
Reasoning
Proving Termination by Divergence
Domagoj Babić, Alan J. Hu, Zvonimir Rakamarić, and Byron Cook 85
Supporting Proof in a Reactive Development Environment
Farhad Mehta 95
Sound Reasoning about Unchecked Exceptions
Bart Jacobs, Peter Müller, and Frank Piessens 105
Reasoning about Linear Systems
Rob Arthan, Ursula Martin, Erik Arne Mathiesen, and Paulo Oliva 115

Keynote Talk
The Role of Abstract Interpretation in Formal Methods
Patrick Cousot, ENS 127

Logics
A Dynamic Logic for Deductive Verification of Concurrent Programs
Bernhard Beckert and Vladimir Klebanov 141
An Ought-to-Do Deontic Logic for Reasoning about Fault-Tolerance: The Diarrheic Philosophers
Pablo F. Castro and Tom S.E. Maibaum 151
An Integrated Specification Framework for Embedded Systems
Marius C. Bujorianu and Manuela L. Bujorianu 161

Semantics
A Thread-Tag Based Semantics for Sequence Diagrams
Haitao Dan, Robert M. Hierons, and Steve Counsell 173
\(\lambda_{\text{AOP}}\): An AOP Extended Lambda-Calculus
Dima Alhadidi, Nadia Belblidia, Mourad Debbabi, and Prabir Bhattacharya 183

Telecommunications
Holger Grandy, Robert Bertossi, Kurt Stenzel, and Wolfgang Reif 195
Recovery from DoS Attacks in MIPv6: Modeling and Validation
Manish Kumar C. and K. Gopinath 205
Protocol Conformance Testing a SIP Registrar: An Industrial Application of Formal Methods
Bernhard K. Aichernig, Bernhard Peischl, Martin Weiglhofer, and Franz Wotawa 215
Testing and Model Checking

Testing Conformance on Stochastic Stream X-Machines
Mercedes G. Merayo and Manuel Núñez

Specification-Based Testing for Refinement
Temesghen Kahsai, Markus Roggenbach, and Bernd-Holger Schlingloff

Hardness for Explicit State Software Model Checking Benchmarks
Neha Rungta and Eric G. Mercer

Model Checking RAISE Applicative Specifications
Juan Ignacio Perna and Chris George

Keynote Talk

Automatically Proving Concurrent Programs Correct
Byron Cook, Microsoft

SE II

Towards A Case-Optimal Symbolic Execution Algorithm for Analyzing Strong Properties of Object-Oriented Programs
Xianghua Deng, Robby, and John Hatcliff

Verification of Object Relational Maps
Krishna K. Mehra, Sriram K. Rajamani, A. Prasad Sistla, and Sumit K. Jha

Formal Specification Using Interaction Diagrams
Kevin Lano

Services

Disciplining Orchestration and Conversation in Service-Oriented Computing
Ivan Lanese, Vasco T. Vasconcelos, Francisco Martins, and António Ravara

Algebraic Approach to Linking the Semantics of Web Services
Huibiao Zhu, Jifeng He, Jing Li, and Jonathan P. Bowen

Security and Safety

Formal Verification of tamper-evident Storage for e-Voting
Dominique Cansell, J. Paul Gibson, and Dominique Méry

A Scalable Lock-Free Stack Algorithm and its Verification
Robert Colvin and Lindsay Groves

Verifying Security Properties of Cryptoprotocols: A Novel Approach
Mohamed Saleh and Mourad Debbabi
Specification and Verification

Configurable Proof Obligations in the Frog Toolkit
Simon Fraser and Richard Banach

Feature Refinement
David Streader and Steve Reeves

Run-Time Composition and Adaptation of Mismatching Behavioural Transactions
Javier Cámara, Gwen Salaün, and Carlos Canal

Flexible Behavioural Compatibility and Substitutability for Component Protocols:
A Formal Specification
Nabil Hameurlain

Author Index