

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

Preface	_____
Committees	_____
Reviewers	_____

Keynote Talk

Specializing in Software Engineering _____	3
<i>Michael Jackson, The Open University</i>	

SE 1

Verification of C Programs Using Automated Reasoning _____	7
<i>David Crocker and Judith Carlton</i>	
Problem Oriented Software Engineering: A Design-Theoretic Framework for Software Engineering _____	15
<i>Jon G. Hall, Lucia Rapanotti, and Michael Jackson</i>	
Formalising Design Patterns in Predicate Logic _____	25
<i>Ian Bayley and Hong Zhu</i>	

Mondex/VSI Challenge

Retrenchment and the Atomicity Pattern _____	29
<i>Richard Banach, Czeslaw Jeske, Anthony Hall, and Susan Stepney</i>	
Verifying the Mondex Case Study _____	39
<i>Peter H. Schmitt and Isabel Tonin</i>	

Applications

Model-Driven Architecture for Cancer research _____	51
<i>Radu Calinescu, Steve Harris, Jeremy Gibbons, Jim Davies, Igor Toujilov, and Sylvia B. Nagl</i>	
Modeling and Verification of TTCAN Startup Protocol Using Synchronous Calendar _____	61
<i>Indranil Saha, Suman Roy, and Kuntal Chakraborty</i>	
How to Test Program Generators? A Case Study Using flex _____	72
<i>Prahladavaradan Sampath, A.C. Rajeev, K.C. Shashidhar, and S. Ramesh</i>	

Reasoning

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

Keynote Talk

The Role of Abstract Interpretation in Formal Methods	127
<i>Patrick Cousot, ENS</i>	

Logics

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

Semantics

A Thread-Tag Based Semantics for Sequence Diagrams	173
<i>Haitao Dan, Robert M. Hierons, and Steve Counsell</i>	
λ _AOP: An AOP Extended Lambda-Calculus	183
<i>Dima Alhadidi, Nadia Belblidia, Mourad Debbabi, and Prabir Bhattacharya</i>	

Telecommunications

ASN1-light: A Verified Message Encoding for Security Protocols	195
<i>Holger Grandy, Robert Bertossi, Kurt Stenzel, and Wolfgang Reif</i>	
Recovery from DoS Attacks in MIPv6: Modeling and Validation	205
<i>Manish Kumar C. and K. Gopinath</i>	
Protocol Conformance Testing a SIP Registrar: An Industrial Application of Formal Methods	215
<i>Bernhard K. Aichernig, Bernhard Peischl, Martin Weiglhofer, and Franz Wotawa</i>	

Testing and Model Checking

Testing Conformance on Stochastic Stream X-Machines _____	227
<i>Mercedes G. Merayo and Manuel Núñez</i>	
Specification-Based Testing for Refinement _____	237
<i>Temesghen Kahsai, Markus Roggenbach, and Bernd-Holger Schlingloff</i>	
Hardness for Explicit State Software Model Checking Benchmarks _____	247
<i>Neha Rungta and Eric G. Mercer</i>	
Model Checking RAISE Applicative Specifications _____	257
<i>Juan Ignacio Perna and Chris George</i>	

Keynote Talk

Automatically Proving Concurrent Programs Correct _____	269
<i>Byron Cook, Microsoft</i>	

SE II

Towards A Case-Optimal Symbolic Execution Algorithm for Analyzing Strong Properties of Object-Oriented Programs _____	273
<i>Xianghua Deng, Robby, and John Hatcliff</i>	
Verification of Object Relational Maps _____	283
<i>Krishna K. Mehra, Sriram K. Rajamani, A. Prasad Sistla, and Sumit K. Jha</i>	
Formal Specification Using Interaction Diagrams _____	293
<i>Kevin Lano</i>	

Services

Disciplining Orchestration and Conversation in Service-Oriented Computing _____	305
<i>Ivan Lanese, Vasco T. Vasconcelos, Francisco Martins, and António Ravara</i>	
Algebraic Approach to Linking the Semantics of Web Services _____	315
<i>Huibiao Zhu, Jifeng He, Jing Li, and Jonathan P. Bowen</i>	

Security and Safety

Formal Verification of <i>tamper-evident</i> Storage for e-Voting _____	329
<i>Dominique Cansell, J. Paul Gibson, and Dominique Méry</i>	
A Scalable Lock-Free Stack Algorithm and its Verification _____	339
<i>Robert Colvin and Lindsay Groves</i>	
Verifying Security Properties of Cryptoprotocols: A Novel Approach _____	349
<i>Mohamed Saleh and Mourad Debbabi</i>	

Specification and Verification

Configurable Proof Obligations in the Frog Toolkit _____	361
<i>Simon Fraser and Richard Banach</i>	
Feature Refinement _____	371
<i>David Streader and Steve Reeves</i>	
Run-Time Composition and Adaptation of Mismatching Behavioural Transactions _____	381
<i>Javier Cámara, Gwen Salaün, and Carlos Canal</i>	
Flexible Behavioural Compatibility and Substitutability for Component Protocols: A Formal Specification _____	391
<i>Nabil Hameurlain</i>	

Author Index _____	401
---------------------------	------------