

Proceedings

HASE 2007

10th IEEE High Assurance Systems Engineering Symposium

14-16 November 2007
Dallas, Texas, USA

Sponsored by
IEEE Computer Society



The University of Texas at Dallas



Los Alamitos, California
Washington • Tokyo



HASE 2007

10th IEEE High Assurance Systems Engineering Symposium

Table of Contents

Message from HASE 2007 General Co-chairs.....	xii
Message from HASE 2007 Program Committee Chairs	xiii
Committees.....	xiv
External Reviewers	xvi

Papers, Keynotes, and Panels

Keynote

TRUSTED <i>ILLIAC</i> : A Configurable Hardware Framework for a Trusted Computing Base.....	3
<i>Ravishankar K. Iyer, University of Illinois</i>	

Session 1a. Panel

Panel: Achieving High Assurance: Formal, Informal, and Combined Approaches <i>Mediator: Bojan Cukic, West Virginia University</i> <i>Panelists:</i> <i>Betty Cheng, Michigan State University, USA</i> <i>Ali Mili, NJIT, USA</i> <i>Jeff Tian, SMU, USA</i>	
---	--

Session 1b. High Assurance Requirements

Goal-Oriented Patterns for UML-Based Modeling of Embedded Systems Requirements	7
<i>Heather J. Goldsby, Sascha Konrad, and Betty H. C. Cheng</i>	
Integrating Product-Line Fault Tree Analysis into AADL Models.....	15
<i>Hongyu Sun, Miriam Hauptman, and Robyn Lutz</i>	
Arguing Safety with Problem Oriented Software Engineering	23
<i>Jon G. Hall, Derek Mannering, and Lucia Rapanotti</i>	

Session 2a. System Design and Architectures

CROWN-C: A High-Assurance Service-Oriented Grid Middleware System.....	35
<i>Paul Townend, Nik Looker, Dacheng Zhang, Jie Xu, Jianxin Li, Liang Zhong, and Jinpeng Huai</i>	
Systems Architectures for Transactional Network Interface	45
<i>Manish Marwah, Shivakant Mishra, and Christof Fetzer</i>	
An Efficient Experimental Methodology for Configuring Search-Based Design Algorithms	53
<i>Simon Poulding, Paul Emberson, Iain Bate, and John Clark</i>	
A Typed Compositional Language for Real-Time Systems	63
<i>Jean-Paul Etienne and Samia Bouzefrane</i>	

Session 2b. State-of-the-Art Presentation. Security Systems Engineering

Speaker: Jeffery Voas, SAIC	
One in a Baker's Dozen: Debugging Debugging	75
<i>Jeffrey Voas and Keith Miller</i>	
Speaker: Catherine Meadows, Naval Research Lab	
The Verification of Crypto Protocols and Application to Security Standards	
<i>Catherine Meadows, Naval Research Lab</i>	
Speaker: Bhavani Thuraisingham, UTD	
Delegation-Based Security Model for Web Services	82
<i>Wei She, Bhavani Thuraisingham, and I-Ling Yen</i>	

Session 3a. Testing

Model Validation Using Automatically Generated Requirements-Based Tests.....	95
<i>Ajitha Rajan, Michael W. Whalen, and Mats P. E. Heimdahl</i>	
A Coverage Relationship Model for Test Case Selection and Ranking for Multi-version Software	105
<i>W. T. Tsai, Xinyu Zhou, Raymond A. Paul, Yinong Chen, and Xiaoying Bai</i>	
Enhanced Traverse of Web Pages	113
<i>Lihua Duan, Yan Wang, and Jessica Chen</i>	
How Can Previous Component Use Contribute to Assessing the Use of COTS?	123
<i>Silke Kuball</i>	

Session 3b. Security Assurance and Policies

Placement in Dependable and Secure Peer-to-Peer Data Grids	133
<i>Manghui Tu, Liangliang Xiao, Hui Ma, I-Ling Yen, and Farokh Bastani</i>	
Vulnerability Discovery in Multi-version Software Systems	141
<i>Jinyoo Kim, Yashwant K. Malaiya, and Indrakshi Ray</i>	

Testing Security Rules with Decomposable Activities	149
<i>Wissam Mallouli and Ana Cavalli</i>	
Flexible Authorization with Decentralized Access Control Model for Grid Computing	156
<i>Xinwen Zhang, Qi Li, Jean-Pierre Seifert, and Mingwei Xu</i>	

Keynote

Session 4a. Panel

Challenging Research Directions and Opportunities in High Assurance Systems Engineering	
<i>Mediator: Raymond Paul</i>	

Session 4b. Distributed Systems

Sustaining Property Verification of Synchronous Dependable Protocols over Implementation	169
<i>Péter Bokor, Marco Serafini, Áron Sisak, András Pataricza, and Neeraj Suri</i>	
Scalable, Adaptive, Time-Bounded Node Failure Detection.....	179
<i>Matthew Gillen, Kurt Rohloff, Prakash Manghwani, and Richard Schantz</i>	
SyncProbe: Providing Assurance of Message Latency through Predictive Monitoring of Internet Paths	187
<i>Jawwad Shamsi and Monica Brockmeyer</i>	

Session 5a. High Assurance Embedded Systems

Behavioral Fault Modeling for Model-Based Safety Analysis	199
<i>Anjali Joshi and Mats P. E. Heimdahl</i>	
Transformation-Based Library Adaptation for Embedded Systems.....	209
<i>Victor L. Winter, Azamat Mamejtanov, Steven E. Morrison, James A. McCoy, and Gregory L. Wickstrom</i>	
Multi-layered Data Consistency Technology, an Enhanced Autonomous Decentralized Data Consistency Technology for IC Card Ticket System.....	219
<i>Akio Shiibashi, Tsuyoshi Nakaniwa, Motoharu Yamana, and Kinji Mori</i>	
Model Transformation for High-Integrity Software Development in Derivative Vehicle Control System Design	227
<i>Shige Wang</i>	

Session 5b. State-of-the-Art Presentation. Software Engineering for High Assurance Systems

Speaker: David Parnas, University of Limerick	
Precise Documentation of Critical Software.....	237
<i>David L. Parnas and Sergiy A. Vilkomir</i>	

Speaker: Joanne Dugan, University of Virginia
 Combining Software Quality Analysis with Dynamic Event/Fault Trees for High Assurance Systems Engineering 245
Joanne Bechta Dugan, Ganesh J. Pai, and Hong Xu

Speaker: Wu-Hon Leung, Illinois Institute of Technology
 On the Verifiability of Programs Written in the Feature Language Extensions..... 256
Wu-Hon F. Leung

Session 6a. Fault Tolerance and Availability

Improving Reliability and Safety by Trading off Software Failure Criticalities..... 267
Atef Mohamed and Mohammad Zulkernine

Pattern-Based Modeling and Analysis of Failsafe Fault-Tolerance in UML 275
Ali Ebneenasir and Betty H. C. Cheng

A Stochastic Characterization of a Fault-Tolerant Gossip Algorithm..... 283
Xiaohu Li, Paul Parker, and Shouhuai Xu

A New Architecture for Single-Event Detection & Reconfiguration of SRAM-Based FPGAs 291
Eze Kamanu, Pratapa Reddy, Kenneth Hsu, and Marcin Lukowaik

Session 7a. Panel

A Systems Engineering Approach to Exception Handling
Mediator: Herbert Hecht, Chief Engineer, SoHaR Incorporated, Moderator
Panelists:
Tom Hoffman, MSAP Project Manager, JPL
Ravi Iyer, UIUC, USA
Roy Maxion, Carnegie Mellon University, USA
Alexander Romanovsky, Newcastle University, UK

On Exceptions, Exception Handling, Requirements and Software Lifecycle..... 301
Alexander Romanovsky

Session 7b. Empirical Analysis

Simulation Models and Implementation of a Simulator for the Performability Analysis of Electric Power Systems Considering Interdependencies..... 305
Francesco Romani, Silvano Chiaradonna, Felicita Di Giandomenico, and Luca Simoncini

Empirical Study of Embedded Software Quality and Productivity 313
Michael F. Siok and Jeff Tian

Availability Monitor for a Software Based System 321
Marc Haberkorn and Kishor Trivedi

Session 8a. Formal Verification and Validation

Validation Support for Distributed Real-Time Embedded Systems in VDM++	331
<i>John S. Fitzgerald, Peter Gorm Larsen, Simon Tjell, and Marcel Verhoef</i>	
Verification of Automatically Generated Pattern-Based LTL Specifications	341
<i>Salamah Salamah, Ann Q. Gates, Vladik Kreinovich, and Steve Roach</i>	
Utilizing Test Case Generation to Inspect Formal Specifications for Completeness and Feasibility	349
<i>Shaoying Liu</i>	
Multiple Pre/Post Specifications for Heap-Manipulating Methods	357
<i>Wei-Ngan Chin, Cristina David, Huu Hai Nguyen, and Shengchao Qin</i>	

Fast Abstracts

Fast Abstracts are short papers reporting on the promising research work still in progress. Unlike the regular papers, fast abstracts undergo only cursory reviews, to ensure timely dissemination of research ideas.

Session 3c. Fault Tolerance

A Fault Taxonomy for Service-Oriented Architecture	367
<i>Stefan Brüning, Stephan Weißleder, and Mirosław Malek</i>	
Advances in Quantum Computing Fault Tolerance and Testing	369
<i>David Y. Feinstein, V. S. S. Nair, and Mitchell A. Thornton</i>	
Preliminary Models of the Cost of Fault Tolerance	371
<i>Ronald J. Leach</i>	
Adding Autonomic Capabilities to Network Fault Management System.....	373
<i>Yan Liu, Michael Jiang, and David Raymer</i>	

Session 3d. Security

Information Assurance Architecture with Storyboarding Models	377
<i>Asesh Das</i>	
Fuzzing Wi-Fi Drivers to Locate Security Vulnerabilities	379
<i>Manuel Mendonça and Nuno Ferreira Neves</i>	
Towards a High Assurance Secure Computing Platform	381
<i>Michael D. DiRossi</i>	

Session 6b. Requirements and Design

High-Assurance Distributed, Adaptive Software for Dynamic Systems.....	385
<i>Kurt Rohloff, Joseph Loyall, Partha Pal, and Richard Schantz</i>	

Finance Sector: Requirements for High Assurance within Spatial SOA Based Grid Infrastructures	387
<i>P. C. Donachy, R. H. Perrott, T. J. Harmer, and F. Sharkey</i>	
A Mobile Agent-Based Multi-Robot Design Method for High-Assurance	389
<i>Sung-Oog Shin, Jung-Oog Lee, and Doo-Kwon Baik</i>	
Building High Assurance Multidisciplinary Design Optimization Framework.....	391
<i>Jeong-Oog Lee and Ho-Jun Lee</i>	

Session 6c. Web, E-Commerce, and Enterprise

Analytic Model for Web Anomalies Classification	395
<i>Nasser Alaeddine and Jeff Tian</i>	
Development of Custom Selling System Using Ad Hoc Networks	397
<i>Masato Asada, Tomoyuki Ohta, Kenji Ishida, and Yoshiaki Kakuda</i>	
Research on Noise Problem of Reputation Estimation in Virtual Enterprise	399
<i>Shaofei Wu and Shixian Wang</i>	

Session 6d. Quality, Reliability, and Safety

Measuring Reliability as a Mean Failure Cost.....	403
<i>Ali Mili and Frederick Sheldon</i>	
An Early-Reply Based Framework: Reliable Concurrency That is Verifiable	405
<i>Stephen W. Cook, Bjarne Stroustrup, and Scott M. Pike</i>	
A Safety Analysis Framework for COTS Microprocessors in Safety-Critical Applications	407
<i>Jason D. Lee, Praveen S. Bhojwani, and Rabi N. Mahapatra</i>	
Automated Test Data Generation and Reliability Assessment for Software in High Assurance Systems	409
<i>Branson W. Murrill</i>	
Parsimonious Classifiers for Software Quality Assessment	411
<i>Miyoungh Shin, Amrit L. Goel, Sunida Ratanothayanon, and Raymond A. Paul</i>	

Session 6e. Formal Methods and Its Applications

Methodology for Evaluating Aeronautical Regulations Using Formal Specifications	415
<i>Eduardo Rafael López Ruiz</i>	
Model-Checker-Based Testing of LTL Specifications	417
<i>Luis García and Steve Roach</i>	
A Formal Approach to Website Maintenance	419
<i>Lihua Duan and Jessica Chen</i>	

Session 8b. Systems and Networks

A Secure and Scalable Update Protocol for P2P Data Grids	423
<i>Manghui Tu, Nasser Tadayon, Zhonghang Xia, and Enyue Lu</i>	
Design of a Fairness Guarantee Mechanism Based on Network Measurement.....	425
<i>Xin Wang, Xiaochen Zhang, Shuang Yang, and Xiangyang Xue</i>	
All-Optical Routing for High Assurance Computer Systems.....	427
<i>Ekpe Okorafor</i>	
Duplication Based Integrated Task and Message Scheduling on a Heterogeneous Network of Workstations (NOWs)	429
<i>Nitin Auluck</i>	

Session 8c. Systems and Applications

Modelling and Exploration Environment for Application Specific Multiprocessor Systems	433
<i>Ismail Assayad and Sergio Yovine</i>	
A Nonparametric Cusum Algorithm for Timeslot Sequences with Applications to Network Surveillance	435
<i>Qi Zhang, Carlos Rendon, Veronica Montes De Oca, Daniel R. Jeske, and Mazda Marvasti</i>	
High Assurance GPS Integrity Monitoring System Using Particle Filtering Approach.....	437
<i>Jeong-Oog Lee, Dae Hee Won, Sangkyung Sung, Tae Sam Kang, and Young Jae Lee</i>	
Author Index.....	439