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

Session 1a. Panel

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

Session 1b. High Assurance Requirements

Goal-Oriented Patterns for UML-Based Modeling of Embedded Systems Requirements .............. 7
  Heather J. Goldsby, Sascha Konrad, and Betty H. C. Cheng

Integrating Product-Line Fault Tree Analysis into AADL Models.................................................. 15
  Hongyu Sun, Miriam Hauptman, and Robyn Lutz

Arguing Safety with Problem Oriented Software Engineering .................................................... 23
  Jon G. Hall, Derek Mannering, and Lucia Rapanotti
Session 2a. System Design and Architectures

CROWN-C: A High-Assurance Service-Oriented Grid Middleware System.................................................. 35
Paul Townend, Nik Looker, Dacheng Zhang, Jie Xu, Jianxin Li, Liang Zhong, and Jinpeng Huai

Systems Architectures for Transactional Network Interface....................................................................... 45
Manish Marwah, Shivakant Mishra, and Christof Fetzer

An Efficient Experimental Methodology for Configuring Search-Based Design Algorithms ..................... 53
Simon Poulding, Paul Emberson, Iain Bate, and John Clark

A Typed Compositional Language for Real-Time Systems........................................................................... 63
Jean-Paul Etienne and Samia Bouzefrane


Speaker: Jeffery Voas, SAIC
One in a Baker’s Dozen: Debugging Debugging......................................................................................... 75
Jeffrey Voas and Keith Miller

Speaker: Catherine Meadows, Naval Research Lab
The Verification of Crypto Protocols and Application to Security Standards
Catherine Meadows, Naval Research Lab

Speaker: Bhavani Thuraisingham, UTD
Delegation-Based Security Model for Web Services.................................................................................. 82
Wei She, Bhavani Thuraisingham, and I-Ling Yen

Session 3a. Testing

Model Validation Using Automatically Generated Requirements-Based Tests.......................................... 95
Ajitha Rajan, Michael W. Whalen, and Mats P. E. Heimdahl

A Coverage Relationship Model for Test Case Selection and Ranking for Multi-version Software .......... 105
W. T. Tsai, Xinyu Zhou, Raymond A. Paul, Yinong Chen, and Xiaoying Bai

Enhanced Traverse of Web Pages........................................................................................................... 113
Lihua Duan, Yan Wang, and Jessica Chen

How Can Previous Component Use Contribute to Assessing the Use of COTS? ................................... 123
Silke Kuball

Session 3b. Security Assurance and Policies

Placement in Dependable and Secure Peer-to-Peer Data Grids ............................................................. 133
Manghui Tu, Liangliang Xiao, Hui Ma, I-Ling Yen, and Farokh Bastani

Vulnerability Discovery in Multi-version Software Systems ........................................................................ 141
Jinyoo Kim, Yashwant K. Malaiya, and Indrakshi Ray
Testing Security Rules with Decomposable Activities .................................................. 149  
Wissam Mallouli and Ana Cavalli

Flexible Authorization with Decentralized Access Control Model for Grid Computing ............... 156  
Xinwen Zhang, Qi Li, Jean-Pierre Seifert, and Mingwei Xu

Keynote

Session 4a. Panel

Challenging Research Directions and Opportunities in High Assurance Systems Engineering  
Mediator: Raymond Paul

Session 4b. Distributed Systems

Sustaining Property Verification of Synchronous Dependable Protocols over Implementation ........... 169  
Péter Bokor, Marco Serafini, Áron Sisak, András Pataricza, and Neeraj Suri

Scalable, Adaptive, Time-Bounded Node Failure Detection .......................................................... 179  
Matthew Gillen, Kurt Rohloff, Prakash Manghwani, and Richard Schantz

SyncProbe: Providing Assurance of Message Latency through Predictive Monitoring of Internet Paths ............................................................................................................... 187  
Jawwad Shamsi and Monica Brockmeyer

Session 5a. High Assurance Embedded Systems

Behavioral Fault Modeling for Model-Based Safety Analysis ....................................................... 199  
Anjali Joshi and Mats P. E. Heimdahl

Transformation-Based Library Adaptation for Embedded Systems.............................................. 209  
Victor L. Winter, Azamat Mametjanov, Steven E. Morrison, James A. McCoy,  
and Gregory L. Wickstrom

Multi-layered Data Consistency Technology, an Enhanced Autonomous Decentralized Data Consistency Technology for IC Card Ticket System ............................................. 219  
Akio Shiibashi, Tsuyoshi Nakaniwa, Motoharu Yamana, and Kinji Mori

Model Transformation for High-Integrity Software Development in Derivative Vehicle Control System Design ........................................................................................................... 227  
Shige Wang

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  
David L. Parnas and Sergiy A. Vilkomir
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 Ebnenasir 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 Lukowiaik

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 Giandomenicco, 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
  John S. Fitzgerald, Peter Gorm Larsen, Simon Tjell, and Marcel Verhoef

Verification of Automatically Generated Pattern-Based LTL Specifications ................................................................. 341
  Salamah Salamah, Ann Q. Gates, Vladik Kreinovich, and Steve Roach

Utilizing Test Case Generation to Inspect Formal Specifications for Completeness and Feasibility ................................................................. 349
  Shaoying Liu

Multiple Pre/Post Specifications for Heap-Manipulating Methods ...................................................................... 357
  Wei-Ngan Chin, Cristina David, Huu Hai Nguyen, and Shengchao Qin

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
  Stefan Brüning, Stephan Weißleder, and Miroslaw Malek

Advances in Quantum Computing Fault Tolerance and Testing ........................................................................ 369
  David Y. Feinstein, V. S. S. Nair, and Mitchell A. Thornton

Preliminary Models of the Cost of Fault Tolerance .......................................................................................... 371
  Ronald J. Leach

Adding Autonomic Capabilities to Network Fault Management System .......................................................... 373
  Yan Liu, Michael Jiang, and David Raymer

Session 3d. Security

Information Assurance Architecture with Storyboarding Models ........................................................................ 377
  Asesh Das

Fuzzing Wi-Fi Drivers to Locate Security Vulnerabilities .................................................................................. 379
  Manuel Mendonça and Nuno Ferreira Neves

Towards a High Assurance Secure Computing Platform ................................................................................ 381
  Michael D. DiRossi

Session 6b. Requirements and Design

High-Assurance Distributed, Adaptive Software for Dynamic Systems .......................................................... 385
  Kurt Rohloff, Joseph Loyall, Partha Pal, and Richard Schantz
Finance Sector: Requirements for High Assurance within Spatial SOA Based Grid Infrastructures ................................................................................................................................... 387
   P. C. Donachy, R. H. Perrott, T. J. Harmer, and F. Sharkey

A Mobile Agent-Based Multi-Robot Design Method for High-Assurance ................................................................. 389
   Sung-Oog Shin, Jung-Oog Lee, and Doo-Kwon Baik

Building High Assurance Multidisciplinary Design Optimization Framework ............................................................. 391
   Jeong-Oog Lee and Ho-Jun Lee

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

Analytic Model for Web Anomalies Classification ........................................................................................................... 395
   Nasser Alaeddine and Jeff Tian

Development of Custom Selling System Using Ad Hoc Networks .................................................................................. 397
   Masato Asada, Tomoyuki Ohta, Kenji Ishida, and Yoshiaki Kakuda

Research on Noise Problem of Reputation Estimation in Virtual Enterprise ............................................................... 399
   Shaofei Wu and Shixian Wang

Session 6d. Quality, Reliability, and Safety

Measuring Reliability as a Mean Failure Cost ..................................................................................................................... 403
   Ali Mili and Frederick Sheldon

An Early-Reply Based Framework: Reliable Concurrency That is Verifiable ................................................................. 405
   Stephen W. Cook, Bjarne Stroustrup, and Scott M. Pike

   Jason D. Lee, Praveen S. Bhojwani, and Rabi N. Mahapatra

Automated Test Data Generation and Reliability Assessment for Software in High Assurance Systems ................. 409
   Branson W. Murrill

Parsimonious Classifiers for Software Quality Assessment ........................................................................................... 411
   Miyoung Shin, Amrit L. Goel, Sunida Ratanothayanon, and Raymond A. Paul

Session 6e. Formal Methods and Its Applications

Methodology for Evaluating Aeronautical Regulations Using Formal Specifications ............................................... 415
   Eduardo Rafael López Ruiz

Model-Checker-Based Testing of LTL Specifications .................................................................................................. 417
   Luis Garcia and Steve Roach

A Formal Approach to Website Maintenance .................................................................................................................. 419
   Lihua Duan and Jessica Chen
Session 8b. Systems and Networks

A Secure and Scalable Update Protocol for P2P Data Grids ................................................................. 423
Manghui Tu, Nasser Tadayon, Zhonghang Xia, and Enyue Lu

Design of a Fairness Guarantee Mechanism Based on Network Measurement ...................................... 425
Xin Wang, Xiaochen Zhang, Shuang Yang, and Xiangyang Xue

All-Optical Routing for High Assurance Computer Systems ....................................................................... 427
Ekpe Okoraror

Duplication Based Integrated Task and Message Scheduling on a Heterogeneous Network of Workstations (NOWs) ...................................................................................................................... 429
Nitin Auluck

Session 8c. Systems and Applications

Modelling and Exploration Environment for Application Specific Multiprocessor Systems .................... 433
Ismail Assayad and Sergio Yovine

A Nonparametric Cusum Algorithm for Timeslot Sequences with Applications to Network Surveillance .............................................................................................................................. 435
Qi Zhang, Carlos Rendon, Veronica Montes De Oca, Daniel R. Jeske, and Mazda Marvasti

High Assurance GPS Integrity Monitoring System Using Particle Filtering Approach ............................ 437
Jeong-Oog Lee, Dae Hee Won, Sangkyung Sung, Tae Sam Kang, and Young Jae Lee

Author Index.................................................................................................................................................. 439