Sixth IEEE International Symposium on High Assurance Systems Engineering
Special Topic: Impact of Networking

22-24 October 2001
Boca Raton, Florida, USA

Sponsored by the IEEE Computer Society
Technical Committee on Distributed Processing

http://computer.org
Los Alamitos, California
Washington Brussels Tokyo
HASE 2001 Organizing Committees ................................................................. ix

Keynotes

Erroneous Requirements: A Linguistic Basis for Their Occurrence and an Approach to Their Reduction ................................................................. 3
  John Knight

Arnold W. Pittler ............................................................................................. 4

Why Testing under Expected Operational Scenarios is Not Sufficient ................. 5
  Jeff Voas

Panel

Software Dependability in Distributed and Mobile Computing Environments .......... 7
  Moderator: R. Paul
  Panelists: A. Nikora
            R. R. Some
            J. Voas
            V. Winter
            J. Xu

Formal Methods

A Formal Testing Framework for UML Statechart Diagrams Behaviours: From Theory to Automatic Verification .............................................................. 11
  D. Latella and M. Massink

Test-Sequence Generation from Formal Requirement Models ................................... 23
  S. Rayadurgam and M. P. E. Heimdahl

Model-Checking for Validation of a Fault Protection System .................................... 32
  M. S. Feather, S. Fickas, and N.-A. Razermra-Mamy

Finite-State Analysis of the CAN Bus Protocol .................................................... 42
  M. van Osch and S. A. Smolka
Transportation

A Survey: Applying Formal Methods to a Software Intensive System.......................... 55
A. de Groot, J. Hooman, F. Kordon, E. Paviot-Adet, I. Mounier,
M. Lemoine, G. Gaudiere, V. L. Winter, and D. Kapur

Highly Reliable Relational Control Programs for Robust Rapid Transit Systems ....... 65
F. B. Bastani, I-L. Yen, and S. Kim

Mechanisms for a Reliable Cooperation of Vehicles ..................................................... 75
E. Nett, M. Gergeleit, and M. Mock

Verification of Assurance of Space On-Board Distributed Computer System .......... 82
H. Yashiro, Y. Takahashi, and T. Fujiwara

Testing

Framework for Testing the Fault-Tolerance of Systems Including OS
and Network Aspects .................................................................................................... 95
K. Buchacker and V. Sieh

A Test Management and Software Visualization Framework for
Heterogeneous Distributed Applications ................................................................. 106
S. Ghosh, N. Bawa, G. Craig, and K. Kalgaonkar

Automating Techniques for Inspecting High Assurance Systems ......................... 117
M. S. Fisher and B. Cukic

Genetic Programming Model for Software Quality Classification .......................... 127
Y. Liu and T. M. Khoshgoftaar

Security

An Unavailability Analysis of Firewall Sandwich Configurations......................... 139
S. Goddard, R. Kieckhafer, and Y. Zhang

Analyzing Internet Security Protocols ................................................................. 149
A. Yasinsac and J. Childs

Systems

The SASHA Architecture for Network-Clustered Web Servers .............................. 163
S. Goddard and T. Schroeder

On Simplifying Modular Specification and Verification of Distributed
Protocols ..................................................................................................................... 173
P. Sinha and N. Suri
Explicit Representation of Exception Handling in the Development of Dependable Component-Based Systems ................................................................. 182
  G. R. M. Ferreira, C. M. F. Rubira, and R. de Lemos

Systems Engineering of Communication Protocols for Command and Control Systems ................................................................................................... 194
  D. J. Thuente and J. K. Whiteman

**Railway Systems (Experience Reports)**

Integrating Automatic Verification of Safety Requirements in Railway Interlocking System Design................................................................. 209
  G. Dipoppa, G. D'Alessandro, R. Semprini, and E. Tronci

High Assurance Technologies for Autonomous Decentralized Train Control System........................................................................................................ 220
  M. Matsumoto, S. Kitamura, and M. Sato

Adaptive Step-by-Step Construction Technique Achieving High Assurance for Tokyo Metropolitan Railway Network ..................................................... 228
  K. Kera, K. Bekki, K. Kamijyo, and K. Mori

**Fast Abstracts**

Research Issues in Assurance of Software Dependability
  E. B. Allen

Are Measures and Metrics for Trusted Information Systems Possible?
  R. B. Vaughn and R. Henning

Generating Test Plans for Distributed Systems with Stochastic Decision Models
  S. Dalibor and M. Dal Cin

A Novel Adaptive Neural Network Based Technique to Enhance Software System Assurance for Regression Testing
  Z. Xu and N. D. Samaan

Application of Software for High Consequences Systems
  J. M. Covan and J. A. Cooper

Fault-Tolerant Cell Location Counter Strategy in Wireless Mobile Environment
  Y. An

Software IV&V Strategy for Small Projects
  R. M. Chapman
Characterization of Dynamic Behavior of Executable Software Objects to Optimize Test Case Selection for Regression
   N. Samaan and A. Ibrahim

A Case Study of IV&V Return on Investment (ROI)
   R. Rogers, D. McCaugherty, and F. Martin

Integrating Software into PRA: A Taxonomy of Software Related Failures
   B. Li, M. Li, and C. Smidts

Software Reliability Analysis for Regression Testing
   N. Samaan and Z. Tan

Assurance Analysis by Scenario-based UML Modeling
   K. Kosmidis and M. Sand

Web-Based Prototype of Real-Time Concurrent Systems by a Specification Technique with Safety and Liveness Properties
   K.-Y. Sung

Dynamic Fault-Tolerance Routing in 2-D Meshes
   Z. Jiang and J. Wu

Architecting eBanking High Assurance Security Solutions
   S. Soundararajan and D. Dey

Theorem-Proving Approach to Generating State Machine Test Sequences
   R. Busser, M. Boughdadi, M. Blackburn, and A. Naumann

Author Index ........................................................................................................................................... 237