# Table of Contents

*International Conference on Dependable Systems and Networks (DSN 2000)*

Message from the Chairs ................................................................. xvi
Program Committee .......................................................................... xviii
Conference Organization ................................................................. xx
Reviewers .......................................................................................... xxii
W.C. Carter Award ............................................................................ xxiv

## Session 1: Opening Session

- Opening Remarks
- Presentation of the W.C. Carter Award
- Keynote Address: The Challenges for Dependability in E-Business  
  *Dr. Timothy Chou, President and CEO of Oracle Business Online*

## Session 2A: Embedded Systems

- Transparent Redundancy in the Time-Triggered Architecture .......... 5  
  *G. Bauer and H. Kopetz*
- Resource Scheduling in Dependable Integrated Modular Avionics ....... 14  
  *Y-H. Lee, D. Kim, M. Younis, J. Zhou, and J. McElroy*
- Executable Assertions for Detecting Data Errors in Embedded Control Systems ........................................... 24  
  *M. Hiller*

## Session 2B: Practical Experience Reports I + Networks

- Experiences with Group Communication Middleware ..................... 37  
  *S. Johnson, F. Jahanian, S. Ghosh, B. Vanvoorst, N. Weininger,  
  and W. Heimerdinger*
Towards Dependable Home Networking: An Experience Report .................................43
Y.-M. Wang, W. Russell, A. Arora, J. Xu, and R. Jagannathan

Design, Implementation, and Performance of Checkpointing in NetSolve .....................49
A. Agbaria and J. Plank

Session 2C: Student Forum

Brief presentations by student travel award winners

Session 3: Panel

EU-USA Program of Research Collaboration on Dependability
Panel Chair: Brian Randell, University of Newcastle
Panelists: Frank Anger, NSF; Helen Gill, DARPA; Andrea Servida, European Commission; Mark LeBlanc, Department of State

Session 4A: Language Support

Efficient Incremental Checkpointing of Java Programs ..................................................61
J. Lawall and G. Muller

A C/C++ Source-to-Source Compiler for Dependable Applications ..........................71
A. Benso, S. Chiusano, P. Prinetto, and L. Tagliaferri

Session 4B: Practical Experience Reports II + COTS Evaluation

Assessment of the Applicability of COTS Microprocessors in High-Confidence Computing Systems: A Case Study .................................................................81
Y. He and A. Avizienis
Evaluating COTS Standards for Design of Dependable Systems........................................................................87
  C. Walter, N. Suri, and T. Monaghan

Session 4C: Student Forum

Brief presentations by student travel award winners

Session 5A: Measurement and Assessment

Whither Generic Recovery from Application Faults? A Fault Study Using Open-Source Software.........................................................97
  S. Chandra and P. Chen

Software-Implemented Fault Detection for High-Performance Space Applications.................................................................107
  M. Turmon, R. Granat, and D. Katz

Session 5B: Practical Experience Reports III + Validation and Evaluation

An Automatic SPIN Validation of a Safety Critical Railway Control System.........................................................................................119
  S. Gnesi, G. Lenzini, D. Latella, C. Abbaneo, A. Amendola,
  and P. Marmo

Sensitivity Analysis on Dependencies in Dynamic Availability Models for Large Systems ..................................................................................125
  M.-L. Yin, C. Hyde, and R. Arellano

Session 5C: Student Forum

Brief presentations by student travel award winners
Session 6A: Mobile Agents

Fault-Tolerant Execution of Mobile Agents ......................................................... 135
  L. Silva, V. Batista, and J. Silva

Exploiting Non-Determinism for Reliability of Mobile Agent Systems ............. 144
  A. Mohindra, A. Purakayastha, and P. Thati

Session 6B: Practical Experience Reports IV ♦ System Architecture

A New Rolling Stock Architecture Using Safety Computers and Networks ........ 157
  J.-B. Boullié and M. Brun

Reliability- Availability- Serviceability Characteristics of a Compressed-Memory System .......................................................... 163

A Fault Tolerant Signal Processing Computer ................................................... 169
  K. Prager, M. Vahey, W. Farwell, J. Whitney, and J. Lieb

Session 6C: Student Forum

Brief presentations by student travel award winners

Session 7: Day 2 ♦ Opening Session

Keynote Address: Internet Performance/Availability from an End User Perspective
  Eric Siegel, Keynote Systems
Session 8A: Analysis and Evaluation

Performability of Algorithms for Connection Admission Control .................................................. 181
    J. Meyer

On the Quality of Service of Failure Detectors ................................................................................. 191
    W. Chen, S. Toueg, and M. Aguilera

Session 8B: Theory

Fault-Secure Scheduling of Arbitrary Task Graphs to Multiprocessor Systems ........................................ 203
    K. Hashimoto, T. Tsuchiya, and T. Kikuno

Diagnosis of Regular Structures ........................................................................................................ 213
    A. Caruso, S. Chessa, P. Maestrini, and P. Santi

Session 8C: Software Demonstrations

OFTT: A Fault Tolerance Middleware Toolkit for Process Monitoring and Control Windows NT Applications ................................................................. 225
    M. Hecht, X. An, B. Zhang, and Y. He

DEEM: A Tool for the Dependability Modeling and Evaluation of Multiple Phased Systems ................................................................. 231
    A. Bondavalli, I. Mura, S. Chiaradonna, R. Filippini, S. Poli, and F. Sandrini

Loki: A State-Driven Fault Injector for Distributed Systems ................................................................. 237
    R. Chandra, R. Lefever, M. Cukier, and W. Sanders

Sensitivity Analysis for System Design Improvement ............................................................................. 243
    S. Contini, S. Scheer, and M. Wilikens
Session 9A: Testing of COTS Systems

Joint Evaluation of Performance and Robustness of a COTS DBMS through Fault-Injection .............................................................. 251
   D. Costa, T. Rilho, and H. Madeira

Robustness Testing of the Microsoft Win32 API ......................................................... 261
   C. Shelton, P. Koopman, and K. Devale

Session 9B: Byzantine Faults

From Crash Fault-Tolerance to Arbitrary-Fault Tolerance: Towards a Modular Approach ................................................................. 273
   R. Baldoni, J.-M. Helary, and M. Raynal

Dynamic Byzantine Quorum Systems ................................................................. 283
   L. Alvisi, D. Malkhi, E. Pierce, M. Reiter, and R. Wright

Session 10A: Analysis and Verification

A Tool Suite for Diagnosis and Testing of Software Design Specifications ................................................................. 295
   J. Li and J. Horgan

Enabling Automated Analysis through the Formalization of Object-Oriented Modeling Diagrams .................................................. 305
   B. Cheng, L. Campbell, and E. Wang

Deadlock Detection of EFSMs Using Simultaneous Reachability Analysis ................................................................. 315
   B. Karaçali, K.-C. Tai, and M. Vouk
Session 10B: Group Communication

A Low Latency, Loss Tolerant Architecture and Protocol for Wide Area Group Communication
Y. Amir, C. Danilov, and J. Stanton

A Reliable Many-to-Many Multicast Protocol for Group Communication over ATM Networks
R. Koch, L. Moser, and P. Melliar-Smith

A Gossip-Based Reliable Multicast for Large-Scale High-Throughput Applications
Q. Sun and D. Sturman

Session 10C: System Demonstrations

Fault-Tolerant Ethernet for IP-Based Process Control: A Demonstration
S. Song, J. Huong, P. Kappler, R. Freimark, J. Gustin, and T. Kozlik

Demonstration of the Remote Exploration and Experimentation (REE) Fault-Tolerant Parallel-Processing Supercomputer for Spacecraft Onboard Scientific Data Processing
R. Some, S. Upchurch, and K. Whisnant

Session 11A: Testing and Applications of Coding

Test-Point Insertion to Enhance Test Compaction for Scan Designs
I. Pomeranz and S. Reddy

Method to Recover Internet Packet Losses Using \((n, n - l, m)\) Convolutional Codes
M. Arai, A. Yamaguchi, and K. Iwasaki
One-Shot Reed-Solomon Decoding for High-Performance Dependable Systems ................................................................. 390
Y. Katayama and S. Morioka

**Session 11B: Panel**

Statistical or Probabilistic Decision Models: How Dependable Are They?
Panel Chair: P. Bose, IBM

**Session 12: Panel**

Running the Bytes without Getting Bitten: Strategies for Dealing with Malicious Code
Panel Chair: Carl Landwehr, Mitretek Systems
Panelists: Crispin Cowan, Oregon Graduate Institute, Gary McGraw, Reliable Software Technologies, and Jeannette Wing

**Session 13A: Software Fault Injection**

A Fault Injection Approach Based on Reflective Programming ................................................................. 407
E. Martins and A. Rosa

On the Emulation of Software Faults by Software Fault Injection ................................................................. 417
H. Madeira, D. Costa, and M. Vieira

Reliability Testing of Applications on Windows NT ......................................................................................... 427
T. Tsai and N. Singh

**Session 13B: Replication**

Implementing Flexible Object Group Invocation in Networked Systems ..................................................... 439
G. Morgan and S. Shrivastava
Implementing E-Transactions with Asynchronous Replication..................................................449
  S. Frölund and R. Guerraoui

Data Replication Strategies for Fault Tolerance and Availability on Commodity Clusters.................................459
  C. Amza, A. Cox, and W. Zwaenepoel

Session 13C: Fast Abstracts

Presentation of work in progress and late-breaking research results

Session 14A: High Performance Architecture

Designing High-Performance & Reliable Superscalar Architectures:
The out of Order Reliable Superscalar (O3RS) Approach..................................................473
  A. Mendelson and N. Suri

Fault Tolerance through Re-Execution in Multiscalar Architecture...........................................482
  F. Rashid, K. Saluja, and P. Ramanathan

A Fault Tolerance Infrastructure for Dependable Computing with High-Performance COTS Components............................................492
  A. Avižienis

Synthesis of Interconnection Networks: A Novel Approach ................................................501
  V. Lakamraju, I. Koren, and C. Krishna

Session 14B: Distributed System Models

The Best of Both Worlds: A Hybrid Approach to Solve Consensus ........................................513
  A. Mostefaoui, M. Raynal, and F. Tronel
Synchronous System and Perfect Failure Detector: Solvability and Efficiency Issues

- B. Charron-Bost, R. Guerraoui, and A. Schiper

The Timely Computing Base: Timely Actions in the Presence of Uncertain Timeliness

- P. Veríssimo, A. Casimiro, and C. Fetzer

Reconfiguration Based Failure Restoration in Wavelength-Routed WDM Networks

- G. Reddy, G. Manimaran, and C. Murthy

Session 14C: Fast Abstracts

Presentation of work in progress and late-breaking research results

Workshop on Dependability of IP Applications Platforms and Networks

Towards Continuous Availability of Internet Services through Availability Domains

- N. Bowen, D. Sturman, and T Liu

Issues in Interoperability and Performance Verification in a Multi-ORB Telecommunications Environment

- C. Lin, A. Avritzer, E. Weyuker, and S.-L Lo

Algorithms for Improving the Dependability of Firewall and Filter Rule Lists

- S. Hazelhurst, A. Attar, and R. Sinnappan

Dynamic-Distributed Differentiated Service for Multimedia Applications

- D. Hai and S. Vuong

xiv
Testing for Software Vulnerability Using Environment Perturbation ........................................603
   W. Du and A. Mathur

Survivability Analysis of Network Specifications .................................................................613
   S. Jha, J. Wing, R. Linger, and T. Longstaff

Benchmarking Anomaly-Based Detection Systems .............................................................623
   R. Maxion and K. Tan

Avoiding Loss of Fairness Owing to Process Crashes in Fair Data Exchange Protocols .........................................................631
   P. Liu, P. Ning, and S. Jajodia

A Formal-Specification Based Approach for Protecting the Domain Name System ..................641
   S. Cheung and K. Levitt

Author Index .........................................................................................................................653