

# Proceedings

---

## 37<sup>th</sup> Annual IEEE/IFIP International Conference on Dependable Systems and Networks



25-28 June 2007 • Edinburgh, UK

### Sponsored by

IEEE Computer Society Technical Committee on Dependable Computing and Fault Tolerance  
IFIP WG 10.4 on Dependable Computing and Fault Tolerance



Los Alamitos, California  
Washington • Tokyo



37<sup>th</sup> Annual IEEE/IFIP International Conference on  
Dependable Systems & Networks  
2007

## TABLE OF CONTENTS

### **KEYNOTE ADDRESS**

|                                                              |          |
|--------------------------------------------------------------|----------|
| <b>Science and Engineering: A Collusion of Cultures.....</b> | <b>1</b> |
| <i>T. Hoare</i>                                              |          |

### **DEPENDABLE COMPUTING AND COMMUNICATIONS SYMPOSIUM (DCCS)**

#### **SESSION 1A: SECURITY PROTECTION: ARCHITECTURAL APPROACHES**

|                                                                             |           |
|-----------------------------------------------------------------------------|-----------|
| <b>Augmenting Branch Predictor to Secure Program Execution .....</b>        | <b>7</b>  |
| <i>Y. Shi, G. Lee</i>                                                       |           |
| <b>A Firewall for Routers: Protecting Against Routing Misbehavior .....</b> | <b>17</b> |
| <i>Y. Zhang, Z.M. Mao, J. Wang</i>                                          |           |
| <b>An Architectural Approach to Preventing Code Injection Attacks.....</b>  | <b>27</b> |
| <i>R. Riley, X. Jiang, D. Xu</i>                                            |           |

#### **SESSION 1B: SOFTWARE FAULT TOLERANCE**

|                                                                           |           |
|---------------------------------------------------------------------------|-----------|
| <b>Failure Resilience for Device Drivers .....</b>                        | <b>37</b> |
| <i>J.N. Herder, H. Bos, G. Gras, P. Homburg, A.S. Tanenbaum</i>           |           |
| <b>Fault Tolerance Connectors for Unreliable Web Services .....</b>       | <b>47</b> |
| <i>N. Salatge, J.C. Fabre</i>                                             |           |
| <b>Robustness and Security Hardening of COTS Software Libraries .....</b> | <b>57</b> |
| <i>M. Sußkraut, C. Fetzer</i>                                             |           |

#### **SESSION 2A: DISTRIBUTED CONSENSUS**

|                                                                                                                    |           |
|--------------------------------------------------------------------------------------------------------------------|-----------|
| <b>Automatic Verification and Discovery of Byzantine Consensus Protocols .....</b>                                 | <b>67</b> |
| <i>P. Zielinski</i>                                                                                                |           |
| <b>Knowledge Connectivity vs. Synchrony Requirements for Fault-tolerant Agreement in<br/>Unknown Networks.....</b> | <b>77</b> |
| <i>F. Greve, S. Tixeuil</i>                                                                                        |           |
| <b>Communication Predicates: A High-level Abstraction for Coping with Transient and<br/>Dynamic Faults.....</b>    | <b>87</b> |
| <i>M. Huttle, A. Schiper</i>                                                                                       |           |
| <b>Synchronous Consensus with Mortal Byzantines.....</b>                                                           | <b>97</b> |
| <i>J. Widder, G. Gridling, B. Weiss, J. Blanquart</i>                                                              |           |

## **SESSION 2B: PRACTICAL EXPERIENCE REPORTS**

|                                                                                 |     |
|---------------------------------------------------------------------------------|-----|
| <b>Reliability Techniques for RFID-Based Object Tracking Applications</b> ..... | 107 |
| <i>A. Rahmati, L. Zhong, M. Hiltunen, R. Jana</i>                               |     |
| <b>Profiling Attacker Behavior Following SSH Compromises</b> .....              | 113 |
| <i>D. Ramsbrock, R. Berthier, M. Cukier</i>                                     |     |
| <b>Dependability Assessment of Grid Middleware</b> .....                        | 119 |
| <i>N. Looker, J. Xu</i>                                                         |     |
| <b>Assessing Robustness of Web-services Infrastructures</b> .....               | 125 |
| <i>M. Vieira, N. Laranjeiro, H. Madeira</i>                                     |     |
| <b>Protecting Cryptographic Keys from Memory Disclosure Attacks</b> .....       | 131 |
| <i>K. Harrison, S. Xu</i>                                                       |     |

## **SESSION 3A: EMBEDDED SYSTEMS**

|                                                                                                                                                         |     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------|-----|
| <b>Fault Tolerant Planning for Critical Robots</b> .....                                                                                                | 137 |
| <i>B. Lussier, M. Gallien, J. Guiochet, F. Ingrand, M. Killijian, D. Powell</i>                                                                         |     |
| <b>Insights into the Sensitivity of the BRAIN (Braided Ring Availability Integrity Network)-<br/>On Platform Robustness in Extended Operation</b> ..... | 147 |
| <i>M. Paulitsch, B. Hall</i>                                                                                                                            |     |
| <b>A Tunable Add-on Diagnostic Protocol for Time-triggered Systems</b> .....                                                                            | 157 |
| <i>M. Serafini, N. Suri, J. Vinter, A. Ademaj, W. Brandstatter, F. Tagliabo, J. Koch</i>                                                                |     |

## **SESSION 3B: DEPENDABILITY MODELING**

|                                                                                                          |     |
|----------------------------------------------------------------------------------------------------------|-----|
| <b>Enhanced Reliability Modeling of RAID Storage Systems</b> .....                                       | 167 |
| <i>J.G. Elerath, M. Pecht</i>                                                                            |     |
| <b>On a Modeling Framework for the Analysis of Interdependencies in Electric Power<br/>Systems</b> ..... | 177 |
| <i>S. Chiaradonna, P. Lollini, F. Di Giandomenico</i>                                                    |     |

## **SESSION 4A: HARDWARE FAULT TOLERANCE: EMERGING CHALLENGES**

|                                                                                                                |     |
|----------------------------------------------------------------------------------------------------------------|-----|
| <b>Superscalar Processor Performance Enhancement through Reliable Dynamic Clock<br/>Frequency Tuning</b> ..... | 187 |
| <i>V. Subramanian, M. Bezdek, N.D. Avirneni, A. Somani</i>                                                     |     |
| <b>Determining Fault Tolerance of XOR-based Erasure Codes Efficiently</b> .....                                | 197 |
| <i>J.J. Wylie, R. Swaminathan</i>                                                                              |     |
| <b>Fault Tolerant Approaches to Nanoelectronic Programmable Logic Arrays</b> .....                             | 207 |
| <i>W. Rao, A. Orailoglu, R. Karri</i>                                                                          |     |

## **SESSION 4B: VM REJUVENATION AND NETWORK RELIABILITY**

|                                                                          |     |
|--------------------------------------------------------------------------|-----|
| <b>Concilium: Collaborative Diagnosis of Broken Overlay Routes</b> ..... | 215 |
| <i>J.W. Mickens, B.D. Noble</i>                                          |     |

|                                                                                           |            |
|-------------------------------------------------------------------------------------------|------------|
| <b>R-Sentry: Providing Continuous Sensor Services Against Random Node Failures .....</b>  | <b>225</b> |
| <i>S. Yu, Y. Zhang</i>                                                                    |            |
| <b>A Fast Rejuvenation Technique for Server Consolidation with Virtual Machines .....</b> | <b>235</b> |
| <i>K. Kourai, S. Chiba</i>                                                                |            |

## **SESSION 5A: SOFT ERRORS: ANALYSIS AND PROTECTION**

|                                                                                                                               |            |
|-------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>A Cost-effective Dependable Microcontroller Architecture with Instruction-level Rollback for Soft Error Recovery .....</b> | <b>245</b> |
| <i>T. Sakata, T. Hirotsu, H. Yamada, T. Kataoka</i>                                                                           |            |
| <b>Architecture-level Soft Error Analysis: Examining the Limits of Common Assumptions .....</b>                               | <b>255</b> |
| <i>X. Li, S.V. Adve, P. Bose, J.A. Rivers</i>                                                                                 |            |
| <b>Feedback Redundancy: A Power Efficient SEU-Tolerant Latch Design for Deep Sub-micron Technologies .....</b>                | <b>265</b> |
| <i>M. Fazeli, A. Patooghy, S.G. Miremadi, A. Ejlali</i>                                                                       |            |
| <b>Using Register Lifetime Predictions to Protect Register Files Against Soft Errors .....</b>                                | <b>275</b> |
| <i>P. Montesinos; Wei Liu, Josep Torrellas</i>                                                                                |            |

## **SESSION 5B: PROCESSOR LEVEL FAULT TOLERANCE**

|                                                                                                       |            |
|-------------------------------------------------------------------------------------------------------|------------|
| <b>Using Process-level Redundancy to Exploit Multiple Cores for Transient Fault Tolerance .....</b>   | <b>285</b> |
| <i>A. Shye, T. Moseley, V.J. Reddi, J. Blomstedt, D.A. Connors</i>                                    |            |
| <b>Inherent Time Redundancy (ITR): Using Program Repetition for Low-overhead Fault Tolerance.....</b> | <b>295</b> |
| <i>V. Reddy, E. Rotenberg</i>                                                                         |            |
| <b>Utilizing Dynamically Coupled Cores to Form a Resilient Chip Multiprocessor.....</b>               | <b>305</b> |
| <i>C. LaFrieda, E. Ipek, J.F. Martinez, R. Manohar</i>                                                |            |
| <b>BlackJack: Hard Error Detection with Redundant Threads on SMT .....</b>                            | <b>315</b> |
| <i>E. Schuchman, T.N. Vijaykumar</i>                                                                  |            |

## **SESSION 6A: CRITICAL SYSTEMS: RISK ANALYSIS AND ASSURANCE**

|                                                                             |            |
|-----------------------------------------------------------------------------|------------|
| <b>Confidence: Its Role in Dependability Cases for Risk Assessment.....</b> | <b>325</b> |
| <i>R.E. Bloomfield, B. Littlewood, D. Wright</i>                            |            |
| <b>Assurance Based Development of Critical Systems.....</b>                 | <b>334</b> |
| <i>P.J. Graydon, J.C. Knight, E.A. Strunk</i>                               |            |

## **SESSION 6B: SECURITY THREATS AND NOVEL DETECTION**

|                                                                                                     |            |
|-----------------------------------------------------------------------------------------------------|------------|
| <b>Multiprocessors May Reduce System Dependability under File-based Race Condition Attacks.....</b> | <b>344</b> |
| <i>J. Wei, C. Pu</i>                                                                                |            |
| <b>Understanding Resiliency of Internet Topology Against Prefix Hijack Attacks .....</b>            | <b>354</b> |
| <i>M. Lad, R. Oliveira, B. Zhang, L. Zhang</i>                                                      |            |

|                                                                    |            |
|--------------------------------------------------------------------|------------|
| <b>User Discrimination through Structured Writing on PDAs.....</b> | <b>364</b> |
| <i>R.R.M. Roberts, R.A. Maxion, K.S. Killourhy, F. Arshad</i>      |            |

## **SESSION 7A: TIMING MODEL AND NETWORK PROTOCOLS**

|                                                                                           |            |
|-------------------------------------------------------------------------------------------|------------|
| <b>How to Choose a Timing Model? .....</b>                                                | <b>374</b> |
| <i>I. Keidar, A. Shraer</i>                                                               |            |
| <b>Electing an Eventual Leader in an Asynchronous Shared Memory System.....</b>           | <b>384</b> |
| <i>A. Fernandez, E. Jimenez, M. Raynal</i>                                                |            |
| <b>Minimizing Response Time for Quorum-system Protocols over Wide-area Networks .....</b> | <b>394</b> |
| <i>F. Oprea, M.K. Reiter</i>                                                              |            |
| <b>HyParView: A Membership Protocol for Reliable Gossip-based Broadcast .....</b>         | <b>404</b> |
| <i>J. Leitaó, J. Pereira, L. Rodrigues</i>                                                |            |

## **SESSION 7B: SECURITY PROTECTION: ALGORITHMIC APPROACHES**

|                                                                                         |            |
|-----------------------------------------------------------------------------------------|------------|
| <b>A Lightweight Mechanism for Dependable Communication in Untrusted Networks .....</b> | <b>414</b> |
| <i>M. Rogers, S. Bhatti</i>                                                             |            |
| <b>Dynamic Cross-realm Authentication for Multi-party Service Interactions .....</b>    | <b>424</b> |
| <i>D. Zhang, J. Xu, X. Li</i>                                                           |            |
| <b>Enhancing DNS Resilience Against Denial of Service Attacks.....</b>                  | <b>434</b> |
| <i>V. Pappas, D. Massey, L. Zhang</i>                                                   |            |
| <b>Automatic Cookie Usage Setting with CookiePicker .....</b>                           | <b>444</b> |
| <i>C. Yue, M. Xie, H. Wang</i>                                                          |            |

## **SESSION 8A: NETWORKING**

|                                                                                  |            |
|----------------------------------------------------------------------------------|------------|
| <b>Greedy Receivers in IEEE 802.11 Hotspots .....</b>                            | <b>454</b> |
| <i>M.K. Han, B. Overstreet, L. Qiu</i>                                           |            |
| <b>Emergent Structure in Unstructured Epidemic Multicast .....</b>               | <b>464</b> |
| <i>N. Carvalho, J. Pereira, R. Oliveira, L. Rodrigues</i>                        |            |
| <b>The Case for FEC-based Reliable Multicast in Wireless Mesh Networks .....</b> | <b>474</b> |
| <i>D. Koutsonikolas, Y.C. Hu</i>                                                 |            |

## **SESSION 8B: EXPERIMENTAL DEPENDABILITY ASSESSMENT**

|                                                                                         |            |
|-----------------------------------------------------------------------------------------|------------|
| <b>On the Selection of Error Model(s) for OS Robustness Evaluation .....</b>            | <b>484</b> |
| <i>A. Johansson, N. Suri, B. Murphy</i>                                                 |            |
| <b>Experimental Risk Assessment and Comparison using Software Fault Injection .....</b> | <b>494</b> |
| <i>R. Moraes, J. Duraes, R. Barbosa, E. Martins, H. Madeira</i>                         |            |

|                                                                                     |            |
|-------------------------------------------------------------------------------------|------------|
| <b>Foundations of Measurement Theory Applied to the Evaluation of Dependability</b> |            |
| <b>Attributes .....</b>                                                             | <b>504</b> |
| <i>A. Bondavalli, M. Vadursi, A. Ceccarelli, L. Falai</i>                           |            |

## **PERFORMANCE AND DEPENDABILITY SYMPOSIUM (PDS)**

### **SESSION 1C: SYSTEM ARCHITECTURE AND SOFTWARE ASSESSMENT**

|                                                                               |            |
|-------------------------------------------------------------------------------|------------|
| <b>A Framework for Architecture-level Lifetime Reliability Modeling .....</b> | <b>514</b> |
| <i>J. Shin, V. Zyuban, Z. Hu, J.A. Rivers, P. Bose</i>                        |            |
| <b>Processor-level Selective Replication .....</b>                            | <b>524</b> |
| <i>N. Nakka, K. Pattabiraman, R. Iyer</i>                                     |            |
| <b>Robustness Testing of the Windows DDK .....</b>                            | <b>534</b> |
| <i>M. Mendonca, N. Neves</i>                                                  |            |

### **SESSION 2C: MEASUREMENT AND MONITORING**

|                                                                                            |            |
|--------------------------------------------------------------------------------------------|------------|
| <b>SLAM: Sleep-Wake Aware Local Monitoring in Sensor Networks .....</b>                    | <b>544</b> |
| <i>I. Khalil, S. Bagchi, N.B. Shroff</i>                                                   |            |
| <b>What Supercomputers Say: A Study of Five System Logs .....</b>                          | <b>554</b> |
| <i>A. Onliner, J. Stearley</i>                                                             |            |
| <b>How do Mobile Phones Fail? A Failure Data Analysis of Symbian OS Smart Phones .....</b> | <b>564</b> |
| <i>M. Cinque, D. Cotroneo, Z. Kalbarczyk, R.K. Iyer</i>                                    |            |
| <b>A Real-time Network Traffic Profiling System .....</b>                                  | <b>574</b> |
| <i>K. Xu, F. Weng, S. Bhattacharyya, Z. Zhang</i>                                          |            |

### **SESSION 3C: PRACTICAL EXPERIENCE REPORTS**

|                                                                                                                          |            |
|--------------------------------------------------------------------------------------------------------------------------|------------|
| <b>RAS by the Yard .....</b>                                                                                             | <b>584</b> |
| <i>A. Wood, S. Nathan</i>                                                                                                |            |
| <b>Web Services Wind Tunnel: On Performance Testing Large-scale Stateful Web Services .....</b>                          | <b>590</b> |
| <i>M. De Barros, J. Shiau, C. Shang, K. Gidewall, H. Shi, J. Forsmann</i>                                                |            |
| <b>Application of Software Watchdog as a Dependability Software Service for Automotive Safety Relevant Systems .....</b> | <b>596</b> |
| <i>X. Chen, J. Feng, M. Hiller, V. Lauer</i>                                                                             |            |

### **SESSION 4C: DISTRIBUTED ALGORITHMS**

|                                                                                                                                   |            |
|-----------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>Evaluating the Impact of Simultaneous Round Participation and Decentralized Decision on the Performance of Consensus .....</b> | <b>602</b> |
| <i>L. Sampaio, M. Hurfin, F. Brasileiro, F. Greve</i>                                                                             |            |
| <b>On the Cost of Modularity in Atomic Broadcast .....</b>                                                                        | <b>612</b> |
| <i>O. Rutti, S. Mena, R. Ekwall, A. Schiper</i>                                                                                   |            |

|                                                                 |            |
|-----------------------------------------------------------------|------------|
| <b>Eventually k-Bounded Wait-free Distributed Daemons .....</b> | <b>622</b> |
| <i>Y. Song, S.M. Pike</i>                                       |            |

## **SESSION 5C: AVAILABILITY OF DISTRIBUTED SYSTEMS**

|                                                                                                               |            |
|---------------------------------------------------------------------------------------------------------------|------------|
| <b>Measuring Availability in Optimistic Partition-tolerant Systems with Data Constraints .....</b>            | <b>632</b> |
| <i>M. Asplund, S. Nadjm-Tehrani, S. Beyer, P. Galdamez</i>                                                    |            |
| <b>Scaling and Continuous Availability in Database Server Clusters through Multiversion Replication .....</b> | <b>642</b> |
| <i>K. Manassiev, C. Amza</i>                                                                                  |            |
| <b>Improving Recoverability in Multi-tier Storage Systems .....</b>                                           | <b>653</b> |
| <i>M.K. Aguilera, K. Keeton, A. Merchant, K-K. Muniswamy-Reddy, M. Uysal</i>                                  |            |
| <b>Portable and Efficient Continuous Data Protection for Network File Servers .....</b>                       | <b>663</b> |
| <i>N. Zhu, T. Chiueh</i>                                                                                      |            |

## **SESSION 6C: MODELING AND EVALUATION**

|                                                                                                              |            |
|--------------------------------------------------------------------------------------------------------------|------------|
| <b>Variational Bayesian Approach for Interval Estimation of NHPP-based Software Reliability Models .....</b> | <b>673</b> |
| <i>H. Okamura, M. Grottke, T. Dohi, K.S. Trivedi</i>                                                         |            |
| <b>Dynamic Fault Tree Analysis using Input/Output Interactive Markov Chains .....</b>                        | <b>683</b> |
| <i>H. Boudali, P. Crouzen, M. Stoelinga</i>                                                                  |            |
| <b>Uniformity by Construction in the Analysis of Nondeterministic Stochastic Systems .....</b>               | <b>693</b> |
| <i>H. Hermanns, S. Johr</i>                                                                                  |            |

## **SESSION 7C: QUALITY OF SERVICE AND ERROR RECOVERY**

|                                                                                          |            |
|------------------------------------------------------------------------------------------|------------|
| <b>A Reinforcement Learning Approach to Automatic Error Recovery .....</b>               | <b>703</b> |
| <i>Q. Zhu, C. Yuan</i>                                                                   |            |
| <b>On the Quality of Service of Crash-recovery Failure Detectors .....</b>               | <b>713</b> |
| <i>T. Ma, J. Hillston, S. Anderson</i>                                                   |            |
| <b>E2EProf: Automated End-to-End Performance Management for Enterprise Systems .....</b> | <b>723</b> |
| <i>S. Agarwala, F. Alegre, K. Schwan, J. Mehalingham</i>                                 |            |
| <b>Bounding Peer-to-Peer Upload Traffic in Client Networks .....</b>                     | <b>733</b> |
| <i>C. Huang, C. Lei</i>                                                                  |            |

## **SESSION 8C: STOCHASTIC MODELING**

|                                                                                                 |            |
|-------------------------------------------------------------------------------------------------|------------|
| <b>Performability Models for Multi-server Systems with High-variance Repair Durations .....</b> | <b>743</b> |
| <i>H. Schwefel, I. Antonios</i>                                                                 |            |
| <b>Computing Battery Lifetime Distributions .....</b>                                           | <b>753</b> |
| <i>L. Cloth, M.R. Jongerden, B.R. Haverkort</i>                                                 |            |
| <b>Quantifying the Effectiveness of Mobile Phone Virus Response Mechanisms .....</b>            | <b>763</b> |
| <i>E. Van Ruitenbeek, T. Courtney, W.H. Sanders, F. Stevens</i>                                 |            |

## **SPECIAL TRACKS**

|                                                                                                                                  |            |
|----------------------------------------------------------------------------------------------------------------------------------|------------|
| <b>DSN 2007 Tutorials .....</b>                                                                                                  | <b>773</b> |
| <i>L. Rodrigues</i>                                                                                                              |            |
| <b>DSN 2007 Workshops .....</b>                                                                                                  | <b>774</b> |
| <i>C. Fetzer</i>                                                                                                                 |            |
| <b>Workshop on Dependable Application Support for Self-Organizing Networks (DASSON 2007) .....</b>                               | <b>775</b> |
| <i>P. Ezhilchelvan, M. Raynal, A. Datta</i>                                                                                      |            |
| <b>Third Workshop on Hot Topics in System Dependability (HotDep'07) .....</b>                                                    | <b>776</b> |
| <i>M. Castro, J. Wilkes</i>                                                                                                      |            |
| <b>Workshops on Architecting Dependable Systems (WADS 2007) .....</b>                                                            | <b>777</b> |
| <i>R. Lemos, F. Di Giandomenico, C. Gacek</i>                                                                                    |            |
| <b>Assurance Cases for Security: The Metrics Challenge .....</b>                                                                 | <b>779</b> |
| <i>R. Bloomfield, M. Masera, A. Miller, O.S. Saydjari, C.B. Weinstock</i>                                                        |            |
| <b>Workshop on Dependable and Secure Nanocomputing .....</b>                                                                     | <b>781</b> |
| <i>J. Arlat, R.K. Iyer, M. Nicolaidis</i>                                                                                        |            |
| <b>Student Forum .....</b>                                                                                                       | <b>783</b> |
| <i>F. Jahanian</i>                                                                                                               |            |
| <b>Fast Abstracts .....</b>                                                                                                      | <b>784</b> |
| <i>H. Nakamura</i>                                                                                                               |            |
| <b>The National Programme for Information Technology in the UK Health Service: Dependability Challenges and Strategies .....</b> | <b>785</b> |
| <i>B. Randell</i>                                                                                                                |            |
| <b>Industry Session .....</b>                                                                                                    | <b>786</b> |
| <i>L. Spainhower</i>                                                                                                             |            |
| <b>Author Index</b>                                                                                                              |            |