# Table of Contents

**Human-Computer System Dependability**  
(Joint ECCE-11 & SAFECOMP 2002)  

Human-Computer System Dependability ..........................1  
*Panel moderators: Sandro Bologna and Erik Hollnagel*  
Dependability of Joint Human-Computer Systems  ..............4  
*Erik Hollnagel*

**Keynote Talk**

Dependability in the Information Society: Getting Ready for the FP6 .. 10  
*Andrea Servida*

**Human Factors**

A Rigorous View of Mode Confusion ..............................19  
*Jan Bredereke and Axel Lankenau*

Dependability as Ordinary Action ...............................32  
*Alexander Voß, Roger Slack, Rob Procter, Robin Williams,  
Mark Hartswood, and Mark Rouncefield*

**Security**

Practical Solutions to Key Recovery Based on PKI in IP Security .......44  
*Yoon-Jung Rhee and Tai-Yun Kim*

Redundant Data Acquisition in a Distributed Security Compound .......53  
*Thomas Droste*

Survivability Strategy for a Security Critical Process ............61  
*Ferdinand J. Dafelmair*

**Dependability Assessment (Poster Session)**

Statistical Comparison of Two Sum-of-Disjoint-Product Algorithms for Reliability and Safety Evaluation ..............................70  
*Klaus Heidtmann*
### Table of Contents

**Safety and Security Analysis of Object-Oriented Models**

Kevin Lano, David Clark, and Kelly Androutsopoulos

---

**The CORAS Framework for a Model-Based Risk Management Process**

Rune Fredriksen, Monica Kristiansen, Bjørn Axel Gran, Ketil Stølen, Tom Arthur Opperud, and Theo Dimitrakos

---

**Keynote Talk**

Software Challenges in Aviation Systems

*John C. Knight*

---

**Application of Formal Methods (Poster Session)**

A Strategy for Improving the Efficiency of Procedure Verification

*Wenhui Zhang*

Verification of the SSL/TLS Protocol Using a Model Checkable Logic of Belief and Time

*Massimo Benerecetti, Maurizio Panti, Luca Spalazzi, and Simone Tacconi*

Reliability Assessment of Legacy Safety-Critical Systems Upgraded with Off-the-Shelf Components

*Peter Popov*

---

**Reliability Assessment**

Assessment of the Benefit of Redundant Systems

*Luping Chen, John May, and Gordon Hughes*

Estimating Residual Faults from Code Coverage

*Peter G. Bishop*

---

**Design for Dependability**

Towards a Metrics Based Verification and Validation Maturity Model

*Jef Jacobs and Jos Trienekens*

Analysing the Safety of a Software Development Process

*Stephen E. Paynter and Bob W. Born*

Software Criticality Analysis of COTS/SOUP

*Peter Bishop, Robin Bloomfield, Tim Clement, and Sofia Guerra*
Safety Assessment

Methods of Increasing Modelling Power for Safety Analysis, Applied to a Turbine Digital Control System .......................... 212
Andrea Bobbio, Ester Ciancamerla, Giuliana Franceschinis, Rossano Gaeta, Michele Minichino, and Luigi Portinale

Checking Safe Trajectories of Aircraft Using Hybrid Automata ........ 224
Italo Romani de Oliveira and Paulo Sérgio Cugnasca

Model-Based On-Line Monitoring Using a State Sensitive Fault Propagation Model .......................... 236
Yiannis Papadopoulos

Keynote Talk

On Diversity, and the Elusiveness of Independence .................. 249
Bev Littlewood

Design for Dependability (Poster Session)

An Approach to a New Network Security Architecture for Academic Environments ......................................................... 252
MahdiReza Mohajerani and Ali Moeini

A Watchdog Processor Architecture with Minimal Performance Overhead ........................................ 261
Francisco Rodríguez, José Carlos Campelo, and Juan José Serrano

Application of Formal Methods

Model-Checking Based on Fluid Petri Nets for the Temperature Control System of the ICARO Co-generative Plant ........................................ 273
M. Gribaudo, A. Horváth, A. Bobbio, E. Tronci, E. Ciancamerla, and M. Minichino

Assertion Checking Environment (ACE) for Formal Verification of C Programs ........................................ 284
B. Sharma, S. D. Dhodapkar, and S. Ramesh

Safety Analysis of the Height Control System for the Elbtunnel ......... 296
Frank Ortmeier, Gerhard Schellhorn, Andreas Thums, Wolfgang Reif, Bernhard Hering, and Helmut Trappenschuh
**Design for Dependability**

Dependability and Configurability:
Partners or Competitors in Pervasive Computing? ....................... 309
*Titos Saridakis*

Architectural Considerations in the Certification of Modular Systems ..... 321
*Iain Bate and Tim Kelly*

A Problem-Oriented Approach to Common Criteria Certification ........ 334
*Thomas Rottke, Denis Hatebur, Maritta Heisel, and Monika Heiner*

**Author Index** ............................................................. 347
Computer Safety, Reliability and Security
Anderson, S.; Bologna, S.; Felici, M. (Eds.)
2002, CCCLXXII, 352 p., Softcover
ISBN: 978-3-540-44157-1