SAFECOMP 96

The 15th International Conference on Computer Safety, Reliability and Security

Vienna, Austria
October 23 - 25, 1996

Edited by
ERWIN SCHOITSCH

SEIBERSDORF

Organized by

Austrian Research Centre Seibersdorf

Co-Organized by

Austrian Federal Ministry of Science, Transport and the Arts

Sponsors

European Workshop on Industrial Computer Systems
Technical Committee 7
(EWICS TC 7)
Federal Research and Testing Centre Arsenal

Co-Sponsored by

OCG (Austrian Computer Society)
IFIP Technical Committee 5 WG 5.4
IFIP Technical Committee 10 WG 10.4
European Joint Research Centre Ispra
ENCRESS

Springer

Contents

List of Contributors xi

INVITED PAPER

A. Avižienis (USA): Systematic Design of Fault-Tolerant Computers 3

SESSION 1: Formal Methods and Models

C. Bernardeschi, A. Fantechi, S. Gnesi (I): Formal Verification of Safety Requirements on Complex Systems 21

M. Heisel, C. Sühl (D): Formal Specification of Safety-Critical Software with Z and Real-Time CSP 31

J. Górski, B. Nowicki (PL): Safety Analysis Based on Object-oriented Modelling of Critical Systems 46

H.-P. Meske, W.A. Halang (D): A Processor Architecture Designed to Facilitate the Safety Certification of Hard Real Time Systems 61

SESSION 2: Testing, V&V

R. Budde, A. Merceron, K.-H. Sylla (D): Formal Verification as a Design Tool - The Transponder Lock Example 73

A. Bertolino (I), L. Strigini (UK): Acceptance Criteria for Critical Software Based on Testability Estimates and Test Results 83

W. Kuhn, H. Selami (A): Developing Dependable Software Using Prototyping and Test-Diversity 95

B. Ciciani, A. Pasquini (I): Software Reliability Models and Test Coverage 105

P. Thévenod-Fosse, C. Mazuet, Y. Crouzet (F): Defining the Unit Testing Level of Synchronous Data Flow Programs 115

J. Voas, F. Charron, K. Miller (USA): Tolerant Software Interfaces: Can COTS-based Systems be Trusted Without Them? 126

Y. Chen (South Africa), J. Arlat (F): Modeling Software Dependability Growth under Input Partition Testing 136

ROUND TABLE

A. Pasquini (I), W. Goerke (D), K. Kanoun (F) and A. Rizzo (I): An Holistic Approach to Dependability? 149

INVITED PAPER

J.-C. Laprie (F): Software-Based Critical Systems 157

SESSION 3: Reliability and Safety Assessment

W.M. Goble (USA), J.V. Bukowski (USA), A.C. Brombacher (NL): Systematic Development of Markov Models for the 1oo2D Programmable Electronic System Architecture -Analysis of Safety and Availability 173

W.J. Gutjahr (A): Failure Risk Estimation via Markov Software Usage Models 183

D.E. Sniezek (USA): Design Methodologies and Systems Safety 193

SESSION 4: Industrial Applications and Experience

R. Eriksen, T. Andersen, C. Feyling (N), H.-J. Petersen (D): Reliability and Vulnerability Assessment as Decision Support during Purchase and Design of Complex, Technical Systems 205

N. Fota, M. Kaâniche, K. Kanoun, A. Peytavin (F): Safety Analysis and Evaluation of an Air Traffic Control Computing System 219

M.J.M. Houtermans, W.M. Goble, A.C. Brombacher (NL): Creating Markov Models for Applications in the Process Industry 230

SESSION 5: Railway Applications and Experience

L.-H. Eriksson (S): Specifying Railway Interlocking Requirements for Practical Use 243

G. Aprea, P. Colantuoni, P. Firpo, R. Lido, D. Pellegrino, M. Rapone, F. Senesi (I): SIGAV, the Italian High Speed Railway Integrated Management System: Safety and Reliability Overview 250

N. Rowden (CH): A Safe, Reliable Control and Supervisory System for Railway Networks 266

S. Mitra, I.D.R. Shannon (UK): Assessment and Certification Requirements in the European Railway Industry 276

SESSION 6: Management and Development

C. Loftus, F. Long, D. Pugh, I. Pyle (UK): Failure Classification Schemes for Analysing System Dependability 289

SESSION 7: Human Factors

J. Griffyth (UK): Human Factors in High Integrity Software Development: A Field Study 301

S.J. Westerman, G.R.J. Hockey (UK): Human Factors in Safety-Critical Systems: An Underestimated Contribution? 311

R. Bloomfield, J. Bowers, L. Emmet, S. Viller (UK): PERE: Evaluation and Improvement of Dependable Processes 322

Z. Żurakowski (PL): Safety and Technology Transfer 332

INVITED PAPER

S. Visram (UK), W. Artner (A), P. Marsden (UK): Safety Case for the NERC Air Traffic Control System 345

SESSION 8: The Safety Case Legal Aspects

P.H. Jesty, K.M. Hobley (UK): Integrity Levels and their Application to Road Transport Systems 365

C.S. Turner, D.J. Richardson, J.L. King (USA): Legal Sufficiency of Testing Processes 375

SESSION 9: Security

F. Koob, M. Ullmann, S. Wittmann (D): Application of Formal Methods in the Scope of IT-Security....389

H. Stöckl (A): Reliability and Security in Communication Software: PBX Systems and CSTA Applications 395

M. Borcherding (D): Byzantine Agreement with Limited Authentication 404

F.J. Dafelmair (D): Implementation of a Security Policy in Distributed Safety Related I&C Systems - A Case Study 414

Author Index 425