Table of Contents

Invited Talk

Software Reliability Engineering in Industry 1
J. D. Musa

Assessment and Certification

A Systematic Approach to Safety Case Maintenance.. 13
T. P. Kelly, J. A. McDermid

SQUALE Dependability Assessment Criteria 27
Y. Deswarte, M. Kaâniche, P. Corneillie, and J. Goodson

Assessment and Certification of Safety-Critical Digital Architectures –
The ACRuDA Project.. 39
G. Sonneck, E. Schoitsch

Safety Assessment and Human Factors (Poster Session)

Safety Evaluation of a Train Leader Telephone System.. 46
G. Dahll

Safety Analysis Techniques for Validating Formal Models During Verification........ 58
R. de Lemos, A. Saeed

Evaluating the Contribution of DesktopVR for Safety-Critical Applications............. 67
C. Johnson

Human Performance Reliability in the Design-for-Usability Life Cycle
for Safety Human-Computer Interfaces.. 79
L. V. L. Filgueiras

The Impact of Different Media on Safety and Usability of
Interactive ATC Applications... 89
F. Paternò, C. Santoro, and S. Tahmassebi

Human Factors

Patterns for Safer Human-Computer Interfaces.. 103
A. Hussey

Impact of Communication on Systems Dependability:
Human Factors Perspectives 113
L. Rognin, J.-P. Blanquart

A Method for Operator Error Detection Based on Plan Recognition 125
J. Mo, Y. Crouzet

Safety Assessment

Hierarchically Performed Hazard Origin and Propagation Studies 139
Y. Papadopoulos, J. A. McDermid

Hardware Redundant Vital Computer – Demonstration of Safety
on the Basis of Current Standards 153
H. Krebs, S. Mitra

Design for Safety (Poster Session)

System and Software Safety Analysis for the ERA Control Computer 163
P.G. Beerthuizen, W. Kruidhof

Safety Markup Language: Concept and Application 177
C.-F. Fan, S. Yih

Extendable Ground-to-Air Communication Architecture for CoDySa 187
A. Pakstas, I. Shagaev

Hierarchical Reliability and Safety Models of Fault Tolerant Distributed Industrial Control Systems 202
J. C. Campelo, P. Yuste, F. Rodríguez, P. J. Gil, and J. J. Serrano

The Development of a Commercial „Shrink-Wrapped Application“
to Safety Integrity Level 2: The DUST-EXPERT™ Story 216
T. Clement, I. Cottam, P. Froome, and C. Jones

Verification and Testing

Safety Verification of Ada 95 Programs Using Software Fault Trees 226
S.-Y. Min, Y.-K. Jang, S.-D. Cha, Y.-R. Kwon, and D.-H. Bae

Programming Rule Static Verification for Reliable Software 239
P. Robert

Automated Black-Box Testing with Abstract VDM Oracles 250
B. K. Aichernig

Towards Statistical Control of an Industrial Test Process 260
G. Lombardi, E. Peciola, R. Mirandola, A. Bertolino, and E. Marchetti

Design for Safety

Choosing Effective Methods for Diversity – How to Progress from
Intuition to Science.. 272
P. Popov, L. Strigini, and A. Romanovsky

A First Step Towards the Integration of Accident Reports
and Constructive Design Documents.. 286
C. Johnson

A Holistic Design Concept to Improve Safety Related Control Systems 297
M. Wimmer, A. Rizzo, and M. Sujan

Dependability Analysis and Evaluation

Comparing Fault Trees and Bayesian Networks for Dependability Analysis............ 310
A. Bobbio, L. Portinale, M. Minichino, and E. Ciancamerla

FlexFi: A Flexible Fault Injection Environment for
Microprocessor-Based Systems.. 323
A. Benso, M. Rebaudengo, and M. Sonza Reorda

Structural Software Reliability Estimation 336
S. Kuball, J. May, and G. Hughes

Formal Methods and Security (Poster Session)

Hazard Analysis in Formal Specification 350
K. Sere, E. Troubitsyna

Modeling Safety-Critical Systems with Z and Petri Nets 361
M. Heiner, M. Heisel

On Formal Languages for Sequences of Authorization Transformations.................. 375
Y. Bai, V. Varadharajan

Scheduling Fault-Tolerant Programs on Multiple Processors
to Maximize Schedule Reliability... 385
I. Czarnowski, P. Jedrzejowicz, and E. Ratajczak

Formal Methods

Formal Design of Distributed Control Systems with Lustre 396
P. Caspi, C. Mazuet, R. Salem, D. Weber

Formal Specification and Development of a
Safety-Critical Train Management System... 410
A. Chiappini, A. Cimatti, C. Porzia, G. Rotondo, R. Sebastaini, P. Traverso, and A. Villafiorita

Formal Validation of the GUARDS Inter-Consistency Mechanism.......................... 420
C. Bernardeschi, A. Fantechi, S. Gnesi

A Graphical Environment for the Specification and
Verification of Reactive Systems 431
A. K. Bhattacharjee, S. D. Dhodapkar, S. Seshia, and R. K. Shyamasundar

Security

Dependability Requirements and Security Architectures
for the Healthcare/Medical Sector 445
G. Trouessin

Three-Pass Hybrid Key Establishment Protocol Based on ESIGN Signature 459
S.-M. Lee, T.-Y. Kim

The Integration of Safety and Security Requirements 468
D. P. Eames, J. Moffett

Author Index 481