

# Table of Contents

## Invited Talk

Software Reliability Engineering in Industry .....	1
<i>J. D. Musa</i>	

## Assessment and Certification

A Systematic Approach to Safety Case Maintenance.....	13
<i>T. P. Kelly, J. A. McDermid</i>	
SQUALE Dependability Assessment Criteria.....	27
<i>Y. Deswarte, M. Kaâniche, P. Corneillie, and J. Goodson</i>	
Assessment and Certification of Safety-Critical Digital Architectures – The ACRuDA Project.....	39
<i>G. Sonneck, E. Schoitsch</i>	

## Safety Assessment and Human Factors (Poster Session)

Safety Evaluation of a Train Leader Telephone System.....	46
<i>G. Dahll</i>	
Safety Analysis Techniques for Validating Formal Models During Verification.....	58
<i>R. de Lemos, A. Saeed</i>	
Evaluating the Contribution of DesktopVR for Safety-Critical Applications.....	67
<i>C. Johnson</i>	
Human Performance Reliability in the Design-for-Usability Life Cycle for Safety Human-Computer Interfaces.....	79
<i>L. V. L. Filgueiras</i>	
The Impact of Different Media on Safety and Usability of Interactive ATC Applications.....	89
<i>F. Paternò, C. Santoro, and S. Tahmassebi</i>	

## Human Factors

Patterns for Safer Human-Computer Interfaces.....	103
<i>A. Hussey</i>	

Impact of Communication on Systems Dependability: Human Factors Perspectives.....	113
<i>L. Rognin, J.-P. Blanquart</i>	
A Method for Operator Error Detection Based on Plan Recognition.....	125
<i>J. Mo, Y. Crouzet</i>	

## Safety Assessment

Hierarchically Performed Hazard Origin and Propagation Studies .....	139
<i>Y. Papadopoulos, J. A. McDermid</i>	
Hardware Redundant Vital Computer – Demonstration of Safety on the Basis of Current Standards.....	153
<i>H. Krebs, S. Mitra</i>	

## Design for Safety (Poster Session)

System and Software Safety Analysis for the ERA Control Computer .....	163
<i>P.G. Beerthuizen, W. Kruidhof</i>	
Safety Markup Language: Concept and Application .....	177
<i>C.-F. Fan, S. Yih</i>	
Extendable Ground-to-Air Communication Architecture for CoDySa.....	187
<i>A. Pakstas, I. Shagaev</i>	
Hierarchical Reliability and Safety Models of Fault Tolerant Distributed Industrial Control Systems.....	202
<i>J. C. Campelo, P. Yuste, F. Rodríguez, P. J. Gil, and J. J. Serrano</i>	
The Development of a Commercial „Shrink-Wrapped Application“ to Safety Integrity Level 2: The DUST-EXPERT™ Story.....	216
<i>T. Clement, I. Cottam, P. Froome, and C. Jones</i>	

## Verification and Testing

Safety Verification of Ada 95 Programs Using Software Fault Trees .....	226
<i>S.-Y. Min, Y.-K. Jang, S.-D. Cha, Y.-R. Kwon, and D.-H. Bae</i>	
Programming Rule Static Verification for Reliable Software .....	239
<i>P. Robert</i>	
Automated Black-Box Testing with Abstract VDM Oracles.....	250
<i>B. K. Aichernig</i>	

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

## **Design for Safety**

Choosing Effective Methods for Diversity – How to Progress from Intuition to Science.....	272
<i>P. Popov, L. Strigini, and A. Romanovsky</i>	
A First Step Towards the Integration of Accident Reports and Constructive Design Documents.....	286
<i>C. Johnson</i>	
A Holistic Design Concept to Improve Safety Related Control Systems .....	297
<i>M. Wimmer, A. Rizzo, and M. Sujan</i>	

## **Dependability Analysis and Evaluation**

Comparing Fault Trees and Bayesian Networks for Dependability Analysis.....	310
<i>A. Bobbio, L. Portinale, M. Minichino, and E. Ciancamerla</i>	
FlexFi: A Flexible Fault Injection Environment for Microprocessor-Based Systems.....	323
<i>A. Benso, M. Rebaudengo, and M. Sonza Reorda</i>	
Structural Software Reliability Estimation .....	336
<i>S. Kuball, J. May, and G. Hughes</i>	

## **Formal Methods and Security (Poster Session)**

Hazard Analysis in Formal Specification .....	350
<i>K. Sere, E. Troubitsyna</i>	
Modeling Safety-Critical Systems with Z and Petri Nets .....	361
<i>M. Heiner, M. Heisel</i>	
On Formal Languages for Sequences of Authorization Transformations.....	375
<i>Y. Bai, V. Varadharajan</i>	
Scheduling Fault-Tolerant Programs on Multiple Processors to Maximize Schedule Reliability.....	385
<i>I. Czarnowski, P. Jędrzejowicz, and E. Ratajczak</i>	

## Formal Methods

Formal Design of Distributed Control Systems with Lustre.....	396
<i>P. Caspi, C. Mazuet, R. Salem, D. Weber</i>	
Formal Specification and Development of a Safety-Critical Train Management System.....	410
<i>A. Chiappini, A. Cimatti, C. Porzia, G. Rotondo, R. Sebastaini, P. Traverso, and A. Villafiorita</i>	
Formal Validation of the GUARDS Inter-Consistency Mechanism.....	420
<i>C. Bernardeschi, A. Fantechi, S. Gnesi</i>	
A Graphical Environment for the Specification and Verification of Reactive Systems .....	431
<i>A. K. Bhattacharjee, S. D. Dhodapkar, S. Seshia, and R. K. Shyamasundar</i>	

## Security

Dependability Requirements and Security Architectures for the Healthcare/Medical Sector .....	445
<i>G. Trouessin</i>	
Three-Pass Hybrid Key Establishment Protocol Based on ESIGN Signature .....	459
<i>S.-M. Lee, T.-Y. Kim</i>	
The Integration of Safety and Security Requirements .....	468
<i>D. P. Eames, J. Moffett</i>	

<b>Author Index</b> .....	481
---------------------------	-----

Computer Safety, Reliability and Security  
18th International Conference, SAFECOMP'99,  
Toulouse, France, September 27-29, 1999,  
Proceedings  
Felici, M.; Kanoun, K.; Pasquini, A. (Eds.)  
1999, XVIII, 490 p., Softcover  
ISBN: 978-3-540-66488-8