

Table of Contents

Invited Paper

The Ten Most Powerful Principles for Quality in (Software and) Software Organizations for Dependable Systems	1
<i>Tom Gilb</i>	

Verification and Validation

Empirical Assessment of Software On-Line Diagnostics Using Fault Injection	14
<i>John Napier, John May and Gordon Hughes</i>	
Speeding-Up Fault Injection Campaigns in VHDL Models	27
<i>B. Parrotta, M. Rebaudengo, M. Sonza Reorda and M. Violante</i>	
Specification and Verification of a Safety Shell with Statecharts and Extended Timed Graphs	37
<i>Jan van Katwijk, Hans Toetenel, Abd-El-Kader Sahraoui, Eric Anderson and Janusz Zalewski</i>	
Validation of Control System Specifications with Abstract Plant Models ...	53
<i>Wenhui Zhang</i>	
A Constant Perturbation Method for Evaluation of Structural Diversity in Multiversion Software	63
<i>Luping Chen, John May and Gordon Hughes</i>	
Expert Error: The Case of Trouble-Shooting in Electronics	74
<i>Denis Besnard</i>	
The Safety Management of Data-Driven Safety-Related Systems	86
<i>A. G. Faulkner, P. A. Bennett, R. H. Pierce, I. H. A. Johnston and N. Storey</i>	
Software Support for Incident Reporting Systems in Safety-Critical Applications	96
<i>Chris Johnson</i>	

Software Process Improvement

A Dependability-Explicit Model for the Development of Computing Systems	107
<i>Mohamed Kaâniche, Jean-Claude Laprie and Jean-Paul Blanquart</i>	

Deriving Quantified Safety Requirements in Complex Systems	117
<i>Peter A. Lindsay, John A. McDermid and David J. Tombs</i>	
Improving Software Development by Using Safe Object Oriented Development: OTCD	131
<i>Xavier Méhaut and Pierre Morère</i>	
A Safety Licensable PES for SIL 4 Applications	141
<i>Wolfgang A. Halang, Peter Vogrin and Matjaž Colnarič</i>	
Safety and Security Issues in Electric Power Industry	151
<i>Zdzisław Żurkowski</i>	
Dependability of Computer Control Systems in Power Plants	165
<i>Cláudia Almeida, Alberto Arazo, Yves Crouzet and Karama Kanoun</i>	
A Method of Analysis of Fault Trees with Time Dependencies	176
<i>Jan Magott and Paweł Skrobanek</i>	

Formal Methods

A Formal Methods Case Study: Using Light-Weight VDM for the Development of a Security System Module	187
<i>Georg Droschl, Walter Kuhn, Gerald Sonneck and Michael Thuswald</i>	
Formal Methods: The Problem Is Education	198
<i>Thierry Scheurer</i>	
Formal Methods Diffusion: Past Lessons and Future Prospects	211
<i>R. Bloomfield, D. Craigen, F. Koob, M. Ullmann and S. Wittmann</i>	

Invited Paper

Safe Tech: A Control Oriented Viewpoint	227
<i>Maarten Steinbuch</i>	

Safety Guidelines, Standards and Certification

Derivation of Safety Targets for the Random Failure of Programmable Vehicle Based Systems	240
<i>Richard Evans and Jonathan Moffett</i>	
IEC 61508 – A Suitable Basis for the Certification of Safety-Critical Transport-Infrastructure Systems??	250
<i>Derek Fowler and Phil Bennett</i>	

Hardware Aspects

- An Approach to Software Assisted Recovery
from Hardware Transient Faults for Real Time Systems 264
D. Basu and R. Paramasivam
- Programmable Electronic System Design & Verification Utilizing DFM 275
*Michel Houtermans, George Apostolakis, Aarnout Brombacher
and Dimitrios Karydas*
- SIMATIC S7-400F/FH: Safety-Related Programmable Logic Controller ... 286
Andreas Schenk

Safety Assessment I

- Assessment of the Reliability of Fault-Tolerant Software:
A Bayesian Approach 294
Bev Littlewood, Peter Popov and Lorenzo Strigini
- Estimating Dependability of Programmable Systems Using BBNs 309
*Bjørn Axel Gran, Gustav Dahll, Siegfried Eisinger, Eivind J. Lund,
Jan Gerhard Norstrøm, Peter Strocka and Britt J. Ystanes*

Design for Safety

- Improvements in Process Control Dependability
through Internet Security Technology 321
Ferdinand J. Dafelmair
- A Survey on Safety-Critical Multicast Networking 333
James S. Pascoe and R. J. Loader

Invited Paper

- Causal Reasoning about Aircraft Accidents 344
Peter B. Ladkin

Transport & Infrastructure

- Controlling Requirements Evolution: An Avionics Case Study 361
Stuart Anderson and Massimo Felici
- HAZOP Analysis of Formal Models
of Safety-Critical Interactive Systems 371
Andrew Hussey

Failure Mode and Effect Analysis for Safety-Critical Systems
with Software Components 382
Tadeusz Cichocki and Janusz Górski

Safety Assessment II

Risk Ordering of States in Safecharts 395
Nimal Nissanke and Hamdan Dammag

Dependability Evaluation: Model and Method Based on Activity Theory .. 406
Mark-Alexander Sujan, Antonio Rizzo and Alberto Pasquini

Forensic Software Engineering and the Need
for New Approaches to Accident Investigation 420
Chris Johnson

Author Index431