

## Contents

### Formal Methods I - Analysis and Specification

CoRSA - A Constraint Based Approach to Requirements and Safety Analysis .....	3
<i>K. Hollingworth and A. Saeed</i>	
An Agenda for Specifying Software Components with Complex Data Models .....	16
<i>K. Winter, T. Santen and M. Heisel</i>	
Safety in Production Cell Components: An Approach Combining Formal Real-Time Specifications and Patterns .....	32
<i>H. Rust</i>	
Safety Properties Ensured by the OASIS Model for Safety Critical Real-Time Systems .....	45
<i>V. David, J. Delcoigne, E. Leret, A. Ourghanlian, P. Hilsenkopf and P. Paris</i>	
Linking Hazard Analysis to Formal Specification and Design in B .....	60
<i>K. Lano, P. Kan and A. Sanchez</i>	

### Management and Human Factors

Controlling Your Design through Your Software Process.....	77
<i>N. Martín-Vivaldi and P. Isacsson</i>	
Operator Errors and Their Causes.....	89
<i>T. Grams</i>	

### Security

A Performance Comparison of Group Security Mechanisms .....	103
<i>A. Hutchison and M. Wallbaum</i>	
Towards Secure Downloadable Executable Content: The Java Paradigm.....	117
<i>J. Iliadis, S. Gritzalis and V. Oikonomou</i>	
Model and Implementation of a Secure SW-Development Process for Mission Critical Software .....	128
<i>F. Dafelmair</i>	
Impact of Object-Oriented Software Engineering Applied to the Development of Security Systems.....	143
<i>S. Jovalekic and B. Rist</i>	

## Medical Informatics

'Profit by Safety' or Quackery in Biomedical Information Technology? .....	159
<i>B.A. de Mol and F. Koornneef</i>	

## Formal Methods II - Languages and Verification

Towards Automated Proof of Fail-safe Behaviour .....	169
<i>P. Liggesmeyer and M. Rothfelder</i>	
Verifying a Time-Triggered Protocol in a Multi-language Environment .....	185
<i>A. Merceron, M. Müllerburg and G.M. Pinna</i>	
Methods and Languages for Safety-Related Real-Time Programming .....	196
<i>W.A. Halang and A.H. Frigeri</i>	
ANSI-C in Safety Critical Applications - Lessons-Learned from Software Evaluation .....	209
<i>A. Lindner</i>	

## Applications

A Structured Approach to the Formal Certification of Safety of Computer Aided Development Tools .....	221
<i>P. Bertoli, A. Cimatti, F. Giunchiglia and P. Traverso</i>	
Applying Formal Methods in Industry - The UseGat Project.....	231
<i>S. Bologna, R. Bove, G. Dipoppa, G. Biondi, G. Mongardi, C. Porzia, B.G. Mortensen and N. Kirkegaard</i>	
Increasing System Safety for by-wire Applications in Vehicles by Using a Time-Triggered Architecture .....	243
<i>Th. Ringler, J. Steiner, R. Belschner and B. Hedenetz</i>	
Fault-Tolerant Communication in Large-Scale Manipulators .....	254
<i>H.-D. Kochs, W. Geisselhardt, H. Hilmer and M. Lenord</i>	
Distributed Fault-Tolerant and Safety-Critical Application in Vehicles – A Time-Triggered Approach .....	267
<i>E. Dilger, T. Fuehrer and B. Müller</i>	
Model Checking Safety-Critical Software with SPIN: An Application to a Railway Interlocking System.....	284
<i>A. Cimatti, F. Giunchiglia, G. Mongardi, D. Romano, F. Torielli and P. Traverso</i>	
EURIS, a Specification Method for Distributed Interlockings .....	296
<i>F.v.Dijk, W. Fokkink, G. Kolk, P.v.d.Ven and B.v.Vlijmen</i>	

Object Oriented Safety Analysis of an Extra High Voltage Substation Bay .....	306
<i>B. Nowicki and J. Górski</i>	

### **Formal Methods III - Petri Nets**

Integration of Logical and Physical Properties of Embedded Systems by Use of Time Petri Nets .....	319
<i>F. Saglietti</i>	

Safety Verification of Software Using Structured Petri Nets .....	329
<i>K. Sacha</i>	

### **Reliability**

Refinement of Safety-Related Hazards into Verifiable Code Assertions .....	345
<i>K. Wong and J. Joyce</i>	

A Conceptual Comparison of Two Commonly Used Safeguarding Principles .....	359
<i>B. Knegtering and A. Brombacher</i>	

A Holistic View on the Dependability of Software-Intensive Systems .....	369
<i>G. Sonneck, E. Schoitsch and L. Strigini</i>	

Verifying Integrity of Decision Diagrams .....	380
<i>R. Drechsler</i>	

<b>Author Index</b> .....	391
---------------------------	-----

<http://www.springer.com/978-3-540-65110-9>

Computer Safety, Reliability and Security  
17th International Conference, SAFECOMP'98,  
Heidelberg Germany, October 5-7, 1998, Proceedings  
Ehrenberger, W. (Ed.)  
1998, XVI, 404 p., Softcover  
ISBN: 978-3-540-65110-9