

Rune Winther Bjørn Axel Gran  
Gustav Dahll (Eds.)

# Computer Safety, Reliability, and Security

24th International Conference, SAFECOMP 2005  
Fredrikstad, Norway, September 28-30, 2005  
Proceedings

 Springer

# Table of Contents

CMMI RAMS Extension Based on CENELEC Railway Standard <i>Jose Antonio Fonseca, Jorge Rady de Almeida Júnior</i> .....	1
The Importance of Single-Source Engineering of Emergency and Process Shutdown Systems <i>Robert Martinez, Torgeir Enkerud</i> .....	13
Combining Extended UML Models and Formal Methods to Analyze Real-Time Systems <i>Nawal Addouche, Christian Antoine, Jacky Montmain</i> .....	24
Defining and Decomposing Safety Policy for Systems of Systems <i>Martin Hall-May, Tim Kelly</i> .....	37
Generalising Event Trees Using Bayesian Networks with a Case Study of Train Derailment <i>George Bearfield, William Marsh</i> .....	52
Control and Data Flow Testing on Function Block Diagrams <i>Eunkyoung Jee, Junbeom Yoo, Sungdeok Cha</i> .....	67
Comparing Software Measures with Fault Counts Derived from Unit-Testing of Safety-Critical Software <i>Wolfgang Herzner, Stephan Ramberger, Thomas Länger, Christian Reumann, Thomas Gruber, Christian Sejkora</i> .....	81
Automatic Analysis of a Safety Critical Tele Control System <i>Edoardo Campagnano, Ester Ciancamerla, Michele Minichino, Enrico Tronci</i> .....	94
A Formal Model for Fault-Tolerance in Distributed Systems <i>Brahim Hamid, Mohamed Mosbah</i> .....	108
Model-Based Safety Analysis of Simulink Models Using SCADE Design Verifier <i>Anjali Joshi, Mats P.E. Heimdahl</i> .....	122
Using Safety Critical Artificial Neural Networks in Gas Turbine Aero-Engine Control <i>Zeshan Kurd, Tim P. Kelly</i> .....	136

On the Effectiveness of Run-Time Checks	
<i>Meine J.P. van der Meulen, Lorenzo Strigini, Miguel A. Revilla</i> . . . . .	151
A Technique for Fault Tolerance Assessment of COTS Based Systems	
<i>Ruben Alexandersson, D. Krishna Chaitanya, Peter Öhman, Yasir Siraj</i> . . . . .	165
Finding Upper Bounds for Software Failure Probabilities – Experiments and Results	
<i>Monica Kristiansen</i> . . . . .	179
Justification of Smart Sensors for Nuclear Applications	
<i>Peter Bishop, Robin Bloomfield, Sofia Guerra, Kostas Turlas</i> . . . . .	194
Evolutionary Safety Analysis: Motivations from the Air Traffic Management Domain	
<i>Massimo Felici</i> . . . . .	208
Public-Key Cryptography and Availability	
<i>Tage Stabell-Kulø, Simone Lupetti</i> . . . . .	222
End-To-End Worst-Case Response Time Analysis for Hard Real-Time Distributed Systems	
<i>Lei Wang, Mingde Zhao, Zengwei Zheng, Zhaohui Wu</i> . . . . .	233
Safety Interfaces for Component-Based Systems	
<i>Jonas Elmqvist, Simin Nadjm-Tehrani, Marius Minea</i> . . . . .	246
A Safety-Related PES for Task-Oriented Real-Time Execution Without Asynchronous Interrupts	
<i>Martin Skambraks</i> . . . . .	261
Are High-Level Languages Suitable for Robust Telecoms Software?	
<i>J.H. Nyström, P.W. Trinder, D.J. King</i> . . . . .	275
Functional Apportioning of Safety Requirements on Railway Signalling Systems	
<i>Ola Løkberg, Øystein Skogstad</i> . . . . .	289
Automatic Code Generation for PLC Controllers	
<i>Krzysztof Sacha</i> . . . . .	303

The TACO Approach for Traceability and Communication of Requirements	
<i>Terje Sivertsen, Rune Fredriksen, Atoosa P-J Thunem, Jan-Erik Holmberg, Janne Valkonen, Olli Ventä, Jan-Ove Andersson</i> .....	317
An IEC 62061 Compliant Safety System Design Method for Machinery	
<i>Bengt Ljungquist, Thomas Thelin</i> .....	330
Design Evaluation: Estimating Multiple Critical Performance and Cost Impacts of Designs	
<i>Tom Gilb</i> .....	344
The Application of an Object-Oriented Method in Information System Security Evaluation	
<i>Qiang Yan, Hua-ying Shu</i> .....	357
Towards a Cyber Security Reporting System – A Quality Improvement Process	
<i>Jose J. Gonzalez</i> .....	368
Security Research from a Multi-disciplinary and Multi-sectoral Perspective	
<i>Atoosa P-J Thunem</i> .....	381
Problem Frames and Architectures for Security Problems	
<i>Denis Hatebur, Maritta Heisel</i> .....	390
<b>Author Index</b> .....	405