

Contents

SESSION 1: GENERAL ISSUES, GUIDELINES

<i>E. Schoitsch (A): Software Best Practices in Dependable Systems: The European Research Projects ENCRESS, OLOS and ESPITI From a Partner's Perspective</i>	3
<i>H. Krebs (D): Assessment on the Basis of Standards – Gaps and How to Bridge Them</i>	12

SESSION 2: SAFETY ANALYSIS

<i>A. Saeed, R. de Lemos, T. Anderson (UK): Safety Analysis for Requirements Specifications: Methods and Techniques</i>	27
<i>M.F. Chudleigh, J.R. Catmur, F. Redmill (UK): A Guideline for HAZOP Studies on Systems Which Include a Programmable Electronic System</i>	42
<i>J.M. Voas, K.W. Miller (USA): An Automated Code-Based Fault-Tree Mitigation Technique</i>	59

SESSION 3: FORMAL METHODS

<i>K.Chan, C. Fencott, B. Hebborn (UK): Formal Support for the Safety Analysis of Requirement Models</i>	75
<i>J. Górski, J. Magott, A. Wardziński (PL): Modelling Fault Trees Using Petri Nets</i>	90
<i>A.J. Harrison, I.D.R. Shannon (UK): The Application of Formal Methods to Railway Signalling Systems Specification and the ESPRIT III Project CASCADE</i>	101
<i>J.A. McDermid, R.H. Pierce (UK): Accessible Formal Method Support for PLC Software Development</i>	113

SESSION 4: HUMAN AND LEGAL ASPECTS

<i>R.J. Tiezema (NL): Eliminating the Unexpected</i>	131
<i>S.J. Westerman, N.M. Shryane, C.M. Crawshaw, G.R.J. Hockey, C.W. Wyatt-Millington (UK): Cognitive Diversity: A Structured Approach to Trapping Human Error</i>	142
<i>D. Davis (UK): Legal Aspects of Safety Critical Systems</i>	156

INVITED PAPER

<i>B. Littlewood, D. Wright (UK): A Bayesian Model that Combines Disparate Evidence for the Quantitative Assessment of System Dependability</i>	173
---	-----

SESSION 5: DESIGN

<i>M. Heisel (D): Six Steps Towards Provably Safe Software</i>	191
<i>W.A. Halang, B.J. Krämer, N. Völker (D): Formally Verified Firmware Modules for Industrial Process Automation</i>	206

SESSION 6: ASSESSMENT

<i>G. Picciolo, P. Gianninò (I): Programmable Electronic Controllers (PEC) Performance Assessment – An Approach for Reliability Quantification</i>	221
--	-----

<i>F. Engelmann (CH), W. Schynoll (D), H. Stienen (CH): BOOTSTRAP: Software Process Assessment – Experiences and Further Developments</i>	237
<i>K.M. Hobley, P.H. Jesty (UK): Analysis and Assessment of Advanced Road Transport Telematic Systems</i>	252

SESSION 7: SAFE SOFTWARE

<i>J. Blieberger (A): Loops for Safety Critical Applications</i>	269
<i>M. Viola (CAN): Ontario Hydro's Experience with New Methods for Engineering Safety Critical Software</i>	283
<i>K.N. Narahari, S. Prasad, K. Karunakar (IND): Is Software Safe to Fly?</i>	299

SESSION 8: APPLICATIONS I

<i>E. Ruiz Morales (EC): A Software Development Approach for Robotics Control Systems</i>	317
<i>J. Christmansson, Z. Kalbarczyk, J. Torin (S): An Attempt to Evaluate Functional Diversity Employed in a Reactor Protection System</i>	331
<i>A. Coombes, J. McDermid, J. Moffett (UK), P. Morris (EC): Requirements Analysis and Safety: A Case Study (Using GRASP)</i>	353

SESSION 9: APPLICATIONS II

<i>A.J.C. Sharkey, N.E. Sharkey, G.O. Chandroth (UK): Neural Nets and Diversity</i>	375
<i>C. Rabéjac (F): On-Line Software Error Detection by Executable Assertions: From Theory to Practice</i>	390
<i>D. Hughes (UK): The Use of Animated Graphical Simulation Techniques to Facilitate Safe Operation, Assembly and Disassembly of Safety Critical Equipment and Systems</i>	403

INVITED PAPER

<i>J.-P. Heckmann, S. Shirlaw (F): An Industrial View of Requirements Engineering and Safety</i>	411
--	-----

SESSION 10: CASE STUDIES

<i>P. Fenelon, T.P. Kelly, J.A. McDermid (UK): Safety Cases for Software Application Reuse</i>	419
<i>P.G. Bishop, R.E. Bloomfield (UK): The SHIP Safety Case Approach</i>	437
<i>M. El Koursi, B. Letrung, H. Waeselynck, F. Baranowski (F): Safety Case: Structure and Role</i>	452

SESSION 11: VALIDATION AND VERIFICATION

<i>M. Hietikko, R. Tiisanen (FIN): Practical Approach for the Evaluation of Safety Related Programmable Electronics</i>	467
<i>A. Anselmi, C. Bernardeschi, A. Fantechi, S. Gnesi, S. Larosa, G. Mongardi, F. Torielli (I): An Experience in Formal Verification of Safety Properties of a Railway Signalling Control System</i>	474
<i>A. Bondavalli, S. Chiaradonna, F. Di Giandomenico, S. La Torre (I): Dependability of Iterative Software: A Model for Evaluating the Effects of Input Correlation</i>	489
<i>T. Jennings, P. Taylor (UK): The Verification of Compiled Code</i>	504
Author Index	515