

Contents

List of Contributors ix

Safe Software

H Papini, F Simon: Software-based Safety-critical Systems: a Taxonomy 3

G Dahll: Safety Assessment of Software Based Systems 14

H Thane: Safe and Reliable Computer Control Systems: an Overview 25

S Scheer, T Maier: Towards Dependable Software Requirement Specifications 37

Safety Cases, Management and Development

T P Kelly, J A McDermid: Safety Case Construction and Reuse Using Patterns 55

P A Lindsay, J A McDermid: A Systematic Approach to Software Safety Integrity Levels 70

M Wilikens, M Masera, D Vallero: Integration of Safety Requirements in the Initial Phases of the Project Lifecycle of Hardware/Software Systems 83

D Jenkins, B Lees, D Livingstone, A Reglinski: Managing the Safety Argument using a Memory Prosthesis 98

Security and Human Factors

J Braband: Safety and Security Requirements for an Advanced Train Control System 111

S Gritzalis, D Spinellis: Cryptographic Protocols over Open Distributed Systems: A Taxonomy of Flaws and related Protocol Analysis Tools 123

A M Dearden, M D Harrison: Using Executable Interactor Specifications to Explore the Impact of Operator Interaction Errors 138

X Yi, K-Y Lam, Y-F Han: Design, Analysis and Implementation of a New Hash Function Based on Block Cipher 148

D Polemi: Biometric Techniques Applied in Security Technology 158

Guidelines, Standards and Certification

<i>B A Wichmann: High Integrity Ada</i>	173
<i>P D Edwards, R S Rivett, G F McCall: Towards an Automotive 'Safer Subset' of C</i>	185
<i>S P Wilson, J A McDermid, P M Kirkham, C H Pygott, D J Tombs: Computer Based Support for Standards and Processes in Safety Critical Systems</i>	197
<i>K Tourlas: An Assessment of the IEC 1131-3 Standard on Languages for Programmable Controllers</i>	210

Formal Methods and Models

<i>K Lano: Refinement and Safety Analysis</i>	223
<i>R Lichtenegger, K Gotthardt: Automated Verification of Safety Requirements using CCS and Binary Decision Diagrams</i>	241
<i>Y Lebbah: Consistency Checking by Type Inference and Constraint Satisfaction</i>	253
<i>B Mermet, D Méry: Safe Combinations of Services using B</i>	265
<i>M Cepin, R de Lemos, B Mavko, S Riddle, A Saeed: An Object-Based Approach to Modelling and Analysis of Failure Properties</i>	281
<i>M Heisel, C Sühl: Methodological Support for Formally Specifying Safety-Critical Software</i>	295

Applications and Industrial Experience

<i>P Baufreton, X Méhaut, É Rutten: Embedded Systems in Avionics and the SACRES Approach</i>	311
<i>P R Croll, C Chambers, M Bowell, P W H Chung: Towards Safer Industrial Computer Controlled Systems</i>	321
<i>S Barker, I Kendall, A Darlison: Safety Cases for Software-intensive Systems: an Industrial Experience Report</i>	332

Testing, Validation and Verification

<i>F Saglietti: Dynamic Decision on Checkpointing by Use of Reduced Ordered Binary Decision Diagrams</i>	345
<i>I T Nabney, M J S Paven, R C Eldridge, C Lee: Practical Assessment of Neural Network Applications</i>	357
<i>J C Knight, L G Nakano: Software Test Techniques for System Fault-Tree Analysis</i>	369

Author Index	381
---------------------------	-----