Contents

Formal Methods I - Analysis and Specification

CoRSA - A Constraint Based Approach to Requirements and Safety Analysis ...............3
  K. Hollingworth and A. Saeed

An Agenda for Specifying Software Components with Complex Data Models .............16
  K. Winter, T. Santen and M. Heisel

Safety in Production Cell Components: An Approach Combining Formal
Real-Time Specifications and Patterns .................................................................32
  H. Rust

Safety Properties Ensured by the OASIS Model for Safety Critical
Real-Time Systems ................................................................................................45
  V. David, J. Delcoigne, E. Leret, A. Ourghanlian, P. Hilsenkopf and P. Paris

Linking Hazard Analysis to Formal Specification and Design in B .......................60
  K. Lano, P. Kan and A. Sanchez

Management and Human Factors

Controlling Your Design through Your Software Process ......................................77
  N. Martín-Vivaldi and P. Isacsson

Operator Errors and Their Causes .......................................................................89
  T. Grams

Security

A Performance Comparison of Group Security Mechanisms .............................103
  A. Hutchison and M. Wallbaum

Towards Secure Downloadable Executable Content: The Java Paradigm ..........117
  J. Iliadis, S. Gritzalis and V. Oikonomou

Model and Implementation of a Secure SW-Development Process for
Mission Critical Software ....................................................................................128
  F. Dafelmair

Impact of Object-Oriented Software Engineering Applied to the Development of
Security Systems .................................................................................................143
  S. Jovalekic and B. Rist
Medical Informatics

‘Profit by Safety’ or Quackery in Biomedical Information Technology? .......... 159
B.A. de Mol and F. Koornneef

Formal Methods II - Languages and Verification

Towards Automated Proof of Fail-safe Behaviour .............................................. 169
P. Liggesmeyer and M. Rothfelder

Verifying a Time-Triggered Protocol in a Multi-language Environment .......... 185
A. Merceron, M. Müllerburg and G.M. Pinna

Methods and Languages for Safety-Related Real-Time Programming .......... 196
W.A. Halang and A.H. Frigeri

A. Lindner

Applications

A Structured Approach to the Formal Certification of Safety of Computer Aided Development Tools .............................................................. 221
P. Bertoli, A. Cimatti, F. Giunchiglia and P. Traverso

Applying Formal Methods in Industry - The UseGat Project ....................... 231
S. Bologna, R. Bove, G. Dipoppa, G. Biondi, G. Mongardi, C. Porzia,
B.G. Mortensen and N. Kirkegaard

Increasing System Safety for by-wire Applications in Vehicles by Using a
Time-Triggered Architecture ........................................................................ 243
Th. Ringler, J. Steiner, R. Belschner and B. Hedenetz

Fault-Tolerant Communication in Large-Scale Manipulators ....................... 254
H.-D. Kochs, W. Geiselhardt, H. Hilmer and M. Lenord

Distributed Fault-Tolerant and Safety-Critical Application in Vehicles –
A Time-Triggered Approach .......................................................................... 267
E. Dilger, T. Fuehrer and B. Müller

Model Checking Safety-Critical Software with SPIN: An Application to a Railway Interlocking System ......................................................... 284
A. Cimatti, F. Giunchiglia, G. Mongardi, D. Romano, F. Torielli and P. Traverso

EURIS, a Specification Method for Distributed Interlockings ......................... 296
Object Oriented Safety Analysis of an Extra High Voltage Substation Bay ..........306
B. Nowicki and J. Górski

Formal Methods III - Petri Nets

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

Safety Verification of Software Using Structured Petri Nets ..............................329
K. Sacha

Reliability

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

A Conceptual Comparison of Two Commonly Used Safeguarding Principles ......359
B. Knegtering and A. Brombacher

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

Verifying Integrity of Decision Diagrams ..........................................................380
R. Drechsler

Author Index ............................................................................................................391