1. Record Nr. UNINA9910143469003321

Titolo	Computer safety, reliability and security : 17th international conference, safecomp'98, heidelberg, germany, october 5-7, 1998 : proceedings / / edited by Wolfgang Ehrenberger
Pubbl/distr/stampa	Berlin, Germany ; ; New York, New York : , : Springer, , [1998] Â©1998
ISBN	3-540-49646-7
Edizione	[1st ed. 1998.]
Descrizione fisica	1 online resource (XVI, 404 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1516
Disciplina	005.1
Soggetti	Computer systems - Reliability Computer security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Formal Methods I - Analysis and Specification -- CoRSA - A Constraint Based Approach to Requirements and Safety Analysis -- An Agenda for Specifying Software Components with Complex Data Models -- Safety in Production Cell Components: An Approach Combining Formal Real Time Specifications and Patterns -- Safety Properties Ensured by the OASIS Model for Safety Critical Real-Time Systems -- Linking Hazard Analysis to Formal Specification and Design in B -- Management and Human Factors -- Controlling Your Design through Your Software Process -- Operator Errors and Their Causes -- Security -- A Performance Comparison of Group Security Mechanisms -- Towards Secure Downloadable Executable Content: The JAVA Paradigm -- Model and Implementation of a Secure SW-Development Process for Mission Critical Software -- Impact of Object-Oriented Software Engineering Applied to the Development of Security Systems -- Medical Informatics -- “Profit by Safety” or Quackery in Biomedical Information Technology? -- Formal Methods II - Languages and Verification -- Towards Automated Proof of Fail-Safe Behavior -- Verifying a time-triggered protocol in a multi-language environment -- Methods and Languages for Safety Related Real Time Programming -- ANSI-C in Safety Critical Applications Lessons-Learned from Software Evaluation -- Applications -- A Structured Approach to the Formal Certification of Safety of

Computer Aided Development Tools -- Applying Formal Methods in Industry The UseGat Project -- Increasing System Safety for By-Wire Applications in Vehicles by Using a Time Triggered Architecture -- Fault-Tolerant Communication in Large-Scale Manipulators -- Distributed Fault Tolerant and Safety Critical Applications in Vehicles - A Time-Triggered Approach -- Model Checking Safety Critical Software with SPIN: an Application to a Railway Interlocking System -- EURIS, a Specification Method for Distributed Interlockings -- Object Oriented Safety Analysis of an Extra High Voltage Substation Bay -- Formal Methods III - Petri Nets -- Integration of Logical and Physical Properties of Embedded Systems by Use of Time Petri Nets -- Safety Verification of Software Using Structured Petri Nets -- Reliability -- Refinement of Safety-Related Hazards into Verifiable Code Assertions -- Conceptual Comparison of two Commonly Used Safeguarding Principles -- A Holistic View on the Dependability of Software-Intensive Systems -- Verifying Integrity of Decision Diagrams.

Sommario/riassunto

Computers and their interactions are becoming the characteristic features of our time: Many people believe that the industrial age is going over into the information age. In the same way as life of the beginning of this century was dominated by machines, factories, streets and railways, the starting century will be characterised by computers and their networks. This change naturally affects also the institutions and the installations our lives depend upon: power plants, including nuclear ones, chemical plants, mechanically working factories, cars, railways and medical equipment; they all depend on computers and their connections. In some cases it is not human life that may be endangered by computer failure, but large investments; e. g. if a whole plant interrupts its production for a long time. In addition to loss of life and property one must not neglect public opinion, which is very critical in many countries against major technical defects. The related computer technology, its hardware, software and production process differ between standard applications and safety related ones: In the safety case it is normally not only the manufacturers and the customers that are involved, but a third party, usually an assessor, who is taking care of the public interest on behalf of a state authority. Usually safety engineers are in a better position than their colleagues from the conventional side, as they may spend more time and money on a particular task and use better equipment.