1. Record Nr. UNINA9910768476303321

Titolo	Computer safety, reliability and security : 18th international conference, safecomp'99, toulouse, france, september 27-29, 1999, proceedings / / edited by Massimo Felici, Karama Kanoun, Alberto Pasquini
Pubbl/distr/stampa	Berlin, Germany ; ; New York, New York : , : Springer, , [1999] Â©1999
ISBN	3-540-48249-0
Edizione	[1st ed. 1999.]
Descrizione fisica	1 online resource (XVIII, 490 p.)
Collana	Lecture Notes in Computer Science, , 0302-9743 ; ; 1698
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	Invited Talk -- Software Reliability Engineering in Industry -- Assessment and Certification -- A Systematic Approach to Safety Case Maintenance -- SQUALE Dependability Assessment Criteria -- Assessment and Certification of Safety-Critical Digital Architectures — the ACRuDA Project -- Safety Assessment and Human Factors (Poster Session) -- Safety Evaluation of a Train Leader Telephone System -- Safety Analysis Techniques for Validating Formal Models during Verification -- Evaluating the Contribution of DesktopVR for Safety—Critical Applications -- Human Performance Reliability in the Design-for-Usability Life Cycle for Safety Human-Computer Interfaces -- The Impact of Different Media on Safety and Usability of Interactive ATC Applications -- Human Factors -- Patterns for Safer Human-Computer Interfaces -- Impact of Communication on Systems Dependability: Human Factors Perspectives -- A Method for Operator Error Detection Based on Plan Recognition -- Safety Assessment -- Hierarchically Performed Hazard Origin and Propagation Studies -- Hardware Redundant Vital Computers — Demonstration of Safety on the Basis of Current Standards -- Design for Safety (Poster Session) -- System and Software Safety Analysis for the ERA Control Computer -- Safety Markup Language: Concept and Application -- Extendable Ground-to-Air Communication Architecture for CoDySa -- Hierarchical Reliability

and Safety Models of Fault Tolerant Distributed Industrial Control Systems -- The Development of a Commercial “Shrink-Wrapped Application” to Safety Integrity Level 2: the DUST-EXPERT™ Story -- Verification and Testing -- Safety Verification of ADA95 Programs Using Software Fault Trees -- Programming Rule Static Verification for Reliable Software -- Automated Black-Box Testing with Abstract VDM Oracle -- Towards Statistical Control of an Industrial Test Process -- Design for Safety -- Choosing Effective Methods for Diversity — How to Progress from Intuition to Science -- A First Step Towards the Integration of Accident Reports and Constructive Design Documents -- A Holistic Design Concept to Improve Safety Related Control Systems -- Dependability Analysis and Evaluation -- Comparing Fault Trees and Bayesian Networks for Dependability Analysis -- FlexFi: A Flexible Fault Injection Environment for Microprocessor-Based Systems -- Structural Software Reliability Estimation -- Formal Methods and Security (Poster Session) -- Hazard Analysis in Formal Specification -- Modeling Safety-Critical Systems with Z and Petri Nets -- On Formal Languages for Sequences of Authorization Transformations -- Scheduling Fault-Tolerant Programs on Multiple Processors to Maximize Schedule Reliability -- Formal Methods -- Forma Design of Distributed Control Systems with Lustre -- Formal Specification and Development of a Safety-Critical Train Management System -- Formal Validation of the GUARDS Inter-consistency Mechanism -- A Graphical Environment for the Specification and Verification of Reactive Systems -- Security -- Dependability Requirements and Security Architectures for the Healthcare/Medical Sector -- Three-Pass Hybrid Key Establishment Protocol Based on ESIGN Signature -- The Integration of Safety and Security Requirements.

Sommario/riassunto

The European Commission emphasizes, in its Fifth Research Framework, the “. . . emerging generic dependability requirements in the information society, stemming both from the ubiquity and volume of embedded and networked systems and services as well as from the global and complex nature of large scale information and communication infrastructures, from citizens, administrations and business in terms of technologies, tools, systems, applications and services". The series of Conference on Computer Safety, Reliability, and Security (Safecomp) contributes to satisfy these requirements by reviewing the state of the art, experiences, and new trends in the relevant scientific and industrial areas. Safecomp is intended to be a platform for technology transfer among academia, industry, and research institutions, providing the opportunity for exchange of ideas, opinions, and visions among experts. This year Safecomp celebrates the 20th anniversary, its first Conference having been organized in Stuttgart by EWICS (European Workshop on Industrial Computer Systems) in 1979, and we hope these Proceedings will contribute to the celebration by supporting Safecomp aims. The Proceedings include the 25 papers that have been presented orally at the Conference and the full version of the 14 papers that have been presented as posters, all of which were selected from 76 submissions. Papers almost uniformly take up Safecomp topics, dealing with the issues of Safety Assessment and Human Factors, Verification and Validation, Design for Safety, Formal Methods, and Security.