

1. Record Nr.	UNISA996466275803316
Titolo	Computer Safety, Reliability, and Security [[electronic resource] ] : 29th International Conference, SAFECOMP 2010, Vienna, Austria, September 14-17, 2010, Proceedings // edited by Erwin Schoitsch
Pubbl/distr/stampa	Berlin, Heidelberg : , : Springer Berlin Heidelberg : , : Imprint : Springer, , 2010
ISBN	1-280-38886-2 9786613566782 3-642-15651-7
Edizione	[1st ed. 2010.]
Descrizione fisica	1 online resource (X, 482 p. 197 illus.)
Collana	Programming and Software Engineering ; ; 6351
Disciplina	005.1
Soggetti	Software engineering Computer security Computer communication systems Algorithms Computers and civilization Software Engineering/Programming and Operating Systems Systems and Data Security Computer Communication Networks Software Engineering Algorithm Analysis and Problem Complexity Computers and Society
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	Session 1 -- Reliability Analysis of Safety-Related Communication Architectures -- A Novel HAZOP Study Approach in the RAMS Analysis of a Therapeutic Robot for Disabled Children -- Variability Management of Safety and Reliability Models: An Intermediate Model towards Systematic Reuse of Component Fault Trees -- QoS Analysis of Weighted Multi-state Probabilistic Networks via Decision Diagrams -- Session 2 -- Comparison between IEC 60880 and IEC 61508 for Certification Purposes in the Nuclear Domain -- Deriving Safety Cases

for Hierarchical Structure in Model-Based Development -- Assurance of Automotive Safety – A Safety Case Approach -- How to “Survive” a Safety Case According to ISO 26262 -- Session 3 -- Benchmarking Software Requirements Documentation for Space Application -- Verifying Mode Consistency for On-Board Satellite Software -- Computational Concerns in the Integration of Unmanned Airborne Systems into Controlled Airspace -- Session 4 -- Residual Error Probability of Embedded CRC by Stochastic Automata -- ANB- and ANBDMem-Encoding: Detecting Hardware Errors in Software -- Session 5 -- Field Test Methods for a Co-operative Integrated Traffic Management System -- 100% Coverage for Safety-Critical Software – Efficient Testing by Static Analysis -- MODIFI: A MODEL-Implemented Fault Injection Tool -- Automated Test Coverage Measurement for Reactor Protection System Software Implemented in Function Block Diagram -- Session 6 -- Overcoming Non-determinism in Testing Smart Devices: A Case Study -- Software Testing by People with Autism -- Session 7 -- Information Flow Analysis of Energy Management in a Smart Grid -- Integrated Cyber-Physical Fault Injection for Reliability Analysis of the Smart Grid -- A Metric for Measuring the Strength of Inter-dependencies -- Session 8 -- Security Analysis of Open Building Automation Systems -- A UML Profile for Requirements Analysis of Dependable Software -- Session 9 -- Model-Based Safety Engineering of Interdependent Functions in Automotive Vehicles Using EAST-ADL2 -- Experiences in Applying Formal Verification in Robotics -- Evolving a Safe System Design Iteratively -- An Approach to Using Non Safety-Assured Programmable Components in Modest Integrity Systems -- Session 10 -- Development of High-Integrity Software Product Lines Using Model Transformation -- On the Safety Implications of E-Governance: Assessing the Hazards of Enterprise Information Architectures in Safety-Critical Applications -- The Right Degree of Configurability for Safety-Critical Embedded Software in Variable Message Signs -- INDEXYS, a Logical Step beyond GENESYS -- Session 11 -- Integrating System Modelling with Safety Activities -- Aspect-Oriented Implementation of Fault Tolerance: An Assessment of Overhead -- Invited Talks (Keynote Abstracts) -- System of Systems Challenges -- Murphy Was an Optimist -- Process Control Security: Go Dutch! (United, Shared, Lean and Mean).

---

## Sommario/riassunto

Computers and microprocessors are indispensable in modern technical systems, their deployment spanning the domains automotive, railway, aerospace, and transportation, security, energy supply, telecommunication, critical infrastructures and process industries. They perform tasks that a few decades ago were very difficult if not impossible. As they perform these tasks with increasing efficiency, more and more tasks are shifted from hardware to software, which means that the dependability of computer systems becomes crucial for the safety, security and reliability of technical systems. With the so-called “embedded systems” (becoming more and more intelligent, networked and co-operating with each other, with humans and the environment) computers have invaded all aspects of daily life. New paradigms have arisen, like ubiquitous computing, systems-of-systems, energy and resource awareness, enormous complexity issues and the like, requiring a more holistic systems view as well. So, after 31 years of SAFECOMP, the emphasis of the 29 event is on critical embedded systems, which are almost omnipresent. Their impact on our lives, risks and challenges are often not well understood (underestimated or exaggerated). The primary issue is to cope with complexity, new failure modes and resource management, due to shrinking feature size, multi-core systems and management of multiple

variants, while maintaining dependability properties and robustness.

---