1. Record Nr. UNISA990000862810203316

Autore	PSELLOS, Michal
Titolo	Imperatori di Bisanzio : Cronografia / Michele Psello ; introduzione di Dario Del Corno ; testo critico a cura di Salvatore Impellizzeri ; commento di Ugo Crisuolo ; traduzione di Silvia Ronchey
Pubbl/distr/stampa	Milano, : Fondazione Lorenzo Villa, : A. Mondadori, 1993
ISBN	88-04-25015-1 88-04-25016-X
Edizione	[2.ed.]
Descrizione fisica	2 v. ; 21 cm
Collana	Scrittori greci e latini
Disciplina	949.5
Collocazione	V.1. Coll.21/ 28/1(VIII A COLL 118/37 I) V.1. Coll.21/ 28/2(VIII A COLL 118/37 II)
Lingua di pubblicazione	Italiano
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Testo originale a fronte
Nota di contenuto	Vol.1 : Libri 1.-6., 75.- Vol.2 : Librin 6., 76-7.

2. Record Nr. UNISALENTO991001098099707536

Titolo	L'insegnamento di Paolo sull'unità della Chiesa (1 Cor 1; Ef 4) : X seminario di esegesi patristica relizzato a Corinto (Grecia), 14-20 aprile 2009 / a cura di Rosario Scognamiglio e Mario Girardi
Pubbl/distr/stampa	Bari : Ecumenica editrice, 2010
ISBN	9788888758534
Descrizione fisica	167 p. ; 25 cm
Collana	Analecta nicolaiana ; 10
Altri autori (Persone)	Scognamiglio, Rosario Girardi, Mario
Lingua di pubblicazione	Italiano
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Contiene riferimenti bibliografici. Indice

3. Record Nr. UNINA9910886991403321

Autore	Ceccarelli Andrea
Titolo	Computer Safety, Reliability, and Security : 43rd International Conference, SAFECOMP 2024, Florence, Italy, September 18–20, 2024, Proceedings / / edited by Andrea Ceccarelli, Mario Trapp, Andrea Bondavalli, Friedemann Bitsch
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	9783031686061 3031686063
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (325 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14988
Altri autori (Persone)	TrappMario BondavalliAndrea BitschFriedemann
Disciplina	004.6
Soggetti	Computer networks Software engineering Information technology - Management Robotics Microprogramming Computer networks - Security measures Computer Communication Networks Software Engineering Computer Application in Administrative Data Processing Control Structures and Microprogramming Mobile and Network Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Fault Injection and Tolerance -- In-Memory Zero-Space Floating-Point-Based CNN Protection Using Non-significant and Invariant Bits -- 1 Introduction -- 2 Background -- 3 Proposed Methodology -- 3.1 Identification of non-Significant bits -- 3.2 Location of invariant bits -- 4 Case Study: LeNet-5 and GoogLeNet -- 4.1 Locating Non-Significant Bits -- 4.2 Locating Invariant Bits -- 4.3 Proposed Error Correcting Codes -- 4.4 Overhead

Estimation of the Proposed ECCs -- 5 Discussion -- 6 Conclusions -- References -- A Failure Model Library for Simulation-Based Validation of Functional Safety -- 1 Introduction -- 2 Related Work -- 3 A Failure Model Library for Simulation-Based FI -- 3.1 Failure Model Collection -- 3.2 Failure Model Semantics -- 4 Case Study -- 5 Limitations -- 6 Conclusion -- References -- Strategic Resilience Evaluation of Neural Networks Within Autonomous Vehicle Software -- 1 Introduction -- 2 Autonomous Driving Frameworks -- 2.1 L4 System: LBC -- 2.2 L2 System: OpenPilot -- 2.3 Driving Simulator: CARLA -- 3 Methodology -- 3.1 Vulnerable Weights: Taylor Guided Fault Injection (TGFI) -- 3.2 Experimental Campaigns -- 4 Resilience Evaluation -- 4.1 Resilience of L4 LBC -- 4.2 Resilience of L2 OpenPilot -- 5 Mitigation -- 5.1 L4 LBC: Ranger -- 5.2 L2 OpenPilot: Driver Intervention -- 6 Case Studies and Discussion -- 6.1 Importance of Layer Depth for Resilience -- 6.2 Sensitivity to Single and Multi-bit Faults -- 6.3 Lessons Learned from L4 LBC and L2 OpenPilot -- 7 Related Work -- 8 Conclusions -- References -- System and Software Safety Assurance -- Reconciling Safety Measurement and Dynamic Assurance -- 1 Introduction -- 2 Conceptual Background -- 3 Motivating Example -- 3.1 Baseline Safety -- 3.2 Practical Drift -- 4 Framework -- 4.1 Defining Safety Metrics and Indicators.
4.2 Updating and Revising the Operational Risk Assessment -- 4.3 Characterizing the Change to Safety Risk -- 4.4 Numerical Examples -- 5 Towards Formal Foundations -- 6 Concluding Remarks -- References -- Safety Invariant Engineering for Interlocking Verification -- 1 Introduction -- 2 Safety Invariants -- 2.1 Requirements -- 2.2 Current Solutions -- 3 Property Engineering -- 3.1 Eliciting Safety Properties from Standards -- 3.2 Reducing the Number of False Positives -- 3.3 Redefining What the Property Violation Is -- 3.4 Regression Testing of Developed Safety Invariants -- 4 Discussion and Conclusions -- References -- Assurance Case Synthesis from a Curated Semantic Triplestore -- 1 Introduction -- 2 The Rapid Assurance Curation Kit (RACK) -- 3 Automated GSN Synthesis from RACK -- 3.1 The GSN Ontology -- 3.2 Project-Specific GSN Pattern Example -- 3.3 Automated Synthesis of GSN Fragments Using Patterns -- 3.4 GUI Support for GSN Generation and Analysis -- 4 Related Work -- 5 Conclusion -- References -- CyberDS: Auditable Monitoring in the Cloud -- 1 Introduction -- 2 Motivating Example -- 3 Monitoring Approach -- 3.1 Specification Language -- 3.2 Security Monitor -- 3.3 Tamper-Proof Claim Database and Auditability -- 4 Claim Revision Control -- 4.1 Revision Model -- 4.2 Monitoring with Revisions -- 5 Implementation and Experimental Results -- 6 Discussion -- 7 Related Work -- 7.1 Runtime Monitoring -- 7.2 Auditability of System Events -- 8 Conclusion -- References -- Automated Driving Systems -- Anatomy of a Robotaxi Crash: Lessons from the Cruise Pedestrian Dragging Mishap -- 1 Introduction -- 2 Background -- 2.1 Terminology -- 2.2 Crash Context and Overview -- 3 Crash Details -- 3.1 Crash Timeline -- 3.2 Crash Analysis -- 3.3 Potential Lessons -- 4 The Immediate Response -- 4.1 Immediate Response Timeline -- 4.2 Post-Crash Analysis.
4.3 Potential Lessons -- 5 Organizational Response -- 5.1 Organizational Response Analysis -- 5.2 Potential Lessons -- 6 Conclusions -- References -- Comprehensive Change Impact Analysis Applied to Advanced Automotive Systems -- 1 Introduction -- 2 Background on CIA for Incremental Safety Assurance -- 3 Running Example -- 4 Original Vehicle Family Models Stage 0 -- 4.1 HARA Metamodels -- 4.2 HAZOP Metamodels -- 4.3 Verification Metamodel -- 4.4 Instance Models -- 4.5 Instances for Stage 0 -- 5 CIA After a

Change to the Battery Management System -- 5.1 Identifying Direct Changes - Stage 1 -- 5.2 Identifying Potential Impacts in the System - Stage 2 -- 5.3 Confirming Actual Impacts in the System - Stage 3 -- 5.4 Identifying Potential Impacts in the Assurance Case - Stage 4 -- 5.5 Confirming Actual Impacts in the Assurance - Stage 5 -- 5.6 Incremental Assurance - Stages 6 and 7 -- 6 Discussion -- 7 Conclusion -- References -- A Case Study of Continuous Assurance Argument for Level 4 Automated Driving -- 1 Introduction -- 2 Related Work -- 3 A Case Study in a Local City -- 3.1 Top Level of Assurance Case for Level 4 Automated Driving -- 3.2 GSN Module M2 for Identification of Risk and Hazard -- 3.3 GSN Module M4 for Evaluation and Validation -- 4 A Toolchain of an Assurance Case Tool and a Monitoring System -- 5 Lessons Obtained from the Case Study -- 6 Concluding Remarks -- References -- Security of Safety-Critical Systems -- TitanSSL: Towards Accelerating OpenSSL in a Full RISC-V Architecture Using OpenTitan Root-of-Trust -- 1 Introduction -- 2 Background and Related Works -- 3 Hardware Architecture -- 4 TitanSSL Software Architecture -- 4.1 Application Processor -- 4.2 Security Controller -- 5 Experimental Results -- 5.1 Comparison with Software Implementation -- 5.2 OpenTitan Firmware Analysis -- 6 Security Assumptions and Implications.
7 Conclusion -- References -- A Lightweight and Responsive On-Line IDS Towards Intelligent Connected Vehicles System -- 1 Introduction -- 2 Methodology -- 2.1 System Overview -- 2.2 Threat Model -- 2.3 ML-BF Model -- 2.4 Feature Engineering -- 2.5 Blacklist Filter -- 3 Implementation -- 3.1 Testbed Setting -- 3.2 Dataset Selection -- 3.3 Data Pre-processing -- 3.4 Machine Learning Approaches Adoption -- 3.5 Model Training -- 4 Experimental Results -- 4.1 Evaluation Metrics -- 4.2 Detection Performance -- 4.3 Computational Consumption -- 4.4 Analysis and Discussion -- 5 Related Work -- 5.1 Machine Learning for Intrusion Detection in ICV -- 5.2 Lightweight IDS in ICV -- 5.3 Responsive IDS in ICV -- 6 Conclusion -- References -- Evaluating the Vulnerability Detection Efficacy of Smart Contracts Analysis Tools -- 1 Introduction -- 2 Background -- 3 Related Works -- 4 Experimental Study Methodology -- 5 Experimental Study Results -- 5.1 RQ1: Contests Versus Vulnerabilities -- 5.2 RQ2: Tools Versus Vulnerabilities -- 5.3 RQ3: Tools in Theory Versus Tools in Practice -- 5.4 RQ4: Analysis Complexity Versus Tool Efficacy -- 6 Conclusions -- References -- Safety-Security Analysis via Attack-Fault-Defense Trees: Semantics and Cut Set Metrics -- 1 Introduction -- 2 Related Work -- 3 Case Study: Gridshield -- 4 Background -- 5 Attack-Fault-Defense Trees -- 5.1 Formal Definition of AFDT -- 5.2 Gridshield AFDT -- 6 Qualitative Analysis of AFDT -- 7 Safety and Security Dependencies via MCS -- 8 Conclusion and Future Work -- References -- Safety Verification -- Coyan: Fault Tree Analysis - Exact and Scalable -- 1 Introduction -- 2 Preliminaries -- 3 Computing Unreliability Values -- 4 Unreliability Through WMC of Tseitin Transformation -- 5 Implementation -- 6 Experimentation -- 6.1 Benchmarks -- 6.2 Results -- 6.3 Industrial Benchmarks -- 7 Concluding Remarks. References -- Safety Argumentation for Machinery Assembly Control Software -- 1 Introduction -- 2 Background -- 2.1 EN ISO 13849:2023 -- 2.2 Assurance Cases -- 2.3 Contract-Based Design -- 3 SAMACS: Safety Argumentation for Machinery Assembly Control Software -- 4 Case Study -- 4.1 Establishment of Software Responsibility -- 4.2 Definition of Software Safety Goals -- 4.3 Identification of Software Safety Requirements -- 4.4 Definition of Contracts -- 4.5 Identification of Verification Techniques and Evidence Provision -- 4.6 Composing the Safety Case Arguments -- 5 Discussion -- 6 Related Work -- 7

Conclusions and Future Work -- References -- Sound Non-interference Analysis for C/C++ -- 1 Introduction -- 2 Sound Static Source Code Analysis -- 3 Data and Control Flow Errors -- 4 Data and Control Flow Analysis -- 5 Taint Analysis -- 5.1 Modeling Interference -- 5.2 Signal Flow Analysis -- 5.3 Freedom of Interference Between Software Components -- 6 Experimental Results -- 7 Related Work -- 8 Conclusion -- References -- Autonomous Systems -- A Dynamic Assurance Framework for an Autonomous Survey Drone -- 1 Introduction -- 2 Related Literature -- 3 Case Study and Monitor Examples -- 3.1 Monitoring Battery State and Required Power Consumption -- 3.2 Monitoring and Predicting Task Scheduling and Executing Times -- 3.3 Reconfigurations Calculation -- 4 Dynamic Assurance Case Approach -- 4.1 Battery Monitor Assurance Case -- 4.2 Discussion -- 4.3 Online Monitoring Interface -- 5 Conclusions -- References -- Redefining Safety for Autonomous Vehicles -- 1 Introduction -- 2 Existing Safety Definitions -- 2.1 ISO 26262 -- 2.2 ISO 21448 -- 2.3 ANSI/UL 4600 -- 2.4 Other Safety Definitions -- 3 Examples of AV Safety Problems -- 4 What is Missing from Safety Definitions -- 4.1 Open World Environment -- 4.2 Self-enforcement of Operational Limitations.
4.3 Ad Hoc Systems of Systems.

Sommario/riassunto

This book constitutes the refereed proceedings of the 43rd International Conference on Computer Safety, Reliability and Security, SAFECOMP 2024, held in Florence, Italy, in September 2024. The 19 full papers included in this volume were carefully reviewed and selected from 80 submissions. They have been organized in topical sections as follows: Fault Injection and Tolerance; System and Software Safety Assurance; Automated Driving Systems; Security of safety-critical systems; Safety Verification; and Autonomous Systems.