1. Record Nr. UNINA9910886992003321

Autore	Ceccarelli Andrea
Titolo	Computer Safety, Reliability, and Security. SAFECOMP 2024 Workshops : DECSoS, SASSUR, TOASTS, and WAISE, Florence, Italy, September 17, 2024, Proceedings / / edited by Andrea Ceccarelli, Mario Trapp, Andrea Bondavalli, Erwin Schoitsch, Barbara Gallina, Friedemann Bitsch
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	9783031687389 3031687388
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (474 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14989
Altri autori (Persone)	TrappMario BondavalliAndrea SchoitschErwin GallinaBarbara BitschFriedemann
Disciplina	004.6
Soggetti	Computer networks Image processing - Digital techniques Computer vision Information technology - Management Software engineering Computer science Data protection Computer Communication Networks Computer Imaging, Vision, Pattern Recognition and Graphics Computer Application in Administrative Data Processing Software Engineering Theory of Computation Security Services
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- 19th International ERCIM/EWICS Workshop on Dependable Smart Embedded Cyber-

Physical Systems and Systems-of Systems (DECSoS 2024) -- 19th International Workshop on Dependable Smart Cyber-Physical Systems and Systems-of-Systems (DECSoS 2024) -- 1 Introduction -- 2 This Year's Workshop -- Organization -- International Program Committee 2024 -- A Systems Viewpoint on the Integration of Subsystems Developed with Heterogeneous Safety Standards -- 1 The Need for Integration -- 2 Why Existing Standards Don't Play Nicely Together -- 2.1 How Existing Standards Differ -- 2.2 Current Approaches to Importance Metrics -- 2.3 Summary of Integration Challenges -- 3 Addressing the Integration Issue -- 3.1 Existing Approaches -- 3.2 The IEC 63187 Approach -- 4 Conclusion -- References -- Intelligent Decision-Making in Lane Detection Systems Featuring Dynamic Framework for Autonomous Vehicles -- 1 Introduction -- 2 Background -- 2.1 AI-Based Approaches -- 2.2 Non AI-Based Approaches -- 2.3 Hybrid Approaches -- 3 Proposed Dynamic Framework -- 3.1 Experimental Setup - Vehicle Demonstrator -- 3.2 Conventional Algorithm -- 3.3 PilotNetC Architecture -- 4 Results -- 4.1 Results for Conventional Algorithms -- 4.2 Results for PilotNetC -- 4.3 The Dynamic Framework -- 5 Conclusion -- References -- Security and Safety in Urban Environments: Evaluating Threats and Risks of Autonomous Last-Mile Delivery Robots -- 1 Introduction -- 2 The Last-Mile Robot in Our Case Study -- 3 Case Study Modeling and Analysis -- 3.1 Extended Multi-level Model -- 3.2 Attack Types -- 4 Analysis of Attack Types and Human-Safety Levels -- 5 Ideas for a Theoretical Approach -- 6 Summary and Outlook -- References -- Safe Road-Crossing by Autonomous Wheelchairs: A Novel Dataset and Its Evaluation -- 1 Introduction -- 2 Related Works.
3 Reference Scenario for Safe Road-Crossing -- 4 Design of the Danger Function -- 5 Dataset Generation -- 5.1 Lab Environment -- 5.2 Data Collection and Preprocessing -- 5.3 Data Elaboration and Sensor Fusion -- 6 Experimental Evaluation -- 7 Threats to Validity -- 8 Conclusions -- References -- Automating an Integrated Model-Driven Approach to Analysing the Impact of Cyberattacks on Safety -- 1 Introduction -- 2 Safety-Critical Networked Control Systems -- 3 Security-Explicit SysML Modelling of NCSs -- 3.1 SysML Modeling of NCSs -- 3.2 Modelling Cyberattacks in SysML -- 4 Modelling and Refinement in Event-B -- 5 Generation of Event-B Specification from SysML Model -- 5.1 Architecture of SysMLToEventB -- 5.2 The Tool-Chain -- 5.3 Tool Validation -- 6 Related Work and Conclusions -- References -- Securing Web Access: PUF-Driven Two-Factor Authentication for Enhanced Protection -- 1 Introduction -- 1.1 Contributions -- 2 Related Work -- 3 Preliminaries -- 3.1 Physically Unclonable Function -- 3.2 Network Model -- 3.3 Threat Assumptions -- 4 Two-Factor User Authentication Using PUF -- 4.1 Enrollment Phase -- 4.2 Authentication Phase -- 5 Security Analysis -- 5.1 Formal Security Analysis -- 5.2 Informal Analysis -- 6 Experimental Validation and Performance Analysis -- References -- Enhancing Tunnel Safety with Artery V2X Simulation for Real-Time Risk Assessment -- 1 Introduction -- 2 Related Work -- 3 Artery-Based Risk Assessment Framework -- 3.1 Artery Simulation Framework (Upper Part) -- 3.2 Data Manipulation and Risk Assessment (Lower Part) -- 4 Case Study: Simulation-Based Risk Assessment in Zederhaus Tunnel -- 4.1 Breakdown Scenario: Artery and SUMO Model -- 4.2 Breakdown Scenario: Risk Assessment -- 5 Conclusion and Future Work -- References -- Detecting and Mitigating Errors in Neural Networks -- 1 Introduction -- 2 State of the Art.
2.1 Error Correcting Memory (ECC Memory) -- 2.2 Memory Tagging -- 2.3 Storage Reduction -- 2.4 2-D ECC/2-D Cyclic Redundancy Check

(CRC) -- 3 Layer Properties -- 4 The Proposed Framework -- 4.1 Preparation Step -- 4.2 Error Detection Phase -- 4.3 Error Correction Phase -- 5 Practical Examples -- 5.1 Deviation in the Weight -- 5.2 Deviation in the Architecture or the Activation Function -- 6 Conclusion -- References -- 11th International Workshop on Next Generation of System Assurance Approaches for Critical Systems (SASSUR 2024) -- 11th International Workshop on Next Generation of System Assurance Approaches for Critical Systems (SASSUR 2024) -- 1 Introduction -- 2 This Year's Workshop -- Organization -- Workshop Committees -- Organization Committee -- Programme Committee -- Additional Reviewers -- Challenges and Limitations of Utilizing Multi-core/Heterogeneous Logic Elements in the Railway Signaling Applications -- 1 Introduction -- 2 Railway Signaling System -- 3 EN 50129:2018: Hardware Requirements and Guidelines to Achieve SIL 4 -- 4 Architecture of State-of-the-Art Object Controller -- 5 Analysis of Using the Latest Logic Elements in Railway Signaling Systems -- 6 Conclusion -- 7 Future Work -- References -- Identifying Difficult Environmental Conditions with Scenario-Based Hazard and Fault Analysis -- 1 Introduction -- 2 Related Work -- 3 Identifying Triggering Conditions with SHFA -- 3.1 Step One: Scenario Modelling -- 3.2 Step Two: Hazardous Maneuver Identification -- 3.3 Step Three: Triggering Condition Identification -- 4 Illustrative Example -- 4.1 Scenario Modelling -- 4.2 Hazardous Maneuver Identification -- 4.3 Triggering Condition Identification -- 5 Result Analysis and Discussion -- 5.1 Triggering Condition Formalization -- 5.2 Findings -- 5.3 Capabilities and Limitations -- 6 Conclusion and Outlook -- References.
Using GPT-4 to Generate Failure Logic -- 1 Introduction -- 2 FLAGPT: Developing a Failure Logic Analysis GPT -- 3 Task and System Descriptions -- 4 Results and Working Experience -- 4.1 Tank Overfill Failure Event -- 4.2 Air Bleed Cabin Supply System -- 4.3 Aircraft Wheel Brake and Gas Leak Systems -- 4.4 Alignment and Consistency -- 5 Conclusions -- References -- Towards an Argument Pattern for the Use of Safety Performance Indicators -- 1 Introduction -- 2 Background -- 3 A High-Level Argument Structure for Using SPIs -- 3.1 Systematic Definition of SPIs -- 3.2 Collection and Analysis of SPIs -- 3.3 Response to SPI Violations -- 4 Critical Analysis of the Argument About SPIs -- 5 Meta-SPIs to Validate the Argument About SPIs -- 6 Related Work -- 7 Summary and Future Work -- References -- Enabling Theory-Based Continuous Assurance: A Coherent Approach with Semantics and Automated Synthesis -- 1 Introduction -- 2 Methodological Foundations for Continuous Assurance -- 2.1 Composing Assurance Cases with Theories and Defeater Patterns -- 2.2 Assessing Assurance Case for Soundness and Validity -- 3 Tools Support for Continuous Assurance -- 3.1 Property-Driven Semantics with LLM Support and Synthesized Prolog Logic-Based Analysis -- 3.2 Synthesis Assistant for Generating Assurance Cases -- 3.3 Continuous Assurance for CI/CD Software Designs Using ETB -- 4 Conclusion -- References -- Managing Changing Product Liability Obligations Emerging from New Proposed EU Directive -- 1 Introduction -- 1.1 Background -- 1.2 Recent and Ongoing Changes to the Legal Framework -- 1.3 Scope and Structure -- 2 How Automation Impacts Risk and Liability Obligations -- 3 The Socio-technical System Perspective -- 4 Impact of New EU Product Liability Directive -- 4.1 Overview of Changes -- 4.2 Overall Impact on Product Liability Obligations.
4.3 Impact on Liability Obligations Due to the Presumption of Defectiveness -- 4.4 Impact on Liability Obligations Due

to the Presumption of Causality -- 5 Thoughts on Transparent and Efficient Management of Product Liability Obligations -- 5.1 Manufacturers' Defense Strategies -- 5.2 Liability Obligations Expressed in Modular Assurance Cases and Contracts -- 5.3 Integration of Present Assurance Cases Required by Standards -- 5.4 Capture Confidence in the Strength of Defense Through Independent and Continuous Assessments of the Modular Assurance Cases -- 5.5 Using Assurance Cases for Rebutting Other Presumptions in New PLD -- 6 Discussion, Conclusions and Further Work -- References -- Reaching Consensus on System-of-Systems Resilience Assurance: A Case of Mobility as a Service -- 1 Introduction -- 2 Concepts and Related Works -- 2.1 System Theoretic Process Analysis -- 2.2 Consensus Process Model -- 2.3 Mobility as a Service -- 3 Resilience Argumentation -- 3.1 Step 1: Identify Loss Scenarios -- 3.2 Step 2: Identify Resilience Requirement -- 4 Conflict and Consensus -- 4.1 Assumption -- 4.2 Conflict -- 4.3 Consensus Process Model -- 4.4 Example -- 5 Conclusion and Further Work -- References -- A Deductive Approach to Safety Assurance: Formalising Safety Contracts with Subjective Logic -- 1 Introduction -- 2 Background -- 2.1 Safety Assurance -- 2.2 Subjective Logic -- 3 A Formally Grounded Assurance Argument Structure -- 4 Constructing the Argument and Computing Confidence -- 5 Related Work -- 6 Discussion and Conclusions -- References -- A New Approach to Creating Clear Operational Safety Arguments -- 1 Introduction -- 2 Related Work -- 3 Proposed Approach -- 4 Illustrative Examples -- 5 Conclusions and Future Work -- References -- Including Defeaters in Quantitative Confidence Assessments for Assurance Cases -- 1 Introduction. 2 Adding Defeaters to Confidence Assessment.

Sommario/riassunto

This book constitutes the proceedings of the Workshops held in conjunction with the 43rd International Conference on Computer Safety, Reliability, and Security, SAFECOMP 2024, which took place in Florence, Italy, during September 2024. The 36 papers included in this book were carefully reviewed and selected from a total of 64 submissions to the following workshops: DECSoS 2024 – 19th Workshop on Dependable Smart Embedded and Cyber-Physical Systems and Systems-of-Systems SASSUR 2024 - 11th International Workshop on Next Generation of System Assurance Approaches for Critical Systems TOASTS 2024 – Towards A Safer Systems' Architecture Through Security WAISE 2024 – 7th International Workshop on Artificial Intelligence Safety Engineering.