1. Record Nr. UNISA996673179203316

Autore	Torngren Martin
Titolo	Computer Safety, Reliability, and Security. SAFECOMP 2025 Workshops : CoC3CPS, DECSoS, SASSUR, SENSEI, SRToITS, and WAISE, Stockholm, Sweden, September 9, 2025, Proceedings / / edited by Martin Törngren, Barbara Gallina, Erwin Schoitsch, Elena Troubitsyna, Friedemann Bitsch
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2026
ISBN	3-032-02018-2
Edizione	[1st ed. 2026.]
Descrizione fisica	1 online resource (808 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 15955
Altri autori (Persone)	GallinaBarbara SchoitschErwin TroubitsynaElena 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	-- 1st International Workshop on Co-Design of Communication, Computing, and Control in Cyber-Physical Systems (CoC3CPS 2025). -- An end-to-end testbed for communication, compute, and control

co-design: the Kista Innovation Park. -- Real-Time Control Selection over the Computing Continuum. -- Temporal Intent-Aware Multi-Agent Learning for Network Optimization. -- 20th International Workshop on Dependable Smart Cyber-Physical Systems and Systems-of-Systems (DECSoS 2025). -- Dependable AI Inference - A work-in-progress on CPU, Co-Processor and FPGA Approaches. -- Methodology for Test Case Allocation based on a Formalized ODD. -- Safety-Aware Strategy Synthesis for Autonomous System of Systems with UPPAAL. -- From Bouncing Break-ins to Frictional Firewalls: Interacting Requirements for Vehicle Safety and Security. -- A ThreatGet-Based Framework for Aligning System Security with the Cyber Resilience Act. -- i7Fuzzer: Neural-Guided Fuzzing for Enhancing Security Testing of Stateful Protocols. -- HyLLM-IDS: A Conceptual Hybrid LLM-Assisted Intrusion Detection Framework for Cyber-Physical Systems. -- PROTECTION: Provably Robust Intrusion Detection system for IoT through recursive Delegation. -- Towards Credible Simulators: A Validation Methodology for Safety-Critical Virtual Testing. -- Cybersecurity in Partitioned Space Embedded Systems. -- 12th International Workshop on Next Generation of System Assurance Approaches for Critical Systems (SASSUR 2025). -- A GSN-Based Requirement Analysis of the EU AI Regulation. -- A Safety Argument Fragment Towards Safe Deployment of Performant Automated Driving Systems. -- Certus: A domain specific language for confidence assessment in assurance cases. -- Doubt in Safety Claims is Inevitable: What is its Impact, and How to Deal with it?. -- Ensuring Information Security in Inclusive Digital Environments. -- Functional Safety with Model-Based Safety Analysis: A Perspective from ARP4761A. -- High-Performance AI Inference for Agile Deployment on Space-Qualified Processors: A Performance Benchmarking Study. -- SCALOFT: An Initial Approach for Situation Coverage-Based Safety Analysis of an Autonomous Aerial Drone in a Mine. -- 4th International Workshop on Safety-Security Interaction (SENSEI 2025). -- Trick or Treat: A Study of Human Detection of Manipulative Tactics in Phishing Emails. -- Rational Verification in Repeated Security Games. -- Quantitative Assessment of Energy Efficiency, Comfort, and Safety in an Intelligent Heating System Under False Data. -- Cyber-Safety Assessment of Wind Turbines: A Reachability Analysis Approach Against Cyber-Attacks. -- 2nd International Workshop on Safety/Reliability/Trustworthiness of Intelligent Transportation Systems (SRToITS 2025). -- Scenario Hazard Prevention for Autonomous Driving Based on Improved STPA. -- Alexandru Forrai. Systematic test scenario generation and risk assessment for automated driving system. -- AV-SLAF: A Scenario-Layered Framework for Safety Analysis of Autonomous Vehicles Based on STPA and CTA. -- Applying Machine Learning towards the Recognition of Driving Behavior. -- External Human-Machine Interaction Design Principles and Supporting Technologies for Autonomous Vehicles. -- Formal Analysis of Resilience in Transport Systems with Bigraphs. -- Vehicle-Level Safety Validation of AD/ADAS Systems via Extreme Value Analysis. -- 8th International Workshop on Artificial Intelligence Safety Engineering (WAISE 2025). -- A Modular AI Testing Framework for Trustworthy AI: Proof-of-Concept Implementation. -- Architectural Mitigation of Control AI Risk Factors for Safe Human-Robot-Collaboration. -- Uncovering Unsafe Feature Interactions in Vehicle Control Using Generative AI and Digital Twins. -- AURORA Networks: Auto-associative Universal Real-time Outlier Risk Assessment Networks. -- Does not impute! Performance and ethical implications of missing data for an AI-based diabetes co-morbidity predictor. -- Facilitating Fault Tree Analysis with Generative

AI. -- Efficient Safety Retrofitting Against Jailbreaking for LLMs. -- Risk Analysis of One-Pixel Image Defects in Safety-Critical Deep Neural Networks. -- Safe Adversarial Control Through Interaction.

Sommario/riassunto

This book constitutes the proceedings of the Workshops held in conjunction with the 44th International Conference on Computer Safety, Reliability, and Security, SAFECOMP 2025, which took place in Stockholm, Sweden, during September 2025. The 43 papers included in this book were carefully reviewed and selected from a total of 61 submissions to the following six workshops: · CoC3CPS 2025, Co-Design of Communication, Computing and Control in Cyber-Physical Systems · DECSoS 2025 – 20th Workshop on Dependable Smart Embedded and Cyber-Physical Systems and Systems-of-Systems · SASSUR 2025 - 12th International Workshop on Next Generation of System Assurance Approaches for Critical Systems · SENSEI 2025 – 4th International Workshop on Safety and Security Interaction · SRToITS 2025 – 2nd International Workshop on Safety/Reliability/Trustworthiness of Intelligent Transportation Systems · WAISE 2025 – 8th International Workshop on Artificial Intelligence Safety Engineering.