1. Record Nr.	UNISA996418299503316
Titolo	Computer Safety, Reliability, and Security [[electronic resource]] : 39th International Conference, SAFECOMP 2020, Lisbon, Portugal, September 16–18, 2020, Proceedings / / edited by António Casimiro, Frank Ortmeier, Friedemann Bitsch, Pedro Ferreira
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2020
ISBN	3-030-54549-0
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (XXIII, 450 p. 251 illus., 78 illus. in color.)
Collana	Programming and Software Engineering ; ; 12234
Disciplina	005.8
Soggetti	Computer organization Artificial intelligence Software engineering Microprogramming Data encryption (Computer science) Computer security Computer Systems Organization and Communication Networks Artificial Intelligence Software Engineering/Programming and Operating Systems Control Structures and Microprogramming Cryptology Systems and Data Security
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Safety Cases and Argumentation -- Synthesis of Runtime Safety Monitors for Cyber-Physical Systems with Digital Dependability Identities -- Systematic Evaluation of (Safety) Assurance Cases -- Just Enough Formality in Assurance Argument Structures -- Towards Recertification of Modular Updates in Integrated Maritime Systems of Systems -- Formal Verification and Analysis -- A functional verification methodology for highly configurable, continuously operating safety-critical FPGA designs: Applied to the CERN RadiatiOn Monitoring

Electronics (CROME) -- A Compositional Semantics for Repairable BDMPs -- Model-Based Safety Analysis of Mode Transitions -- Efficient Translation of Safety LTL to DFA using Symbolic Automata Learning and Inductive Inference -- Security Modelling and Methods -- Automated Attacker Synthesis for Distributed Protocols -- An Attacker Modeling Framework for the Assessment of Cyber-Physical Systems Security -- Predicting Railway Signalling Commands using Neural Networks for Anomaly Detection -- Automated Anomaly Detection in CPS Log Files - A Time Series Clustering Approach -- Assurance of Learning-enabled Systems -- Assuring the Safety of Machine Learning for Pedestrian Detection at Crossings -- Safety-Aware Hardening of 3D Object Detection Neural Network Systems -- Model-Centered Assurance for Autonomous Systems -- A Safety Framework for Critical Systems Utilising Deep Neural Networks -- Assurance Argument Elements for Off-the-Shelf, Complex Computational Hardware -- Quantifying Assurance in Learning-enabled Systems -- Practical Experience and Tools -- Cyber Security of Neural Networks in Medical Devices -- FASTEN.Safe: A Model-driven Engineering Tool to Experiment with Checkable Assurance Cases -- Threat Analysis and Risk Mitigation -- On Validating Attack Trees with Attack Effects -- Safety meets Security: Using ISA-62443 for a Highly Automated Road Vehicle -- Threat Analysis Framework for Safety Architectures in SCDL -- Cyber-Physical Systems Security -- Efficient Load-Time Diversity for an Embedded Real-Time Operating System -- Towards an Automated Exploration of Secure IoT/CPS Design-Variants -- Securing Electric Vehicle Charging Systems through Component Binding -- Fault Injection and Fault Tolerance -- Using Hardware-In-Loop-Based Fault Injection to Determine the Effects of Control Flow Errors in Industrial Control Programs -- On Configuring a Testbed for Dependability Experiments: Guidelines and Fault Injection Case Study -- A Classification of Faults Covering the Human-Computer Interaction Loop.

Sommario/riassunto

This book constitutes the proceedings of the 39th International Conference on Computer Safety, Reliability and Security, SAFECOMP 2020, held in Lisbon, Portugal, in September 2020.* The 27 full and 2 short papers included in this volume were carefully reviewed and selected from 116 submissions. They were organized in topical sections named: safety cases and argumentation; formal verification and analysis; security modelling and methods; assurance of learning-enabled systems; practical experience and tools; threat analysis and risk mitigation; cyber-physical systems security; and fault injection and fault tolerance. *The conference was held virtually due to the COVID-19 pandemic. The chapter ‘Assurance Argument Elements for Off-the-Shelf, Complex Computational Hardware’ is available open access under an Open Government License 3.0 via link.springer.com.