1. Record Nr. UNINA9910881098303321

Autore	Haxthausen Anne E
Titolo	Formal Methods for Industrial Critical Systems : 29th International Conference, FMICS 2024, Milan, Italy, September 9–11, 2024, Proceedings / / edited by Anne E. Haxthausen, Wendelin Serwe
Pubbl/distr/stampa	Cham : , : Springer Nature Switzerland : , : Imprint : Springer, , 2024
ISBN	9783031681509 9783031681493
Edizione	[1st ed. 2024.]
Descrizione fisica	1 online resource (267 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 14952
Altri autori (Persone)	SerweWendelin
Disciplina	005.45
Soggetti	Compilers (Computer programs) Software engineering Application software Artificial intelligence Computer science Computer engineering Computer networks Compilers and Interpreters Software Engineering Computer and Information Systems Applications Artificial Intelligence Theory of Computation Computer Engineering and Networks
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Real-Time Systems/Robotics -- Safe Linear Encoding of Vehicle Dynamics for the Instantiation of Abstract Scenarios -- 1 Introduction -- 2 Related Work -- 3 Encoding of Abstract Scenarios -- 4 Encoding Vehicle Dynamics and Scenes -- 4.1 Encoding Trajectories as Splines -- 4.2 Encoding of Scenes -- 4.3 Encoding of Vehicle Dynamics -- 5 Correctness -- 6 Demonstration -- 7 Conclusion -- References -- Evaluating the Effectiveness of Digital Twins Through Statistical Model Checking with

Feedback and Perturbations -- 1 Introduction -- 2 Case Studies -- 3 The Stark Tool -- 3.1 The Evolution Sequence Model -- 3.2 RobTL -- 4 DT-Stark -- 4.1 The Feedback Mechanism -- 5 Experiments -- 6 Related Work -- 7 Concluding Remarks -- References -- UPPAAL-Based Modeling and Verification of ROS 2 Multi-threaded Execution and Operating System Reservations -- 1 Introduction -- 2 Background -- 2.1 ROS 2 -- 2.2 Reservation Based Scheduling -- 2.3 Timed Automata and UPPAAL -- 2.4 Pattern-Based Verification of ROS 2 Systems -- 3 Modeling and Verification in UPPAAL -- 3.1 Feature Selection and Abstraction -- 3.2 Modeling of Callbacks -- 3.3 Modeling of the Multi-threaded Executor -- 3.4 System Declaration and Verification in UPPAAL -- 3.5 Modeling of Operating System Reservations -- 4 Evaluation -- 4.1 Experimental Setup -- 4.2 Multi-threaded Execution -- 4.3 Reservation-Based Scheduling -- 4.4 Answer to the Research Questions -- 5 Related Work -- 6 Conclusion and Future Work -- References -- Semantics and Verification -- Formalising the Industrial Language SMMT in mCRL2 -- 1 Introduction -- 2 The SMMT Language -- 3 A Formal Semantics of SMMT -- 4 Translational Semantics in mCRL2 -- 5 Validation and Experiments -- 6 Discussion -- 7 Conclusions -- References.
Fault Tree Inference Using Multi-objective Evolutionary Algorithms and Confusion Matrix-Based Metrics -- 1 Introduction -- 2 Preliminaries -- 2.1 Fault Trees -- 2.2 Failure Data Set -- 2.3 Inference of Fault Tree Models -- 3 FT-MOEA-CM's Methodology -- 4 Experimental Evaluation -- 5 Results -- 5.1 Feature Assessment -- 5.2 Comparing FT-MOEA and FT-MOEA-CM -- 5.3 FT-MOEA-CM's Features: Parallelization and Caching -- 6 Conclusions -- References -- Logika: The Sireum Verification Framework -- 1 Introduction -- 2 Design Goals and Background -- 3 Features -- 4 Assessment -- 5 Related Work -- 6 Conclusion -- References -- Case Studies -- Fuzzing an Industrial Proprietary Protocol -- 1 Introduction -- 2 Challenges -- 3 BinFuzz -- 3.1 Protocol Reconstruction Phase -- 3.2 Fuzzing Phase -- 4 Protocol Fuzzing -- 4.1 FTP Protocol -- 4.2 Proprietary Drone Control Protocol -- 4.3 Limitations and Potential Extensions -- 5 Related Work -- 6 Conclusion -- References -- Modelling and Analysis of DTLS: Power Consumption and Attacks -- 1 Introduction -- 2 Background -- 2.1 DTLS 1.3 -- 2.2 Uppaal -- 2.3 Uppaal SMC -- 3 Modelling DTLS -- 3.1 Default DTLS 1.3 Protocol -- 3.2 DTLS 1.3 with Heartbeat Extension on Server -- 3.3 DTLS 1.3 with Heartbeat Extension on Client -- 4 Modelling DTLS Under Attack -- 5 Experiments -- 5.1 Power Consumption Comparison -- 5.2 Power Consumption with Malicious Actor -- 6 Related Work -- 7 Conclusion -- References -- Verifying a Radio Telescope Pipeline Using HaliVer: Solving Nonlinear and Quantifier Challenges -- 1 Introduction -- 2 Background -- 3 Case Study Description -- 3.1 DDECAL -- 3.2 Halide Implementation -- 4 Verification Challenges and Solutions -- 4.1 Tuple Support -- 4.2 Verifying Flattened Multidimensional Arrays -- 4.3 Dealing with Quantifiers -- 5 Experiments -- 5.1 Micro-benchmarks -- 6 Lessons Learned -- 7 Related Work.
8 Conclusion -- References -- Reconstructing the High-Level Structure of Legacy Code via Software Model Checking: An Experience Report -- 1 Introduction -- 2 Methodology -- 2.1 Operating Assumptions -- 2.2 Main FSM Extraction Algorithm -- 2.3 Code Abstractions -- 3 The fsm-explorer Tool -- 3.1 Configuration -- 3.2 Analysis -- 4 Analysis of a Legacy Heat Pump Controller -- 5 Conclusions -- References -- Formal Analysis and Monitoring of Legacy Safety-Critical Interlocking Systems with the Use of Certified Industrial Tools -- 1 Introduction -- 2 Relay-Based RIS -- 3 The CLEARSY Safety Platform (CSSP) -- 4 Logical

Description of the RIS Behaviour -- 5 Creation and Use of the RIS CSSP Monitor -- 6 Case Studies -- 6.1 Temporary Reversed Direction Installation -- 6.2 Signalling Light Panel -- 7 Discussion -- 8 Conclusion -- References -- Neural Networks -- Unifying Syntactic and Semantic Abstractions for Deep Neural Networks -- 1 Introduction -- 2 Background -- 2.1 Notation -- 2.2 Formal Analysis of Neural Networks -- 2.3 Semantic Compressions and Abstractions with Empirical Guarantees -- 2.4 Strong Formal Connections Between N and N' -- 2.5 Syntactic Neural Network Splitting and Merging -- 2.6 Syntactic Refinement -- 3 Methodology -- 3.1 Semantic Closeness Factor -- 3.2 Tree of Merges -- 3.3 Tree-Cuts and Refinement -- 3.4 Optimality of Tree -- 3.5 CEGAR ch12cegarspsnn,ch12cegar Loop Framework -- 4 Experiments -- 5 Related Work -- 6 Conclusion and Future Work -- References -- Multimodal Model Predictive Runtime Verification for Safety of Autonomous Cyber-Physical Systems -- 1 Introduction -- 2 Preliminaries -- 2.1 Mission-Time Linear Temporal Logic (MLTL) ch13LVR19,ch13RRS14 -- 2.2 Abstract Syntax Tree Architecture -- 2.3 Model Predictive Runtime Verification (MPRV) ch13ZADJR23 -- 3 Multimodal Model Predictive Runtime Verification (MMPRV). 3.1 Predictive Mission-Time Linear Temporal Logic (PMLTL) -- 3.2 MMPRV Algorithm -- 3.3 Memory Requirements for MMPRV -- 4 Autonomous Vehicle Case Study -- 4.1 F1Tenth Autonomous Racing -- 4.2 Argoverse Autonomous Driving -- 5 Conclusion and Future Work -- References -- Surrogate Neural Networks Local Stability for Aircraft Predictive Maintenance -- 1 Introduction -- 2 Related Work -- 3 Case Study: Aircraft Loads-to-Stress Prediction -- 3.1 Description -- 3.2 Tested Models -- 3.3 Property to be Ensured: Local Stability -- 4 Method Combination for Local Stability Assessment -- 5 Experiments -- 6 Results -- 6.1 A Significant Verification Time Gain -- 6.2 Insights into the Models -- 7 Conclusions and Future Work -- A Open-Source Verification Pipeline -- References -- Author Index.

Sommario/riassunto

This book constitutes the proceedings of the 29th International Conference on Formal Methods for Industrial Critical Systems, FMICS 2024, held in Milan, Italy, during September 9–13, 2024. The 14 full papers included in this book were carefully reviewed and selected from 22 submissions. These papers have been organized in the following topical sections: Real-Time Systems/ Robotics; Semantics and Verification; Case Studies; Neural Networks.