

1. Record Nr.	UNISA996550555403316
Autore	Cimatti Alessandro
Titolo	Formal Methods for Industrial Critical Systems : 28th International Conference, FMICS 2023, Antwerp, Belgium, September 20-22, 2023, Proceedings
Pubbl/distr/stampa	Cham : , : Springer International Publishing AG, , 2023 ©2023
ISBN	3-031-43681-4
Edizione	[1st ed.]
Descrizione fisica	1 online resource (270 pages)
Collana	Lecture Notes in Computer Science Series ; ; v.14290
Altri autori (Persone)	TitoloLaura
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Experimenting with Formal Verification and Model-Based Development in Railways: The Case of UMC and Sparx Enterprise Architect -- 1 Introduction -- 2 Related Work -- 3 MBSD, Sparx Enterprise Architect and UMC -- 3.1 Sparx Enterprise Architect -- 3.2 UML Model Checker -- 4 Methodology -- 5 Case Study -- 5.1 Model Checking Sparx EA Models -- 6 Lessons Learned and Limitations -- 7 Conclusion -- References -- The 4SECU Rail Case Study on Rigorous Standard Interface Specifications -- 1 Introduction -- 2 The Demonstrator Case Study -- 2.1 The 4SECU Rail Case Study -- 2.2 The Formalization of the Case Study -- 3 Cost-Benefit Analysis -- 4 Discussion and Conclusions -- References -- Statistical Model Checking for P -- 1 Introduction -- 2 An Overview of P -- 2.1 An Overview of P and its Semantics -- 2.2 A Case Study: A Bike Sharing System -- 3 Statistical Model Checking with MultiVeStA -- 4 Integration of P and MultiVeStA -- 5 A Case Study -- 5.1 Verifying Quantitative Properties of the Bikes Example -- 5.2 On the Scalability of Statistical Model Checking -- 6 Concluding Remarks -- References -- Pattern-Based Verification of ROS 2 Nodes Using UPPAAL -- 1 Introduction -- 2 Background -- 2.1 ROS 2 -- 2.2 Timed Automata and UPPAAL -- 3 Modeling and Verification of ROS 2 Nodes in UPPAAL -- 4 Evaluation of Pattern-Based Verification -- 5 Related Work -- 6 Conclusions and Future Work -- References -- Configurable Model-

Based Test Generation for Distributed Controllers Using Declarative Model Queries and Model Checkers -- 1 Introduction -- 2 Preliminaries -- 2.1 Railway Interlocking System and its Object Manager Subsystem -- 2.2 Component Integration and Test Generation Approach -- 2.3 VIATRA Query Language -- 3 Configuring Message Queues for Component Interactions -- 4 Property Specification Using Model Queries. 5 Practical Evaluation -- 6 Related Work -- 7 Conclusion and Future Work -- References

Refinement of Systems with an Attacker Focus -- 1 Introduction -- 2 Modelling Systems and Attacks -- 3 Attacker Objectives -- 4 Refinement Checking -- 5 Implementation -- 6 Case Study -- 6.1 Amazon Delivery -- 6.2 Duqu Malware -- 7 Conclusion -- References

Modelling of Hot Water Buffer Tank and Mixing Loop for an Intelligent Heat Pump Control -- 1 Introduction -- 2 Case House and Problem Statement -- 3 Buffer Tank and Mixing Loop Thermodynamics -- 4 System Modelling in Uppaal Stratego -- 4.1 Buffer Tank Modelling in Uppaal Stratego -- 4.2 Online Synthesis -- 5 Experimental Evaluation -- 5.1 Evaluation Setup -- 5.2 Buffer Tank Quality Assessment -- 5.3 Buffer Tank Evaluations with Intelligent Stratego Controller -- 5.4 Mixing Loop Evaluations with Intelligent Stratego Controller -- 6 Conclusion -- References

Automated Property-Based Testing from AADL Component Contracts -- 1 Introduction -- 2 Background -- 3 Example -- 4 Property-Based Testing Framework Overview -- 5 GUMBOX Illustrated -- 6 Experience Report -- 7 Related Work -- 8 Conclusion -- References

Impossible Made Possible: Encoding Intractable Specifications via Implied Domain Constraints -- 1 Introduction -- 2 Preliminaries: Mission-Time LTL and Formula-Wise Encoding -- 2.1 MLTL Formula-Wise AST Encoding Structure -- 2.2 MLTL AST Encoding Memory Requirements ch9KZJZR20 -- 3 MLTL Encoding Optimizations -- 4 Realizing Self-Reference via Slot-Based MLTL Encoding -- 5 Realizing Unboundedness via Dynamic Set Specification Unrolling -- 6 Realizing Counting via Domain-Bounded Dynamic Sets -- 7 Applying MLTL Rewrite Rules to DBDS Specifications -- 8 Impacts and Future Work -- References.

Robustness Verification of Deep Neural Networks Using Star-Based Reachability Analysis with Variable-Length Time Series Input -- 1 Introduction -- 2 Preliminaries -- 2.1 Neural Network Verification Tool and Star Sets -- 2.2 Time Series and Regression Neural Network -- 2.3 Reachability of a Time Series Regression Network -- 3 Adversarial Noise -- 4 Verification Properties -- 5 Robustness Verification Problem Formulation -- 6 Reachability of Specific Layers to Allow Variable-Length Time Series Input -- 7 Experimental Setup -- 7.1 Dataset Description -- 7.2 Network Description -- 8 Experimental Results and Evaluation -- 9 Conclusion and Future Work -- References

Testing Logical Diagrams in Power Plants: A Tale of LTL Model Checking -- 1 Introduction -- 2 Logical Diagram -- 3 LTL Encoding of Logical Diagrams -- 3.1 LTL Encoding of Logical Diagrams and Initializing Functions -- 3.2 LTL Encoding of Properties -- 4 Proofs -- 5 Evaluation and Discussion -- References

Optimal Spare Management via Statistical Model Checking: A Case Study in Research Reactors -- 1 Introduction -- 1.1 Related Work -- 2 Spare Management for a Research Reactor -- 2.1 Research Reactor -- 2.2 Optimal Spare Management -- 2.3 System Parameters -- 2.4 Performance Metrics -- 3 Preliminaries -- 3.1 Fault Trees -- 3.2 Stochastic Priced Timed-Game Automata -- 3.3 Uppaal Stratego -- 4 Methodology -- 5 INVAP Emergency Shutdown System as an SPTGA -- 6 Analysis and Results -- 6.1 Formal Queries -- 6.2 Analysis Results -- 6.3 Discussion -- 7 Conclusion and Future Work -- References

Applying Rely-Guarantee

Reasoning on Concurrent Memory Management and Mailbox in C/OS-ii:
A Case Study -- 1 Introduction -- 2 Background -- 2.1 Rely-Guarantee
Reasoning -- 2.2 Concurrent Reactive System and PiCore -- 3 Kernel
Services in C/OS-ii -- 3.1 Data Structure -- 3.2 Mechanism of Kernel
Services.
3.3 Safety Invariants of Kernel Service -- 4 Formal Modelling of Kernel
Services of C/OS-ii -- 4.1 Execution Model of C/OS-ii -- 4.2 Formal
Specification of Kernel Service of C/OS-ii -- 5 Correctness and Rely-
Guarantee Proof -- 6 Experience Using PiCore -- 7 Related Work and
Conclusion -- References -- Conformance in the Railway Industry:
Single-Input-Change Testing a EULYNX Controller -- 1 Introduction --
2 Background -- 2.1 Point Architecture in EULYNX -- 2.2
Programmable Logic Controllers -- 2.3 Single-Input-Change Testing --
3 Interpretation of EULYNX Specifications -- 3.1 Proposed
Interpretation -- 3.2 Formal Model -- 4 From FSM to SIC-DFSM -- 4.1
SIC-DFSM -- 4.2 SIC-DFSM Derivation -- 5 Case Study -- 5.1 Pipelines
-- 5.2 Results -- 5.3 Validation -- 6 Related Work -- 7 Final Remarks
-- References -- Author Index.
