1. Record Nr. UNISA996490368003316

Titolo	Formal methods for industrial critical systems : 27th International Conference, FMICS 2022, Warsaw, Poland, September 14-15, 2022, proceedings / / Jan Friso Groote, Marieke Huisman (editors)
Pubbl/distr/stampa	Cham, Switzerland : , : Springer, , [2022] ©2022
ISBN	3-031-15008-2
Descrizione fisica	1 online resource (246 pages)
Collana	Lecture notes in computer science ; ; 13487
Disciplina	004.0151
Soggetti	Formal methods (Computer science) Software engineering
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Intro -- Preface -- Organization -- Contents -- Invited Keynote Talks -- Reinforcement Learning with Guarantees that Hold for Ever -- 1 Learning from Rewards -- 2 Learning with -Regular Objectives -- 2.1 Good-for-MDP Automata -- 2.2 From GFM Büchi Automata to Reachability and RL -- 3 Related Work -- References -- Supporting Railway Innovations with Formal Modelling and Verification -- References -- Certification -- Formal Monotony Analysis of Neural Networks with Mixed Inputs: An Asset for Certification -- 1 Introduction -- 2 Certification Preamble -- 3 Related Work -- 4 Monotony Analysis -- 4.1 Goal of the Analysis -- 4.2 MILP Formulation -- 4.3 Verification Procedure -- 5 Case Study: Braking Distance Estimation -- 5.1 Description of the Case Study -- 5.2 Experimentation -- 6 Conclusion -- References -- Generating Domain-Specific Interactive Validation Documents -- 1 Introduction and Motivation -- 2 Validation Workflow -- 3 Static VisB HTML Export -- 4 Dynamic HTML Export: Code Generation to HTML and JavaScript -- 4.1 Graphical User Interface -- 4.2 Applicability of JavaScript Code Generation -- 5 Case Studies -- 6 Related Work -- 7 Conclusion and Future Work -- References -- Deductive Verification of Smart Contracts with Dafny -- 1 Introduction -- 2 Verification of Closed Smart Contracts -- 3 Verification Under Adversarial Conditions -- 3.1 Aborting a

Computation -- 3.2 Reasoning with Arbitrary External Calls -- 4 Conclusion -- References -- Industrial Use Cases -- Towards Reusable Formal Models for Custom Real-Time Operating Systems -- 1 Introduction -- 2 Preliminaries -- 2.1 Core Components of Real-Time Operating Systems -- 2.2 Uppaal Timed Automata -- 3 Related Work -- 4 Reusable Formal Models for Custom RTOS -- 4.1 Formalization of Tasks -- 4.2 Formalization of Cyclic Handlers -- 4.3 Events and Timing Behavior.
4.4 Configurable Formal Scheduler Model -- 4.5 Modeling Sensor Inputs and Communication -- 5 Case Study: Search and Rescue Robots -- 6 Conclusion -- References -- Formal Verification of an Industrial UML-like Model using mCRL2 -- 1 Introduction -- 2 Cordis Models -- 2.1 Class Diagrams -- 2.2 State Machine Diagrams -- 3 Cylinder -- 4 Model Checking Cordis Models Using mCRL2 -- 4.1 Translation to mCRL2 -- 4.2 Formal Verification of Requirements -- 4.3 Results -- 5 Discussion -- 6 Concluding Remarks -- References -- Chemical Case Studies in KeYmaera X -- 1 Introduction -- 2 Background -- 2.1 Differential Dynamic Logic -- 2.2 KeYmaera X -- 3 Results -- 3.1 Controlled Irreversible Reactions -- 3.2 Uncontrolled Reversible Reactions -- 4 Related Work -- 5 Conclusion -- References -- Analysing Capacity Bottlenecks in Rail Infrastructure by Episode Mining -- 1 Introduction -- 2 Related Work -- 3 Identification of Capacity Bottlenecks -- 3.1 Method -- 3.2 Results -- 4 Analysing Delay Propagations -- 4.1 Goals and Overview -- 4.2 Episode Mining -- 4.3 Algorithm and Implementation -- 4.4 Adaptations -- 5 Evaluation Results -- 6 Conclusions and Outlook -- References -- Testing and Monitoring -- Test Suite Augmentation for Reconfigurable PLC Software in the Internet of Production -- 1 Introduction -- 1.1 Limitations and Contributions -- 2 Related Work -- 3 Methodology -- 3.1 Intermediate Representation -- 3.2 Bounded Symbolic Execution -- 3.3 Shadow Symbolic Execution -- 4 Evaluation -- 5 Conclusion -- References -- Monitoring of Spatio-Temporal Properties with Nonlinear SAT Solvers -- 1 Introduction -- 2 Preliminaries -- 3 Running Example -- 3.1 Formalization of Road Traffic Rules with LTL MS -- 3.2 Scenario and Trace Encoding (Static and Dynamic Objects) -- 4 Monitoring Model Construction -- 5 Empirical Evaluation -- 6 Related Work.
7 Conclusion and Future Work -- References -- Model-Based Testing of Internet of Things Protocols -- 1 Introduction -- 1.1 Related Work -- 1.2 Contributions -- 2 Preliminaries -- 2.1 Internet of Things -- 2.2 Model-Based Testing -- 2.3 Axini Modeling Platform (AMP) -- 3 MBT in the Context of IoT -- 3.1 IoT Testing Challenges -- 3.2 Positioning MBT in IoT -- 4 The AMP MBT Environment to Test BLE IoT Systems -- 4.1 SUT -- 4.2 Model Creation -- 4.3 AML Model Example -- 4.4 Adapter -- 5 Testing BLE Using AMP -- 5.1 Assumption -- 5.2 Test Generation Configurations -- 5.3 Conformance Experiment -- 5.4 Model Assumption Experiment -- 6 Discussion -- 7 Conclusion -- 7.1 Future Work -- References -- Methodology -- Formally Verifying Decompositions of Stochastic Specifications -- 1 Introduction -- 2 Problem Illustration -- 3 A Theory for Specifying Stochastic Behavior -- 3.1 Traces and Behaviors -- 3.2 Specifications -- 3.3 Trace Automata -- 3.4 Probabilistic Automaton Contracts -- 4 Verification of Refinement -- 5 Case Study -- 6 Related Work -- 7 Conclusions -- References -- Verification of Behavior Trees using Linear Constrained Horn Clauses -- 1 Introduction -- 2 Related Works -- 3 Preliminaries -- 3.1 Behavior Trees -- 3.2 Constrained Horn Clauses -- 4 Encoding of Behavior Trees -- 4.1 Idea -- 4.2 Action Node -- 4.3 Condition Node -- 4.4 Sequence Node -- 4.5 Sequence Node with Memory -- 4.6 Selector Node -- 4.7 Parallel Node -- 4.8 Root Node -- 4.9 Safety

Property -- 4.10 Environment -- 5 Experiments -- 5.1 Benchmark -- 5.2 Discussion -- 6 Conclusion and Outlook -- References -- A Multi-level Methodology for Behavioral Comparison of Software-Intensive Systems -- 1 Introduction -- 2 Background -- 2.1 Software Behavior -- 2.2 State Machines -- 2.3 State Machine Comparison -- 3 Behavioral Comparison Methodology -- 3.1 Level 1: Model Set Variants. 3.2 Level 2: Model Set Variant Relations -- 3.3 Level 3: Model Set Variant Differences -- 3.4 Level 4: Model Variants -- 3.5 Level 5: Model Variant Relations -- 3.6 Level 6: Model Variant Differences -- 4 Evaluation -- 4.1 Case Study 1: Legacy Component Technology Migration -- 4.2 Case Study 2: System Behavior Matching Recipe -- 5 Conclusions and Future Work -- References -- Author Index.