1. Record Nr. UNINA9910574056603321

Titolo	NASA Formal Methods : 14th International Symposium, NFM 2022, Pasadena, CA, USA, May 24–27, 2022, Proceedings / / edited by Jyotirmoy V. Deshmukh, Klaus Havelund, Ivan Perez
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2022
ISBN	3-031-06773-8
Edizione	[1st ed. 2022.]
Descrizione fisica	1 online resource (846 pages)
Collana	Lecture Notes in Computer Science, , 1611-3349 ; ; 13260
Disciplina	004.0151
Soggetti	Software engineering Software Engineering
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di contenuto	Invited Keynotes -- Formal Methods for Trusted Space Autonomy: Boon or Bane -- An Essence of Domain Engineering - A Basis for Trustworthy Aeronautics and Space Software -- Concept Design Moves -- Automating Program Transformation with Coccinelle -- The Prusti Project: Formal Verification for Rust -- Summers Reachability Analysis for Cyber-Physical Systems: Are we there yet -- Regular Submissions -- Towards Better Test Coverage: Merging Unit Tests for Autonomous Systems -- Quantification of Battery Depletion Risk Made Efficient -- Hierarchical Contract-based Synthesis for Assurance Cases -- Verified Probabilistic Policies for Deep Reinforcement Learning -- NNLander-VeriF: A Neural Network Formal Verification Framework for Vision-Based Autonomous Aircraft Landing -- The Black-Box Simplex Architecture for Runtime Assurance of Autonomous CPS -- Case Studies for Computing Density of Reachable States for Safe Autonomous Motion Planning -- Towards Refactoring FRETish Requirements -- Neural Network Compression of ACAS Xu Early Prototype is Unsafe: Closed-Loop Verification through Quantized State Backreachability -- ZoPE: A Fast Optimizer for ReLU Networks with Low-Dimensional Inputs -- Permutation Invariance of Deep Neural Networks with ReLUs -- Configurable Benchmarks for C Model Checkers -- AssumeGuarantee Reasoning with Scheduled Components

-- Stateful Black-Box Fuzzing of Bluetooth Devices Using Automata Learning -- From Verified Scala to STIX File System Embedded Code using Stainless -- On the Termination of Borrow Checking in Featherweight Rust -- Programming Than Programming: Teaching Formal Methods in a Software Engineering Programme -- Zone Extrapolations in Parametric Timed Automata -- Exemplifying Parametric Timed Specifications over Signals with Bounded Behavior -- Timed Automata Learning via SMT Solving -- Asynchronous Composition of Local Interface LTL Properties -- Elucidation and Analysis of Specification Patterns in Aerospace System Telemetry -- Robust Computation TreeLogic -- On the-Fly Model Checking with Neural MCTS -- Checking and Test Generation for Comprehensive Verification -- Operational Annotations: a New Method for Sequential Program Verification -- Byzantine Fault Tolerant Consensus in Agda -- DSV: Disassembly Soundness Validation without Assuming a Ground Truth -- Probabilistic Hyperproperties with Rewards -- Hypercontracts -- Monitorability of Expressive Verdicts -- BDDs Strike Back: Efficient Analysis of Static and Dynamic Fault Trees -- Approximate Translation from Floating-Point to Real-Interval Arithmetic -- Synthesis of Optimal Defenses for System Architecture Design Model in MaxSMT -- Certified Computation of Nondeterministic Limits -- The Power of Disjoint Support Decompositions in Decision Diagrams -- Incremental Transitive Closure for Zonal Abstract Domain -- Proof Mate: an Interactive Proof Helper for PVS -- Runtime Verification Triggers -- Real-time, Autonomous Fault Recovery on the CySat-I.

Sommario/riassunto

This book constitutes the proceedings of the 14th International Symposium on NASA Formal Methods, NFM 2022, held in Pasadena, USA, during May 24-27, 2022. The 33 full and 6 short papers presented in this volume were carefully reviewed and selected from 118submissions. The volume also contains 6 invited papers. The papers deal with advances in formal methods, formal methods techniques, and formal methods in practice. The focus on topics such as interactive and automated theorem proving; SMT and SAT solving; model checking; use of machine learning and probabilistic reasoning in formal methods; formal methods and graphical modeling languages such as SysML or UML; usability of formal method tools and application in industry, etc. .