1. Record Nr. UNINA9910484069303321

Titolo	Dependable Software Engineering: Theories, Tools, and Applications : First International Symposium, SETTA 2015, Nanjing, China, November 4-6, 2015, Proceedings / / edited by Xuandong Li, Zhiming Liu, Wang Yi
Pubbl/distr/stampa	Cham : , : Springer International Publishing : , : Imprint : Springer, , 2015
ISBN	3-319-25942-3
Edizione	[1st ed. 2015.]
Descrizione fisica	1 online resource (XIX, 317 p. 86 illus.)
Collana	Programming and Software Engineering ; ; 9409
Disciplina	005.1
Soggetti	Software engineering Computer logic Computer simulation Mathematical logic Software Engineering Logics and Meanings of Programs Simulation and Modeling Mathematical Logic and Formal Languages
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Bibliographic Level Mode of Issuance: Monograph
Nota di contenuto	Intro -- Preface -- Organization -- Invited Talks -- Criticality-Cognizant Modeling and Analysis of Mixed-Criticality Systems (Extended Abstract) -- Wise Computing (Abstract of Invited Lecture) -- The Myth of Linearization Points -- Contents -- Probabilistic Systems -- Fault Trees on a Diet -- 1 Introduction -- 2 Dynamic Fault Trees -- 3 Rewrite Rules for Dynamic Fault Trees -- 4 Rewriting DFTs via Graph Transformation -- 5 Experiments -- 6 Conclusions and Future Work -- Cost vs. Time in Stochastic Games and Markov Automata -- 1 Introduction -- 2 Foundations -- 3 Transformation of Stochastic Games -- 4 Case Studies and Experimental Results -- 5 Conclusion -- References -- A Comparative Study of BDD Packages for Probabilistic Symbolic Model Checking -- 1 Introduction -- 2 Probabilistic Model Checking -- 2.1 Markov Decision Processes -- 2.2 PCTL Model

Checking -- 2.3 BDD-Based Probabilistic Symbolic Model Checking -- 2.4 BDD Packages -- 3 Experimental Results -- 4 Conclusion -- References -- Hybrid and Cyber-Physical Systems -- Refinement and Proof Based Development of Systems Characterized by Continuous Functions -- 1 Introduction -- 2 Discretization of Continuous Functions -- 3 The Event-B Method -- 4 Refinement Strategy -- 4.1 The Illustrating System -- 4.2 Continuous Controller -- 4.3 Discrete Controller -- 4.4 Top-Down Refinement -- 4.5 About Modeling of Time -- 5 A Formal Development of a Discrete Controller with Event-B -- 5.1 Abstract Machine: The Top-Level Specification -- 5.2 The First Refinement: Introducing Continuous Functions -- 5.3 The Second Refinement: Introducing Discrete Representation -- 5.4 Proofs Statistics -- 6 Related Works and Applications -- 7 Conclusion -- References -- Synthesizing Controllers for Multi-lane Traffic Maneuvers -- 1 Introduction -- 2 Car Traffic Modeling -- 2.1 The Multi-lane Highway.
2.2 A Hybrid Model of a Car -- 2.3 Highway Traffic with Lane Change -- 3 Controller Synthesis for Multi-lane Traffic Maneuvers -- 3.1 Overview of Controller Synthesis -- 3.2 A Simple Algorithm for Lane Change -- 3.3 Interleaving Semantics or Synchronous Models? -- 3.4 Lane Change Algorithm Allowing for Parallel Transitions -- 3.5 Using a Helper Car -- 4 Conclusion -- References -- Extending Hybrid CSP with Probability and Stochasticity -- 1 Introduction -- 2 Background and Notations -- 3 Stochastic HCSP -- 3.1 A Running Example -- 4 Operational Semantics -- 4.1 Operational Semantics -- 5 Assertions and Specifications -- 5.1 Assertion Language -- 5.2 Specifications -- 6 Proof System -- 7 Conclusion -- References -- Testing, Simulation and Inference -- Towards Verified Faithful Simulation -- 1 Introduction -- 2 Related Work -- 3 Background -- 3.1 Coq -- 3.2 Compert-C -- 3.3 SimSoC -- 4 Verified Simulation -- 4.1 Constructing the Formal Model -- 4.2 Proof Structure -- 4.3 Projection -- 4.4 Lemmas Library -- 4.5 Inversion -- 4.6 Instruction Proofs -- 5 Conclusion -- References -- Cardinality of UDP Transmission Outcomes -- 1 Introduction -- 2 Background -- 3 Formal Analysis of Unreliable UDP Behavior -- 3.1 Unreliable UDP Transmissions -- 3.2 Cardinality of Unreliable UDP Transmissions -- 4 Generating UDP Transmission Outcomes -- 5 Experimental Results -- 6 Related Work -- 7 Conclusion -- References -- Inferring Software Behavioral Models with MapReduce -- 1 Introduction -- 2 Approach Overview -- 2.1 MapReduce -- 2.2 Behavioral Model Inference -- 2.3 Our Approach -- 3 Formal Definitions -- 4 Distributed Trace Slicing with MapReduce -- 4.1 Data Encoding -- 4.2 Mapper -- 4.3 Reducer -- 5 Distributed Model Synthesis with MapReduce -- 5.1 Data Encoding -- 5.2 Mapper and Reducer -- 6 Experimental Evaluation -- 7 Related Works -- 8 Conclusion -- References.
Bisimulation and Correctness -- An Application of Temporal Projection to Interleaving Concurrency -- 1 Introduction -- 2 Propositional Interval Temporal Logic -- 3 Temporal Projection -- 4 Formalisation of Imperative Concurrent Programs -- 4.1 Formalising Interleaving without Projection -- 4.2 Comparison of State Projection with Time-Step Projection -- 5 Related Work -- References -- A High-Level Model for an Assembly Language Attacker by Means of Reflection -- 1 Introduction -- 2 Security Overview -- 2.1 PMA and the Assembly Language Attacker -- 2.2 Contextual Equivalence -- 2.3 The High-Level Attacker Model La -- 3 A Bisimulation over the High-Level Attacker -- 3.1 The Source Language MiniML -- 3.2 The High-Level Attacker Model MiniMLa -- 3.3 MiniML+: Interoperation Between MiniMLa and MiniML -- 3.4 Ba: A Bisimulation over the MiniMLa

Attacker -- 4 A Bisimulation over the Assembly Language Attacker -- 4.1 A Trace Semantics for the Assembly Language Attacker -- 4.2 Bl: A Bisimulation over the Assembly Language Attacker -- 5 Full Abstraction -- 6 Related Work -- 7 Conclusions -- References -- Design and Implementation -- Improving Design Decomposition -- 1 Introduction -- 2 A Relational Model of Software Systems -- 3 Subsystem Decomposition -- 4 Case Studies -- 5 Related Work -- 6 Summary -- References -- From Requirements Engineering to Safety Assurance: Refinement Approach -- 1 Introduction -- 2 Modelling and Verification of Safety-Critical Systems in Event-B -- 3 From Event-B Models to Safety Cases -- 4 Case Study: A Steam Boiler System -- 5 Integrated Automated Tool Support -- 6 Related Work and Conclusions -- References -- Pareto Optimal Scheduling of Synchronous Data Flow Graphs via Parallel Methods -- 1 Introduction and Related Work -- 2 System Model and Problem Formulation -- 3 Pareto Optimal Scheduling and Mapping -- 4 Experiments.
5 Conclusion -- References -- Symbolic Execution and Invariants -- PathWalker: A Dynamic Symbolic Execution Tool Based on LLVM Byte Code Instrumentation -- 1 Introduction -- 1.1 Background -- 1.2 Overview -- 1.3 Contributions -- 1.4 Structure of the Paper -- 2 Example -- 3 Our Approach -- 3.1 Concolic Execution -- 3.2 Splitting Complex Type Variable -- 3.3 Generation of Test Driver -- 3.4 Program Instrumentation Based on LLVM Byte Code -- 4 Implementation and Evaluation -- 4.1 Implementation -- 4.2 Evaluation -- 5 Related Work -- 6 Conclusion and Future Work -- References -- Generating Specifications for Recursive Methods by Abstracting Program States -- 1 Introduction -- 2 Methodology -- 3 Application Scenarios -- 4 Background -- 4.1 Program Logic -- 4.2 Integrating Abstraction -- 5 Generation of Method Contracts -- 5.1 Example -- 5.2 Gathering Partial Method Contracts -- 5.3 Dealing with Other Method Calls, Mutual Recursion -- 6 Experimental Evaluation -- 7 Related Work -- 8 Conclusion and Future Work -- References -- Assertion-Directed Precondition Synthesis for Loops over Data Structures -- 1 Introduction -- 2 Preliminary -- 2.1 Scope Logic -- 2.2 Weakest-Precondition Calculus in Scope Logic -- 3 Motivating Example -- 4 Design -- 4.1 Information Extractor -- 4.2 Pre-processor -- 4.3 Pre-condition Generator -- 4.4 Checking Precondition Candidates -- 5 Implementation and Application -- 6 Limitations -- 7 Related Work -- 8 Conclusion -- References -- Verification and Case Studies -- Automatic Fault Localization for BIP -- 1 Introduction -- 2 The BIP Language -- 3 Overview of the Algorithm -- 4 Fault Localization Algorithm for BIP -- 5 Experimental Evaluation -- 6 Conclusion -- References -- Formal Verification of the Pastry Protocol Using TLA+ -- 1 Introduction -- 1.1 The Pastry Protocol -- 1.2 The Methodology.
2 Modelling the Concurrent Join Protocol of Pastry -- 2.1 Static Model -- Leaf Set. -- Messages. -- Statuses. -- 2.2 Dynamic Model -- 2.3 The Correctness Properties -- 3 Theorem Proving -- 3.1 Inductive Proof of Invariant HalfNeighbor -- 3.2 Proof of NeighborClosest -- Induction Invariant. -- Proof Sketch of the Invariant IRN. -- 4 Conclusion, Related Work and Future Work -- References -- Formal Modelling and Verification of IEC61499Function Blocks with Abstract State Machinesand SMV - Execution Semantics -- 1 Introduction -- 2 Related Facts -- 2.1 Function Blocks -- 2.2 Abstract State Machines -- 2.3 Formal Modeling of IEC 61499 and Cross-Platform Portability -- 3 Functional Structure of Operational Model -- 4 Modular formalism for FB operational semantics - Synchronous Execution -- 4.1 Definition of Scheme for the Model -- 4.2 Definition of Dynamics of the Model -- 4.3 Model of the Dispatcher for Synchronous Execution Model -- 5

Model of the Dispatcher in SMV -- 6 Verification Results -- 7 Conclusion and Future Work -- References -- Erratum to: Pareto Optimal Scheduling of Synchronous Data Flow Graphs via Parallel Methods -- Erratum to: Formal Modelling and Verification of IEC61499 Function Blocks with Abstract State Machines and SMV - Execution Semantics -- Author Index.

Sommario/riassunto

This book constitutes the refereed proceedings of the First International Symposium on Dependable Software Engineering: Theories, Tools, and Applications, SETTA 2015, held in Nanjing, China, in November 2015. The 20 full papers presented together with 3 invited talks were carefully reviewed and selected from 60 submissions. The papers are organized on topical sections on probabilistic systems; hybrid and cyber-physical systems; testing, simulation and inference; bisimulation and correctness; design and implementation; symbolic execution and invariants; and verification and case studies.