1. Record Nr. UNINA9910831059503321

Titolo	Industrial used of formal method [[electronic resource]] : formal verification / / edited by Jean-Louis Boulanger
Pubbl/distr/stampa	London, : ISTE Hoboken, N.J., : Wiley, c2012
ISBN	1-118-58784-7 1-118-56182-1 1-299-18707-2 1-118-58790-1
Descrizione fisica	1 online resource (307 p.)
Collana	ISTE
Altri autori (Persone)	BoulangerJean-Louis
Disciplina	005.101 620.0042
Soggetti	Systems engineering - Data processing Computer simulation Formal methods (Computer science) Computer software - Verification Nondestructive testing
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Cover; Title; Copyright; Table of Contents; Introduction; Chapter 1. SPARK - A Language and Tool-Set for High-Integrity Software Development; 1.1. Introduction; 1.2. An overview of SPARK; 1.2.1. What is SPARK?; 1.3. The rationale behind SPARK; 1.3.1. Flow analysis; 1.3.2. Code proof; 1.3.3. Correctness by construction; 1.4. Industrial applications of SPARK; 1.4.1. SHOLIS; 1.4.2. Lockheed-Martin C-130J mission computer; 1.4.3. MULTOS CA; 1.4.4. Tokeneer; 1.4.5. Aircraft monitoring software; 1.4.6. iFACTS; 1.4.7. SPARK Skein; 1.5. Conclusion; 1.6. Bibliography Chapter 2. Model-Based Testing Automatic Generationof Test Cases Using the Markov Chain Model2.1. Preliminaries on the test process; 2.1.1. Findings; 2.1.2. Test optimization; 2.1.3. The statistical usage test; 2.1.4. Generating test cases; 2.2. Modeling using Markov chains; 2.2.1. Origin; 2.2.2. Mathematical formalization; 2.2.3. Principles of

generation; 2.2.4. Some indicators; 2.2.5. Calculating reliability; 2.3. The MaTeLo tool; 2.3.1. Engineering tests directed by models,model-based testing; 2.3.2. A chain of tools; 2.3.3. The usage model; 2.3.4. Configuration of test strategies
2.3.5. Generating test campaigns2.3.6. Analysis of the results and indicators; 2.4. Examples of industrial applications; 2.4.1. AUDI; 2.4.2. Magneti marelli; 2.4.3. Other industrial applications; 2.4.4. Industrialization of the tests; 2.5. Conclusion; 2.6. Bibliography; Chapter 3. Safety Analysis of the Embedded Systems with the AltaRica Approach; 3.1. Introduction; 3.2. Safety analysis of embedded systems; 3.3. AltaRica language and tools; 3.3.1. The AltaRica language; 3.3.2. Modeling the propagation of failures with AltaRica; 3.3.3. Tools associated with AltaRica
3.4. Examples of modeling and safety analysis3.4.1. Integrated modular avionics architecture; 3.4.2. System of electric power generation and distribution; 3.5. Comparison with other approaches; 3.5.1. Some precursors; 3.5.2. Tools for preexisting formal languages; 3.5.3. Languages for physical systems; 3.5.4. Injecting faults in nominal models; 3.6. Conclusion; 3.6.1. An approach to assess the safetyof systems tested in aeronautics; 3.6.2. Clarification of the system architectureand horizontal exploration of the failure propagation:impacts on the scope of analyses
3.6.3. Clarification of the nominal system characteristics:impacts on the generic definitions of the failure modes3.6.4. Compositional models of failure propagation:impacts on the overall safety process; 3.7. Special thanks; 3.8. Bibliography; Chapter 4. Polyspace®; 4.1. Overview; 4.2. Introduction to software quality and verification procedures; 4.3. Static analysis; 4.4. Dynamic tests; 4.5. Abstract interpretation; 4.6. Code verification; 4.7. Robustness verification or contextual verification; 4.7.1. Robustness verification; 4.7.2. Contextual verification
4.8. Examples of Polyspace® results

Sommario/riassunto

"At present the literature gives students and researchers of the very general books on the formal technics. The purpose of this book is to present in a single book, a return of experience on the used of the "formal technics" (such proof and model-checking) on industrial examples for the transportation domain.This book is based on the experience of people which are completely involved in the realization and the evaluation of safety critical system software based. The implication of the industrialists allows to raise the problems of confidentiality which could appear and so allow to supply new useful information (photos, plan of architecture, real example)"--