A09
155
Methods and Tools for Railway Safety, Reliability and Security

edited by

Francesco Flammini
Contents

7 Preface

Part I

Software verification techniques

11 A Grey–Box Approach to the Functional Testing of Complex Automatic Train Protection Systems
Giuseppe De Nicola, Pasquale di Tommaso, Rosaria Esposito, Francesco Flammini, Pietro Marmo, Antonio Orazzo

29 The Simulation of Anomalies in the Functional Testing of the ERTMS/ETCS Trackside System
Pasquale di Tommaso, Francesco Flammini, Armando Lazzaro, Raffaele Pellecchia, Angela Sanseviero

49 Modelling of Railway Logics for Reverse Engineering, Verification and Refactoring
Francesco Flammini, Armando Lazzaro, Nicola Mazzocca

77 Automatic instantiation of abstract tests on specific configurations for large critical control systems
Francesco Flammini, Nicola Mazzocca, Antonio Orazzo

Part II

Model–based dependability evaluation

109 Using Repairable Fault Trees for the evaluation of design choices for critical repairable systems
Francesco Flammini, Nicola Mazzocca, Mauro Iacono, Stefano Marrone

133 Modeling system reliability aspects of ERTMS/ETCS by Fault Trees and Bayesian Networks
Francesco Flammini, Stefano Marrone, Nicola Mazzocca, Valeria Vittorini
155  A new modeling approach to the safety evaluation of N-modular redundant computer systems in presence of imperfect maintenance
Francesco Flammini, Stefano Marrone, Nicola Mazzocca, Valeria Vittorini

181  Multiformalism techniques for critical infrastructure modeling
Francesco Flammini, Nicola Mazzocca, Francesco Moscato, Alfio Pappalardo, Concetta Pragliola, Valeria Vittorini

Part III
Security risk assessment and mitigation

207  Security Risk Management of Railway Transportation Systems
Francesco Flammini, Nicola Mazzocca

225  Dependable integrated surveillance systems for the physical security of metro railways
Giovanni Bocchetti, Francesco Flammini, Concetta Pragliola, Alfio Pappalardo

243  On–line integration and reasoning of multi–sensor data to enhance infrastructure surveillance
Francesco Flammini, Andrea Gaglione, Nicola Mazzocca, Vincenzo Moscato, Concetta Pragliola

267  Formal evaluation of a majority voting concept to improve the dependability of multiple technology sensors
Francesco Flammini
Preface

Modern rail transport systems feature an increasing level of complexity. One of the main reasons for this growth is the trend to automate delicate control and supervisory functions through heterogeneous distributed computer systems.

This book aims at presenting a set of novel and advanced techniques used in real-world industrial applications to improve the dependability of rail-based transportation systems. The analyses address both natural/random and intentional/malicious threats (ranging from human errors, e.g. coding or maintenance mistakes, to terrorist attacks), which can compromise system integrity both at the hardware (control devices, infrastructures) and software (logic code, data network) levels.

To date, most existing books only address general safety-critical real-time systems engineering; only a few exist covering all the subjects related to railway safety, reliability and security in a holistic and systemic fashion.

On this regard, this book can be a useful reference for experts, consultants and railway system engineers who need to perform risk or dependability analyses for development or certification purposes. It also provides a collection of techniques and case-studies for students of university courses about security and dependability of critical systems and infrastructures.

The book is structured as a collection of self-contained chapters which are (revised and extended) reprint versions of papers which I have co-authored and have been recently published in proceedings of international conferences, contributed books or research journals. All the chapters refer to railway dependability either as the main application scenario or for the example case-studies.

More in detail, the book is organized as follows. It is divided into three main parts, each one containing 4 chapters. The first part covers verification techniques for railway control software, focusing on
testing approaches which can improve both the effectiveness and efficiency of the safety assessment processes. The second part surveys model-based approaches to formally evaluate quantitative dependability attributes (like safety and reliability), mostly at the hardware abstraction level. Finally, part three addresses railway infrastructure security issues from the risk management perspective, including vulnerability assessment and design of protection mechanisms.

Francesco Flammini