Railway Safety, Reliability, and Security:
Technologies and Systems Engineering

Francesco Flammini
Ansaldo STS, Italy
Chapter 1
U.S. Regulatory Requirements for Positive Train Control Systems ............................................. 1
Mark Hartong, Federal Railroad Administration, USA
Duminda Wijesekera, George Mason University, USA

Positive Train Control (PTC) Systems are a type of Communications Based Train Control System (CBTC) designed to enhance railroad safety. As a consequence of a series of high profile train accidents in the United States, a statutory mandate for the installation of these systems in high risk areas by the end of 2015 has been established. This chapter identifies the impetus behind the statute, the statutory requirements associated with PTC, the implementing regulations for the statutory requirements, and the current status of regulatory compliance.

Chapter 2
The Model-Driven openETCS Paradigm for Secure, Safe and Certifiable Train Control Systems .................................................. 22
Jan Peleska, University of Bremen, Germany
Johannes Feuser, University of Bremen, Germany
Anne E. Haxthausen, Technical University of Denmark, Denmark

A novel approach to managing development, verification, and validation artifacts for the European Train Control System as open, publicly available items is analyzed and discussed with respect to its implications on system safety, security, and certifiability. After introducing this so-called model-driven openETCS approach, a threat analysis is performed, identifying both safety and security hazards that may be common to all model-based development paradigms for safety-critical railway control systems, or specific to the openETCS approach. In the subsequent sections state-of-the-art methods suitable to counter these threats are reviewed, and novel promising research results are described. These research results comprise domain-specific modeling, model-based code generation in combination with automated object code verification and explicit utilization of virtual machines to ensure containment of security hazards.
Section 2
Hazard Analysis and Model-Based Evaluation

Chapter 3
Semi-Quantitative Risk Assessment of Technical Systems on European Railways

Jens Braband, Siemens AG, Germany

The European Railway Agency (ERA) has the challenging task of establishing common safety targets and common safety methods throughout Europe. In this context, the harmonization of risk analysis methods is also discussed. The purpose of this paper is to present a new semi-quantitative approach for the risk analysis of technical systems and the means by which compliance with legal and regulatory requirements can be demonstrated. As a particular reference, a new German pre-standard, which lays out requirements for semi-quantitative approaches, is taken into account.

Chapter 4
The ForMoSA Approach to Qualitative and Quantitative Model-Based Safety Analysis

Axel Habermaier, Universität Augsburg, Institut für Informatik, Germany
Matthias Güdemann, Otto-von-Guericke University of Magdeburg, Germany
Frank Ortmeier, Otto-von-Guericke University of Magdeburg, Germany
Wolfgang Reif, Universität Augsburg, Institut für Informatik, Germany
Gerhard Schellhorn, Universität Augsburg, Institut für Informatik, Germany

This chapter presents ForMoSA (FORmal MOdels and Safety Analysis), an integrated approach for the safety assessment of safety-critical embedded systems. The approach brings together the best of engineering practice, formal methods, and mathematics: traditional safety analysis, temporal logics and verification, as well as statistics and optimization. These three orthogonal techniques cover three different aspects of safety: fault tolerance, functional correctness, and quantitative analysis. The ForMoSA approach combines these techniques to assess system safety in a structured and formal way. Furthermore, the tight combination of methods from different analysis domains results in mutual benefits. The combined approach yields results which cannot be produced by any single technique on its own. The methodology was applied to several case studies from different industrial domains. One of them is an autonomous control of level crossings using radio-based communication, which is used in this chapter to describe the individual steps of the ForMoSA methodology.

Section 3
Verification and Validation

Chapter 5
Verification and Validation of Interoperability

Lars Ebrecht, DLR (German Aerospace Center), Institute of Transportation Systems, Germany
Michael Meyer zu Hörste, DLR (German Aerospace Center), Institute of Transportation Systems, Germany

The chapter shows an approach to use existing test methods to prove technical as well as operational interoperability. The first kinds of tests are test sequences to validate conformity of a single constituent – here, an on-board on-board unit (OBU) of the European Train Control System (ETCS) in the European Rail Traffic Management System (ERTMS). The second kind of tests is the integration test for assemblies – here, the complete on-board equipment. The third kinds of tests are the tests for the
validation of operational serviceability. An approach for the stepwise integration of the different kinds of tests is shown. As a conclusion the perspective for the use of these test sequences in an independent test lab is given.

Chapter 6
Fault Injection for On-Board ERTMS/ETCS Safety Assessment .......................................................... 128

Almir Villaro Arriola, CEIT and Tecnun (University of Navarra), Spain
Jon Mendizabal Samper, CEIT and Tecnun (University of Navarra), Spain
Juan Meléndez Lagunilla, CEIT and Tecnun (University of Navarra), Spain

On-Board ERTMS/ETCS equipment performs safety related functions where the tolerable hazard rate is kept below 10⁻⁹ f/h. Safety standards such as EN50129 or IEC61508 impose requirements on the architecture used to fulfill this safety figure and the associated Safety Integrity Level (SIL). From these standards, the mandatory use of redundancy and physical independence can be derived. Due to the introduction of these requirements, a new functionality is added at the system level (e.g. majority voting processes among redundant lines). Unfortunately, neither the safety nor the interoperability standards provide technical specification that defines how to test the performance of the complete system when internal malfunction has occurred in safety related components. This chapter proposes the use of fault injection techniques to facilitate safety assessment. By means of communication saboteurs, it is possible to excite and test the associated internal functionality in systems performing safety related functions. The chapter also contributes to the definition of the test setup and test procedure of the architecture-associated safety-related internal functionality of the SIL4 odometer and Balise Transmission Module (BTM) subsystems within the on-board European Railway Traffic Management System/ European Train Control System (ERTMS/ETCS).

Chapter 7
Impact of Electromagnetic Environment on Reliability Assessment for Railway Signalling Systems .................................................................................................................. 151

Iñigo Adin, CEIT and Tecnun (University of Navarra), Spain
Jaizki Mendizabal, CEIT and Tecnun (University of Navarra), Spain
Jon del Portillo, CEIT and Tecnun (University of Navarra), Spain

The electromagnetic interferences (EMI) are threats that affect the reliability of the railway signalling systems. Consequently, the identification of the reliability requirements dependent on environment conditions is a major issue for signalling systems designers, and therefore for evaluators, and testing and certification bodies. Signalling systems work in the complex and heterogeneous railway environment, where low power electronics have to work together with high voltages and currents from trains and railway infrastructure. This chapter presents the relationship between the railway electromagnetic interoperability and the reliability assessment by analyzing the signalling systems and the associated inter-dependencies with other components of the rolling stock. It is composed of two main sections; the first gathers an exhaustive state of the art approach to the issue of electromagnetic interoperability and railway industry. This subsection steers towards the combination of electromagnetic interferences and the signalling systems present in the rolling stock noise environment. That is the basis of the second section that finally sets how to establish the reliability requirement for a communication path in this environment. This requirement is established because of the electromagnetic noise environment, as well as the radiated and conducted fields, which are a combination of all the surrounding threats a focused railway system has to face. It also depends on the modulation of the communication signal under study.
Implementation of railway controller application logic is a highly safety-critical and time-consuming task carried out individually for each client and station by specialised signalling engineers, with corresponding high costs. MivGa is a software development framework designed to create code generators for application logic for the client railway companies of Ansaldo STS that use the Microlok II controller to lower the cost and increase repeatability. This chapter describes the evolution of MivGa from prototype to framework, and introduces the software engineering approaches of object-oriented meta-modelling and framework development along the way. It also presents known limitations and further application areas of the framework.

Chapter 9
Software-Based Self-Test for Reliable Applications in Railway Systems ............................... 198

Alfredo Benso, Politecnico di Torino, Italy
Stefano Di Carlo, Politecnico di Torino, Italy
Alessandro Savino, Politecnico di Torino, Italy

The very strict safety standards, which must be guaranteed in a railway system, make the testing of all electronic components a unique and challenging case study. Software-based self-test represents a very attractive test solution to cope with the problem of on-line and off-line testing of microprocessor-based systems. It makes it possible to deeply test hardware components without introducing extra hardware and stressing the system in its operational condition. This chapter overviews the basic principles of software-based self-test techniques, focusing on a set of best practices to be applied in writing, verifying and computing the final test coverage of high-quality test programs for railway systems.

Chapter 10
Real-Time Hardware-in-the-Loop in Railway: Simulations for Testing Control Software of Electromechanical Train Components .............................................................. 221

Silvio Baccari, University of Sannio, Italy
Giulio Cammeo, AnsaldoBreda, Italy
Christian Dufour, Opal-RT Technologies, Canada
Luigi Iannelli, University of Sannio, Italy
Vincenzo Mungiguerra, AnsaldoBreda, Italy
Mario Porzio, AnsaldoBreda, Italy
Gabriella Reale, University of Sannio, Italy
Francesco Vasca, University of Sannio, Italy
The increasing complexity of modern ground vehicles is making crucial the role of control for improving energetic efficiency, comfort and performance. At the same time, the control software must be frequently updated in order to let the vehicle respond safely and efficiently within more sophisticated environments and to optimize the operations when new vehicle components are integrated. In this framework real-time hardware-in-the-loop simulations represent a fundamental tool for supporting the verification and validation processes of the control software and hardware. In this chapter a railway case study will be presented. The mathematical models of the most relevant electromechanical components of the vehicle powertrain are presented: the pantograph connected to an ideal overhead line with continuous voltage; the electrical components of a pre-charge circuit, the line filter and the braking chopper; the three-phase voltage source inverter and the induction motor; and, finally, the mechanical transmission system, including its interactions with the rail. Then the issues related to the real-time simulation of the locomotive components models are discussed, concentrating on challenges related to the stiff nature of the dynamic equations and on their numerical integration by combining field programmable gate array (FPGA) and central processing unit (CPU) boards. The usefulness of the real-time hardware-in-the-loop simulations for the analysis of railway control software will be demonstrated by considering the powertrains of two real metropolitan trains under complex scenarios, i.e., stator winding disconnection of the induction motor, pantograph missing contact, wheel-rail slipping phenomenon.

Chapter 11
Hardware-In-the-Loop Testing of On-Board Subsystems:
Some Case Studies and Applications................................................................. 249

Luca Pugi, University of Florence, Italy
Benedetto Allotta, University of Florence, Italy

Hardware In the Loop testing is a very powerful tool for the development, tuning, and synthesized homologation of safety-relevant on-board subsystems and components. In this chapter some case-studies, based on typical topics of industrial research for railways, are introduced in order to emphasize some aspects of the mechatronic design with a particular attention to the integration of actuation systems into rig design.

Section 5
Formal Methods

Chapter 12
The Role of Formal Methods in Software Development for Railway Applications.......................... 282

Alessandro Fantechi, Università degli Studi di Firenze, Italy

Formal methods for thirty years have promised to be the solution for the safety certification headaches of railway software designers. This chapter looks at the current industrial application of formal methods in the railway domain. After a recall of the dawning of formal methods in this domain, recent trends are presented that focus in particular on formal verification by means of model checking engines, with its potential and limitations. The paper ends with a perspective into the next future, in which formal methods will be expected to pervade in more respects the production of railway software and systems.

Chapter 13
Symbolic Model Checking for Interlocking Systems.......................................................... 298

Kirsten Winter, The University of Queensland, Australia
Model checking is a fully automated technique for the analysis of a model of a system. Due to its degree of automation it is in principle suitable for application in industry but at the same time its scalability is limited. Symbolic model checking is one approach that improves scalability through the use of Binary Decision Diagrams (BDDs) as an internal data structure. This approach allows the user to increase the efficiency by customising the ordering of state variables occurring in the model to be checked. In the domain of railway interlockings represented as control tables, it is found that this task can be supported using an algorithm that has access to the track layout information. In our work we propose optimisation strategies that render symbolic model checking feasible for large scale interlocking systems. Our results yield a verification tool suitable for use in industry.

Section 6
Human Factors

Chapter 14
Designing Usable Interactive Systems within the Railway Domain: A Human Factors Approach

Nina Jellentrup, German Aerospace Center, Institute of Transportation Systems, Germany
Michael Meyer zu Hörste, German Aerospace Center, Institute of Transportation Systems, Germany

Train drivers as well as signallers interact with several computer based information and communication systems to ensure safe and effective train operations. So far the technical progress mostly determines the design of such interactive systems and requirements out of a human factors perspective are not integrated. Beside the development of technical functions it is essential to take the usability as a quality attribute of every interactive system into account. If the usability is not considered during system development, it could occur that there are several functions available within a system but the user does not know how to use them in an efficient way. This chapter describes a psychological approach to design or redesign usable interactive systems within the railway domain. Some examples will be discussed to demonstrate the approach and the results.

Chapter 15
Integration of Human Factors to Safety Assessments by Human Barrier Interaction

Markus Talg, German Aerospace Center, Institute of Transportation Systems, Germany
Malte Hammerl, German Aerospace Center, Institute of Transportation Systems, Germany
Michael Meyer zu Hörste, German Aerospace Center, Institute of Transportation Systems, Germany

Human factors have a strong impact on railways safety. However, the assessments of these factors still follow traditional and inadequate approaches. While failure probabilities of technical systems can be measured in sufficient precision, human error probabilities are still estimated in a very rough and vague way. Upon this motivation, the contribution presents a method analyzing human influence in railway applications. The approach of human-barrier-interaction relies on a new model of human behavior, a classic model of human-machine-interaction and a model of safety measures by barriers. Applying the method, human reliability can be assessed in comparative way. An advantage over existing approaches is the substantial combination of cognitive psychology and engineering expertise without unpractical complexity.
Section 7
Security, Monitoring and Surveillance

Chapter 16
Advanced Techniques for Monitoring the Condition of Mission-Critical Railway Equipment 
Clive Roberts, University of Birmingham, UK
Joe Silmon, University of Birmingham, UK

This chapter provides an overview of advanced techniques for monitoring the condition of mission-critical railway assets. The safe operation of railways depends on a large number of geographically distributed components, each of which has a low cost when compared to the highly complex arrangements of assets found in other industries, such as rolling mills and chemical plants. Failure of any one of these components usually results in a degradation of service in order to maintain safety, and is thus very costly to modern railway operators, who are required to compensate their customers when delays occur. In this chapter, techniques for industrial condition monitoring are reviewed, highlighting the main approaches and their applicability, advantages, and disadvantages. The chapter first makes some basic definitions of faults, failures, and machine conditions. The analysis of faults through methods such as Fault Tree Analysis and Failure Modes Effects Analysis are examined. The field of fault diagnosis is then reviewed, partitioning into the three main areas: numeric/analytical models, qualitative models, and data/history-based methods. Some of the key approaches within each of these areas will be explained at a high level, compared, and contrasted.

Chapter 17
Security of Railway Infrastructures 
A. Di Febbraro, University of Genoa, Italy
F. Papa, University of Genoa, Italy
N. Sacco, University of Genoa, Italy

In recent years, some sadly famous terrorist attacks that occurred in different countries have put into evidence that railway transportation systems are not suitably protected, and not capable of tolerating and promptly reacting to them. Moreover, it is clear that such mass transportation systems are particularly attractive for terrorists, due to the potentially far-reaching, often “spectacular” results of attacks. Examples of such kinds of events are the New York (2001), Madrid (2004), and London (2005) terrorist attacks. In addition, by focusing on ground transportation networks, and especially on railway systems, it is also easy to observe that they are particularly difficult to be secured since they are characterized by high accessibility and wide extension, as also noted by Fink (2003). In this sense, the needs of security and of mobility often conflict with each other. In effect, while an open and accessible system provides an efficient transportation of people and goods, this openness also allows malicious entities to exploit the transportation system as a target, weapon, or means to reach another target (Murray-Tuite, 2007). Then, on the contrary, it is clearly evident that security actions taken to limit malicious adversaries from reaching or capturing their targets may degrade the transportation system performances, so they have to be designed with particular attention. This is the reason why worldwide institutions are more and more sensitive to the growing need for security of the so-called Critical Infrastructures (CI), such as railway transportation systems, and are adopting a number of regulatory measures (US Congress, 2007; EU Commission, 2005, 2008, and 2010). For what concerns scientific research, the efforts are intended to define methodologies, build risk mitigation devices, and find out best practices that are technologically advanced, soon achievable, reliable, so as to increase the infrastructure protection without affecting the relevant transportation system performances. In this framework, Quantitative Risk Analysis (QRA) represents the main methodological approach for assessing security, which is indeed often character-
ized by a large set of variables dependent on human sensitivity, and requires calibration and adaptive
tuning, thus resulting into unfriendly tools for the non-skilled users. Then, in this chapter, to tackle with
the problem of clarifying the aims, the characteristics, and the limitations, a general architecture for a
possible QRA tool for railway security assessment is presented, with particular attention to the relevant
specifications (Di Febbraro et al., 2010).

Section 8
Experiences and Case-Studies

Chapter 18
ETCS Developing and Operation: Italian Experience

Raffaele Malangone, RFI, Italy
Fabio Senesi, ANSF, Italy

ETCS/ERTMS actually is the present for Italian Railways but it will also be the next future for the sign-
alling system in many countries and the best technological choice for ATC (Automatic Train Control)
systems. Italian Railways, first in the world, have carried out ETCS Level2 merging the technologies and
the regulations respecting the highest safety level. RFI, following the CENELEC 50-126 Lyfe-Cycle, has developed a process for planning, managing, monitoring and controlling of ETCS achievements. In particular the Disposal 29 and 32 in the year 2002 have been issued for the assessment and homologation process of Generic and Specific Applications and other following procedures have permitted the final configuration of the project until its putting in service. The goal of this course is the Preliminary Acceptance of a Generic Application and later, after a successful testing period on field, its Homologation. RFI has followed the developing process starting from the idea to define the specifications, evaluating the hazards and their probabilities, finding mitigations to improve the safety, validating the products of the suppliers, testing the subsystems and the entire system, until the final activation of the whole systems (compliant with the Technical Specifications for interoperability, UNISIG v.2.2.2). Much attention has been paid to the testing of functional scenarios (using also formal languages) and the real tests on the track have been reduced with the support of an ERTMS Laboratory in Rome (unique in the world for its characteristics) where on-board and track-side subsystem permit to reproduce easily and quickly most of the real situations. This testing process in ETCS laboratories has been useful not only before the putting the ETCS in service but also for the reconfiguration of the actual ETCS lines as it would be hard to do so many test scenario during a commercial service. These activities have been replicated several times, for example, to reach the actual ETCS version compliant to the UNISIG 2.3.0d. The success of the formal language analysis of Test-Specifications has also encouraged the RFI ETCS group to develop a state-charts model of the functional specification. This work is actually in progress but a first result, on the logical behavior of the system at the transition with a historical signalling system, has been done and validated.

Chapter 19
Adoption of Low-Cost Rail Level Crossing Warning Devices: An Australian Case Study

Christian Wullems, Cooperative Research Centre for Rail Innovation, & Centre for Accident
Research and Road Safety – Queensland (CARRS-Q), Australia
George Nikandros, Australian Safety Critical Systems Association, Australia

The objective of this chapter is to provide rail practitioners with a practical approach for determining safety requirements of low-cost level crossing warning devices (LCLCWDs) on an Australian railway by way of a case study. LCLCWDs, in theory, allow railway operators to improve the safety of passively
controlled crossing by upgrading a larger number of level crossings with the same budget that would otherwise be used to upgrade these using the conventional active level crossing control technologies, e.g. track circuit initiated flashing light systems. The chapter discusses the experience and obstacles of adopting LCLCWDs in Australia, and demonstrates how the risk-based approach may be used to make the case for LCLCWDs.

Compilation of References ............................................................... 424

About the Contributors ................................................................. 449

Index ......................................................................................... 460