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

Alfredo Benso  
Politecnico di Torino, Italy

Stefano Di Carlo  
Politecnico di Torino, Italy

Alessandro Savino  
Politecnico di Torino, Italy

ABSTRACT

The introduction of computers in the control and automation of railway systems led to the massive use of microprocessor-based devices in almost all critical elements of a modern railway infrastructure (e.g., signaling systems, trains control, etc.). Therefore, microprocessor-based systems play a crucial role in the safety, reliability and security of these infrastructures.

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.

DOI: 10.4018/978-1-4666-1643-1.ch009
INTRODUCTION

Safety-critical railway systems are developed according to the highest Safety Integrity Level SIL 4 (IEC, 2011), as imposed by the European Committee for Electrotechnical Standardization (CENELEC) in the standards applicable to the railway industry (CENELEC 50126, 50128, 50129, railway applications standards available at http://www.cenelec.eu). These standards cover the safety management of electrical, electronic, and programmable systems throughout their lives, from concept to decommissioning. They bring safety principles to the management of systems and safety engineering to their development.

In the last few decades, the control and automation of the railway systems have increasingly engineered around microprocessor-based architectural solutions that, consequently, started playing a crucial role in the safety, reliability, and security of modern railway infrastructures. The design of the testing mechanisms that have to guarantee the correct behavior of a microprocessor-based railway system, their organization and implementation are unique and challenging case studies.

In the UK, the first document addressing safety issues in railway systems is the “Regulation of Railways Act” of 1889. Although it was published a lot earlier than the advent of microprocessors, it introduced a series of requirements on matters such as the implementation of interlocked block signaling and other safety measures motivated by a railway disaster in that year. One of the evolutions of this document is the “Railway Safety Principles and Guidance”, produced by the Health and Safety Executive (HSE) for use by organizations wishing to obtain approval for new or altered works, plants and equipment under the Railways and Other Transport Systems Regulations in 1994 (HSE, 2011). Although these manuals have been now replaced, they set the standard for basic guidelines related to safety measures and may help developers in getting a clearer idea of the challenges that need to be addressed when designing testing techniques for railways applications.

The “Guidance on signaling” manual (HSE, 2011) states:

“[… ] 5 – INTERLOCKING […]

(41) Design and construction of mechanical or relay interlocking to inherently ‘fail-safe’ criteria are required. Programmable electronic interlocking should be designed to composite or reactive fail-safe criteria, using techniques such as redundancy, diversity and self-testing […]” (pp. 14).

“[… ] 8 DEGRADED OPERATION OF SIGNALING SYSTEMS […]

(118) Failure of the signaling system should not result in an unsafe situation being created. However, consideration should be given to the actions necessary to allow the passage of trains to continue while the failure condition is rectified. […]

(119) The signaling system should be able to be reconfigured so that failed equipment can be isolated and, once the nature of the failure is confirmed, the other parts of the system, which are working correctly, can then be used.” (pp. 26)

“[… ] DEGRADED CONDITIONS […]

The signaling system should continue to provide for safe passage of trains permitted to run under degraded conditions. The factors for consideration should include: (a) design for ‘graceful degradation’ so that correctly working parts of the signaling system may continue to provide for safe passage of trains permitted to run under degraded conditions; (b) protection from failure modes creating unsafe situations; […]” (pp. 34).

From these guidelines, it is feasible to isolate properties that challenge the work of a railway systems test engineer. A safety-critical railway system should be:
Related Content

**Introduction to Multirate Systems**
[www.igi-global.com/chapter/introduction-multirate-systems/27222?camid=4v1a](www.igi-global.com/chapter/introduction-multirate-systems/27222?camid=4v1a)

**Using Attack Graphs to Analyze Social Engineering Threats**
[www.igi-global.com/article/using-attack-graphs-to-analyze-social-engineering-threats/136466?camid=4v1a](www.igi-global.com/article/using-attack-graphs-to-analyze-social-engineering-threats/136466?camid=4v1a)

**Information Theoretic XSS Attack Detection in Web Applications**
[www.igi-global.com/article/information-theoretic-xss-attack-detection-in-web-applications/118145?camid=4v1a](www.igi-global.com/article/information-theoretic-xss-attack-detection-in-web-applications/118145?camid=4v1a)

**Generation of Concurrency Control Program by Extending Functions in Genetic Programming**
[www.igi-global.com/article/generation-of-concurrency-control-program-by-extending-functions-in-genetic-programming/120516?camid=4v1a](www.igi-global.com/article/generation-of-concurrency-control-program-by-extending-functions-in-genetic-programming/120516?camid=4v1a)