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

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

ABSTRACT

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).

DOI: 10.4018/978-1-4666-1643-1.ch006
INTRODUCTION

This chapter has two objectives; to propose a fault injection technique based on communication saboteurs for carrying out the safety assessment of systems composed of redundant components performing safety related functions, and to contribute to the definition of the test setup and test procedure of the SIL4 odometer and balise transmission module subsystems within the on-board ERTMS/ETCS (Dhabbi, 2011) in order to facilitate safety assessment.

In order to achieve these objectives, the chapter is divided in five parts:

- The characteristics of the on-board ERTMS/ETCS that affect validation are initially discussed. Here the most important requirements derived from safety standards (CENELEC EN 50128, EN 50129, EN 50159; IEC 61508), the building of the equipment and the on-board ERTMS/ETCS architecture requirements are discussed and their implications for the validation of the ERTMS/ETCS are explained.
- The tests needed for the functionality assessment are analyzed, focusing on the on-board ERTMS/ETCS tests.
- The fault injection technique for safety assessment is then discussed. In this part, the characteristics of the DUT with safety related functions are briefly analyzed and the different methods to inject faults in the design are compared. By means of an Failure Mode and Effect Analysis (FMEA) of the system, the effects of the different types of faults are identified. This tool demonstrates that the effect of any fault at component level can be emulated by means of a communication error (corruption, deletion, masquerade, delay, etc.). Moreover, a practical method to inject fault, which enables the validation of systems composed of redundant components performing safety-related functions, is described.
- The fourth part of the chapter discusses architecture-associated safety related to the internal functionality of the odometer and BTM (Balise Transmission Module) subsystems within the on-board ERTMS/ETCS. Currently, the interoperability standards dealing with testing define the black box testing of the ETCS functionality. The authors propose the test setup and test procedure based on fault injection for two SIL4 on-board ERTMS/ETCS subsystems to excite the functionality when a component malfunction occurs. By means of this technique it is possible to facilitate the safety assessment of the on-board ERTMS/ETCS.
- Finally, the last part summarizes the most relevant points covered in the chapter.

CHARACTERISTICS OF THE ON-BOARD ERTMS/ETCS THAT IMPACT VALIDATION

The on-board ERTMS/ETCS is in charge of train control. This system is comprised of a set of functions that enable train command and control such as receiving information from wayside signaling systems (e.g. BTM, Loop Transmission Module or GSM-R), identifying the position and defining the speed profile.

Some of these functions are safety-related, and therefore the involved subsystems shall comply with a set of standards during their complete life cycle. Some of these standards define specific requirements for the on-board ERTMS/ETCS constituents that deal with electrical performance (e.g. EN50155), electromagnetic compatibility (e.g. EN50121 series) or environmental conditions (e.g. EN61373 or EN50125).

Another set of documents (Technical Specifications for Interoperability or TSI) defines the requirements for the different ERTMS/ETCS functions, leaving decisions about the architecture and
Related Content

Using DRAM as Cache for Non-Volatile Main Memory Swapping
www.irma-international.org/article/using-dram-as-cache-for-non-volatile-main-memory-swapping/144142/

Facilitating Biodefense Research with Mobile-Cloud Computing
www.irma-international.org/article/facilitating-biodefense-research-mobile-cloud/58510/

From Frequent Features to Frequent Social Links
www.irma-international.org/article/from-frequent-features-to-frequent-social-links/80197/

Numerical Methods of Multifractal Analysis in Information Communication Systems and Networks
www.irma-international.org/chapter/numerical-methods-of-multifractal-analysis-in-information-communication-systems-and-networks/79657/

Survey of Cardinality Constraints in Snapshot and Temporal Semantic Data Models
www.irma-international.org/chapter/survey-cardinality-constraints-snapshot-temporal/30012/