Available online at www.sciencedirect.com

ScienceDirect

Transportation Research Procedia 14 (2016) 1894 – 1903

Transportation Research Procedia

www.elsevier.com/locate/procedia

6th Transport Research Arena April 18-21, 2016

Development of an advanced laboratory for ETCS applications

Gonzalo Solas[a,*], Jaizki Mendizabal[a], Leonardo Valdivia[a], Javier Añorga[a], Iñigo Adin[a], Adam Podhorski[a], Stanislas Pinte[b], Luis Gerardo Marcos[b], Jesús Mª González[c], Francisco Cosín[c]

[a]*CEIT and Tecnun (University of Navarra), San Sebastian, Spain*
[b]*ERTMS Solutions, Brussels, Belgium*
[c]*Asociación de Acción Ferroviaria CETREN, Madrid, Spain*

Abstract

The current process of putting ETCS equipment in service is affected by the testing process and laboratory procedures. This paper deals with two novel laboratory tools that the EATS project (FP7-TRANSPORT-314219) has produced in order to overcome some of the problems those processes show and advance towards the "Zero On-Site Testing" paradigm. On the one hand, saboteurs for the internal interfaces of the ETCS on-board system have been created. These saboteurs integrate seamlessly with the rest of the elements of the testing laboratory and allow to gather evidences regarding the safety functions of the equipment under test. On the other hand, the Wireless Communication Emulators have been also developed. These tools allow to put the wireless interfaces of the ETCS on-board equipment in the worst cases it will find in a real environment, by reproducing and injecting noise and interferer signals, and measuring the effect in the equipment under test.

Peer-review under responsibility of Road and Bridge Research Institute (IBDiM)

Keywords: ETCS; ERTMS; laboratory testing; fault injection; saboteur; emulator

* Corresponding author. Tel.: +34-943212800; fax: +34-943213076.
E-mail address: gsolas@ceit.es

Peer-review under responsibility of Road and Bridge Research Institute (IBDiM)
doi:10.1016/j.trpro.2016.05.156

1. Introduction

Nomenclature

BTM	Balise Transmission Module
DMI	Driver Machine Interface
EMC	Electromagnetic Compatibility
EMI	Electromagnetic Interference
EATS	ETCS Advanced Testing and Smart Train Positioning System
ERA	European Railway Agency
ERT	Euroloop Leaky Cable Reference Tool
ERTMS	European Railway Traffic Management System
ETCS	European Train Control System
EVC	European Vital Computer
FFFIS	Form Fit Functional Interface Specification
GSM-R	Global System for Mobile Communications - Railway
GRM	Golden Reference Model
JRU	Juridical Recording Unit
LTM	Loop Transmission Module
ODO	Odometer
OS	Operating System
SC	Scenario Controller
SIL	Safety Integrity Level
TCP	Transmission Control Protocol
THR	Tolerable Hazard Rate
TSI	Technical Specification for Interoperability
TIU	Train Interface Unit
TSOE	Test Signal of the On-board Equipment
UMTS	Universal Mobile Telecommunications System
WCE	Wireless Communication Emulator

Currently European Train Control System (ETCS) rollout is a major concern for train manufacturers and railway infrastructure operators. Available ETCS equipment suffered from a long process before being put into service. One of the reason of such a long process deals with the need of the costly field-testing phase of ETCS on-board equipment. The laboratory procedures and tools need to be improved in order to reach the objective of “Zero On--Site Testing” searched for long time.

Two of the main improvements have to do with: first, the testing of the safety functions of the ETCS on-board equipment; second, with the capability of reproducing in the laboratory the worst case scenarios that such equipment will encounter when put in the field.

It is proved that ERTMS on-board equipment is considered a safety critical system and it must be designed against failures. For that, according to the corresponding normative, internal faults inside the ETCS sub-systems have to be injected to provide evidences of the robustness against failures.

On the other hand, the presence of electromagnetic interferences (EMI) is considered as serious issue regarding the availability of the ETCS system, and therefore it also affects the cost and duration of the on-board equipment’s testing phase. Moreover, current laboratory procedures and tools don’t address completely the question of testing the equipment against the worst case of EMIs it must overcome when operating in real environments.

This research work has been carried out with two objectives: first, to develop the suitable tools to enable the gathering of evidences regarding the safety functionalities of ETCS on-board equipment; second, to develop laboratory tools that allow to test that equipment in the worst conditions that its wireless interfaces can find in real environment, specially focusing on the electromagnetic interferences.

For that, two new laboratory tools have been created: the saboteur, an autonomous device prepared to test the safety of the equipment by injecting faults in the internal interfaces. And the Wireless Communication Emulator (WCE), a tools that can be used to inject different kinds of noise and interferers in the airgap between the wireless interfaces of the on-board equipment and the corresponding trackside equipment. Both tools have been designed taking into account the existing specifications regarding the testing laboratories in which they have to be integrated. This work shows how the design and implementation of these novel tools have been carried out.

2. State of the Art and current problems

This section introduces the safety testing and the Wireless Communication Emulation, moreover, the current issues are also described.

2.1. Safety testing

ERTMS on-board equipment has safety functions with a tolerable hazard rate of less than 10^{-9} F/h. The hazards of the different functions contributing to the core hazard of the ERTMS on-board equipment are identified in (SUBSET091) and a safety target for them is derived. Thus, all the functions have been assigned a THR and a safety integrity level (SIL). Therefore, ERTMS on-board sub-systems are designed against failures. (IEC61508) and (EN50129) impose requirements to the architecture to fulfil this safety figure as redundancy and physical independency. Moreover, (IEC61508) and (EN50129) require tests to assess safety, where Fault Injection is a mandatory part.

As the normative defines, internal faults inside the ETCS sub-systems have to be injected to provide evidences to the Notified Body. These failures do not occur during normal operation, so if the test is only done as a black box as defined by ETCS test normative, the safe function implementations will not be tested since there is no ETCS technical specification to test safety. Traditional methods to inject faults cannot be used for safety assessment as they change the operations conditions of the product.

Previous EU projects as (EMSET) only defined functional testing and therefore the normative available as (SUBSET076), (SUBSET094) for on-board ERTMS system validation testing, (SUBSET085) for BTM testing, and (SUBSET103) for LTM testing, only addresses functional tests. The entire test normative for the ETCS considers the systems or functionalities as black boxes and therefore extra functionality to implement reactive or composite safety is not evaluated, thus the fulfilment of (EN50129) or (IEC61508) is not assured with these tests. Therefore, ETCS test specification does not define any fault introduction to test safety of the equipment, even though it must be tested.

2.2. Wireless Communication Emulation

A number of norms exist regarding railway EMC as (EN50121) series, (EN50238), ((EN50388), (EN50122) and (EN50215)). These include train detection, signalling systems (BTM and LTM), and telecommunications (both land and air based). However, the limits defined do not ensure a safe operation. The scientific community has gone one step forward describing and analysing concrete situations of electromagnetic interferences (EMI) between the rolling stock and a wide range of systems, applications, etc., which are not covered by the previously mentioned standards, such as EMI and GSM-R (N. Ben Slimen et al. 2008), EMI and spot signalling systems (J. del Portillo et al. 2008), (I. Adin et al. 2012). However, the electromagnetic noise in the track is still unpredictable.

Due to the noise and interferences in the railway environment, air-gap communication can be corrupted and therefore, ETCS service stopped. Some previous experiences have been found as ETCS has been out of service due to the problems found in the air-gap communication. Electromagnetic environment is not included when testing the system and therefore, air-gap problems are not translated to the test cases employed nowadays. Previous EC funded works have not addressed the problem entirely yet (i.e. (RAILCOM)), although nowadays, (TREND) project is working towards the full definition and modelling of the track noise.

2.3. Current issues

The current technology employed in testing the ETCS onboard equipment shows some problems. On the one hand, the verification of the safety related functions as defined by (EN50128) and (EN50129) requires specific safety testing. However, the corresponding technical specification defining the test procedures for the safety requirements for the complete on-board ERTMS does not exist. Moreover, the necessary laboratory tools to address the testing of such safety features does not exist either. Thus, novel test strategies have to be developed and carried out to provide safety assessment evidences to the Notified Body.

On the other hand, occasionally problems still appear even in already tested equipment because the trains have not been tested against the worst case real scenarios that the systems may find in the field (e.g. electromagnetic compatibility issues). Then, neither the responsibilities nor the technical solutions are straight forward. The duration of the field-testing employed to solve this railway EMC problems may vary between 3 and 12 months, and the cost of the complete process may vary between 25k€ to 1,5M€ (ERA 2010). This situation could be improved by employing a more realistic model of the air gap interfaces that the ETCS onboard equipment uses for some of its functionalities.

3. Objectives

The main objective of this research work consists of advancing towards the so called “Zero On-Site Testing” paradigm. For that, two secondary objectives must be fulfilled.

(SUBSET076) specifies the methodology to test the on-board ERTMS system in order to assure the fulfilment of the functionality described in (SUBSET026) baseline v.2.3.0. The functional requirements for the test facilities currently available and its architecture in which all the test sequences from (SUBSET076) can be evaluated is defined in (SUBSET094). The testing methodology and laboratory architecture can be improved by overcoming their drawbacks, in order to reduce the time and effort in the verification and certification processes.

Thus, the two improvements which lead to the fulfilment of the objectives are:

- Fault injection in the internal and external interfaces to aid the safety assessment. By employing saboteurs in the interfaces it is possible to excite the functionality of the different subsystems in order to check the failsafe state.
- Emulator of the dynamic behaviour of the wireless interfaces to test the on-board system with the representative worst case conditions these interfaces will find. Especially relevant is the inclusion of EM fields generated by the train during the regenerative break, the cross with other trains, or the reduction of the signal to noise ratio by the arcing of the pantograph.

4. Proposal

This research work proposes to add new tools to the ETCS On Board Class 1 reference test architecture specified in (SUBSET094). Fig. 1 shows the ETCS Advanced Testing Strategy proposed by EATS. Saboteurs and Wireless Communication Emulators have been defined and implemented by EATS project for that ETCS Advanced Testing Strategy. For testing and validation purposes, an implementation of the reference testing facility has been implemented. There is an equivalence between the modules of that implementation and the building blocks of the reference architecture. That equivalence is indicated by the acronyms in parenthesis.

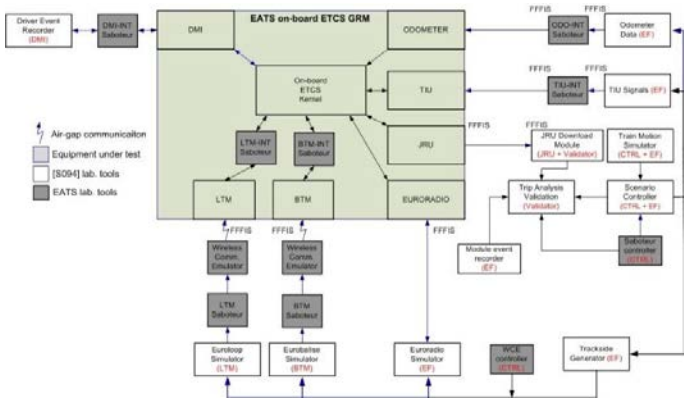


Fig. 1. ETCS Advanced Testing Strategy.

The strategy proposed by this work in order to overcome the first of the aforementioned problems consists of using fault injection techniques by means of saboteurs in communications between physically independent parts. The reproduction of the consequences in communications emulates faults in low levels, and the response of the complete system can be observed.

On the other hand, the strategy followed to include the realistic air-gap scenario into the on-board ERTMS laboratory testing, Wireless Communication Emulators (WCE) are proposed. Two different WCE have been developed, one for each air-gap links of the on-board ERTMS system (BTM and LTM). As shown in Fig. 1, the Wireless Communication Emulators take the signal created by the simulators currently employed in the ETCS testing laboratory, and include the effects expected in the track due to noise and/or interferences.

5. Saboteurs

This section lists the faults to be injected by the saboteur and the interfaces to be sabotaged. Additionally, the implementation of the saboteurs is also shown.

5.1. Faults to be injected

The first step in developing new tools to test the safety functionality of ETCS onboard equipment consists of identifying the necessary safety requirements. Afterwards, EATS project completes ETCS specifications by defining the faults to be included to the system in order to assess its safety by means of saboteurs and therefore define a way of providing evidences to the Notified Body.

This paper describes the methodology that has been followed, in order to define the mentioned faults. That methodology consists of the following steps:

- Identify the hazards to which safety functions are related to.
- Identify the safety functions of the module of the referred interface from the standard.
- Identify specific functionality for the on-board equipment.
- Identify specific hazards for the on-board equipment.
- Identify the tasks that can fail and affect to the safety.
- Identify the tasks that can fail and affect to the availability, if there are any.
- Identify the faults that can be injected to provoke the failure of the previous tasks.

5.2. Interfaces to be sabotaged

Fig. 1 shows which saboteurs have been developed are which interface each of them applies to: Driver Machine Interface (SUBSET033), Train Interface Unit (SUBSET034), Balise Transmission Module (SUBSET036), Loop Transmission Module (SUBSET044) and Odometer (EEIG 97E267).

Internal communications between functionalities are company specific, for example the communication between BTM and the Kernel. Thus the company specific communications shall be adapted to the testing interfaces. For the testing interfaces Ethernet protocol has been chosen, since Ethernet is the protocol that is nowadays being employed for railway applications, including safety systems (M. Hassan et al. 2008), (M. Aziz et al. 2008) and (Westermo 2011).

Regarding the nature of the interfaces to be sabotaged, two types of saboteurs can be identified:

- ***Interface saboteurs***: these are the saboteurs that operate at packet level, modifying the data packets that travel through the Ethernet connection.
- ***Physical saboteurs***: for those interfaces that are defined as having a wireless transmission channel, interface saboteurs don't fulfill all the requirements needed to inject the whole list of identified faults. This is due to the fact that some fault require to alter the physical properties of the wireless signal transmitted through these interfaces. Thus, saboteurs that operate at physical signal level have been created for the BTM and LTM interfaces.

5.3. Implementation

This subsection describes the implementation of the two types of saboteurs, the interface saboteurs and the physical saboteurs.

5.3.1. Interface saboteurs

Since message modification tasks does not require many resources consumption, interface saboteurs offer an efficient solution for EATS fault injection. Located in wired communication between devices, interface saboteurs modify the communication information between devices. Interface saboteurs are transparent for every device in EATS Laboratory and act as a logical bridge between devices whose communication is intended to be sabotaged.

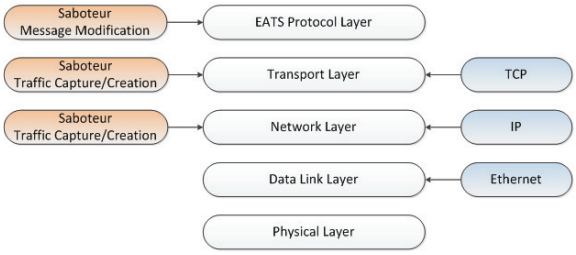


Fig. 2. ETCS Advanced Testing Strategy.

Fig. 2 shows a layer diagram of communication and saboteur level actions. The intended traffic is captured through network and transport layers and information modification is done at "EATS Protocol Layer". At "EATS Protocol Layer" each event has associated an event time with it (this event time makes reference to the relative time of each EATS event from the beginning of the simulation). Interface saboteur modifies, deletes or creates packets containing the information according to the event time.

Interface saboteurs for EATS are implemented using "Rasbperry Pi model B" boards. The decision of choosing "Rasbperry Pi model B" has made based on its reduced size and running Linux feature, which enables the use of all routing characteristics that Linux OS offers. The operating system chosen for "Raspberry Pi" board is "Raspbian". It provides more than a pure OS: it comes with over 35,000 packages, pre-compiled software bundled in a nice format for easy installation. Interface saboteurs make a special use of these Linux packages:

- ***Bridge-utils***: it provides the functionality for making network bridges for network interfaces.
- ***Netfilter/Iptables***: it offers various options for packet filtering, network address translation, and port translation.

Apart from those, interface saboteurs are endowed with a database and two "ad-hoc" running executables listening to them:

- ***Interface Saboteur Database***: each interface saboteur holds a MySQL database in order to store needed information for interface saboteur actions.
- ***Listening Configurator***: developed in Java. "Listening configurator" is listening at a TCP port. When a connection is made from EATS network configurator module to this port (it means that needed data for interface saboteur is set in Interface Saboteur Database) this software interprets filtering information at Interface Saboteur Database table and establishes the proper "iptables" rules for filtering actions. Once filtering configuration is done, it runs the actuators at specified ports.
- ***Actuator***: the actuator is an application executable developed in C language. This software performs sabotage actions based on Interface Saboteur Database information.

5.3.2. Physical saboteurs

Physical Saboteurs are implemented within the computational models that simulate the BTM and LTM components of the onboard ETCS equipment, and also within the models that simulate the Eurobalise and Euroloop signal generators. The saboteurs are integrated in them. The aim of these two saboteurs is to introduce faults at a physical level, operating inside the building blocks of these modules, in order to force an incorrect operation of the corresponding device.

The Balise Transmission Module (BTM) physical saboteur operation is controlled from the Scenario Controller (SC). The SC provides saboteur with all the information required to make available to the EVC both correct BTM information and data signals including different types of errors adequate to evaluate the safety behavior of the EVC. Similarly to the BTM function, the saboteur architecture includes two sets of modules reproducing the functionalities of the trackside equipment (balise set) and the on-board one (on-board set), respectively.

The Loop Transmission Module (LTM) physical saboteur operation is also controlled from the Scenario Controller (SC), which provides saboteur with all the information required to make available to the EVC both correct LTM information and data signals including different types of errors adequate to evaluate the safety behaviour of the EVC. Similarly to the LTM function, the saboteur architecture includes two sets of modules reproducing the functionalities of the trackside equipment (loop set) and the on-board one (on-board set), respectively.

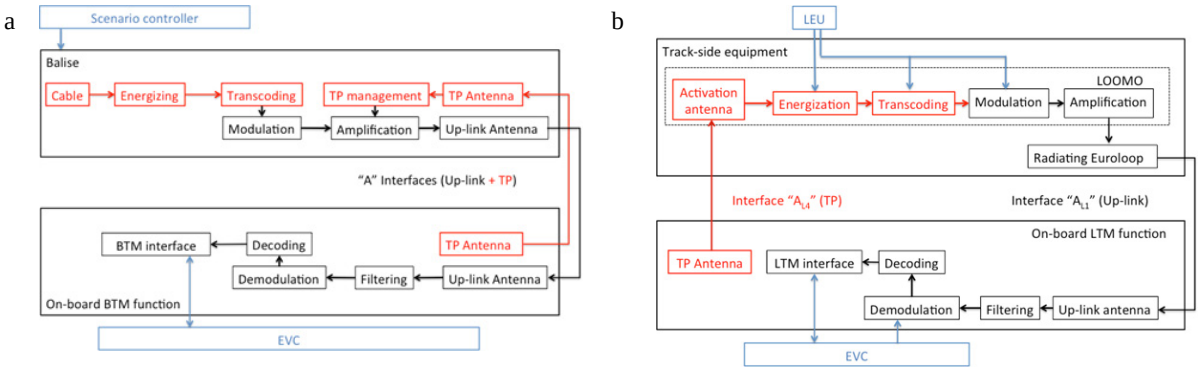


Fig. 3. (a) BTM physical saboteur architecture; (b) LTM physical saboteur architecture.

6. Wireless Communication Emulators (WCEs)

The WCE reproduce the potential interferers that can be found in the air gap of BTM and LTM wireless communication channels. The identification of the potential interferers to be included in the emulators has been done first, and the design and implementation of the emulators has been carried out afterwards.

6.1. Potential interferers

Regarding the BTM operation, (SUBSET036) constitutes the mandatory requirements for achieving air-gap interoperability. Specifically for the threats to take into account for the BTM air gap, the section "6.7.4 In-band Susceptibility" has to be considered. This section defines that the Eurobalise on-board Transmission equipment (BTM) shall be able to operate when being exposed to a pure sinusoidal constant wave disturbance radiated noise and a transient as defined by Fig. 4.

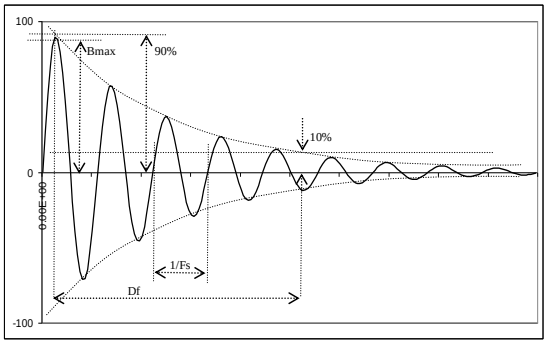


Fig. 4. Shape of the Damped Interference Signal.

Regarding the LTM operation, it is (SUBSET103) that defines a number of expected interferers in front of which LTM has to accomplish its function. A list Test Signal of the On-board Equipment (TSOE) is included in the specification.

6.2. Wireless Communication Emulator of the Balise Transmission Module

The goal of the BTM WCE is to inject the balise signal accompanied by the noise interferers into the BTM function. Then, the sum of the signals could be faced prior to its injection in the air gap or subsequent to it. Moreover, the signals could be summed from the generation or from the reception, in the air or by software. The final option implemented in this research work is shown in Fig. 5.

a b

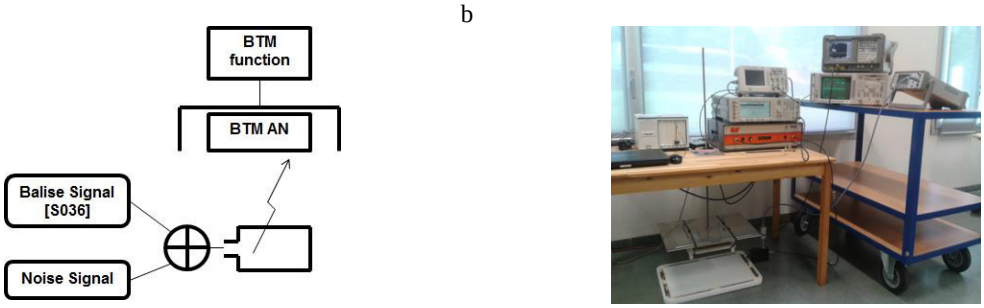


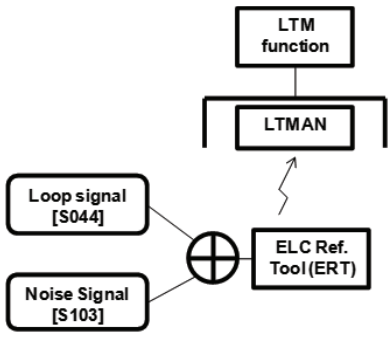
Fig. 5. (a) BTM WCE architecture; (b) Laboratory implementation of BTM WCE.

The main components are: a Signal Generator, which generates both the noise and balise signals; a Reference Loop, which inject the signal in the air gap; a BTM Antenna, which is in charge of receiving the signal coming from the air-gap; and the BTM function, composed of specific tools and components that reproduce the operation of the on-board BTM subsystem.

6.3. Wireless Communication Emulator of the Loop Transmission Module

This research work proposes the LTM Wireless Communication Emulator architecture shown in Fig. 6. It complements the overall LTM system and test-benches with the consideration of the air gap. The setup is similar to the one proposed for the BTM WCE.

a



b

Fig. 6. (a) LTM WCE architecture; (b) Laboratory implementation of LTM WCE.

The main components are: a Signal Generator, which generates both the noise and balise signals; a Euroloop Leaky Cable Reference Tool (ERT), which inject the signal in the air gap; a LTM Antenna, which is in charge of receiving the signal coming from the air-gap; and the LTM function, composed of specific tools and components that reproduce the operation of the on-board BTM subsystem.

7. Conclusions

This research work shows the results obtained to reach the objective of “Zero On-Site Testing” for ETCS on--board equipment. For that, an analysis of the requirements made by the specifications has been done and current technology’s problems have been identified. In order to overcome those problems, two new tools are proposed: saboteurs, which inject faults deliberately in the internal interfaces of the equipment under test, and Wireless Communication Emulators, that generate and add noise and interferers to the wireless communication channels used by the ETCS equipment to communicate with the trackside equipment.

These new tools provide the testing laboratories with the capability of increasing the number and type of tests to perform to ETCS equipment, thus reducing the duration and cost of field-testing.

Acknowledgements

This work is funded by FP7-TRANSPORT under the project EATS contract number 314219.

References

Adin, I., Mendizabal, J., del Portillo J., 2012. Railway Safety, Reliability, and Security: Technologies and Systems Engineering: Impact of Electromagnetic Environment on Reliability Assessment for Railway Signalling Systems.

Aziz, M., Raouf, B., Riad, N., Daoud, R.M., Elsayed, H.M. (2008). The Use of Ethernet for Single On-board Train Network; American Univ. in Cairo, Cairo. IEEE International Conference on Networking, Sensing and Control, ICNSC 2008.

CENELEC EN50121: Railway applications - Electromagnetic compatibility – Parts 1, 2, 3–1, 3–2, 4 and 5.

CENELEC EN50122: Railway applications. Fixed installations. Protective provisions relating to electrical safety and earthing. 1998.

CENELEC EN50128: Railway applications. Communication, signalling and processing systems. Software for railway control and protection systems.

CENELEC EN50129: Railway applications. Communication, signalling and processing systems. Safety related electronic systems for signalling.

CENELEC EN50215: Railway applications. Testing of rolling stock after completion of construction and before entry into service. 1999.

CENELEC EN50238: Railway applications. Compatibility between rolling stock and train detection systems. 2003.

CENELEC EN50388: Railway applications. Power supply and rolling stock. Technical criteria for the coordination between power supply (substation) and rolling stock to achieve interoperability. 2005.

CENELEC IEC61508: Functional Safety of Electrical/Electronic/Programmable Electronic Safety-related Systems.

del Portillo, J., Osinalde, M., Sukia, E., Sancho, I., Mendizabal, J., Meléndez, J. (2008). Characterization of the EM environment of railway spot communication systems. Symposium on Electromagnetic Compatibility, 2008. EMC 2008. IEEE International.

EMSET FP4 Granted European Project 1996–1999: Eurocab Madrid-Seville European tests.

ERA (2010). 67575_ERA_EMC_Final_Report - Study to collect and document rules, processes and procedures to verify the electromagnetic compatibility of railway vehicles in member states of the European rail area, for ERA. Lloyd's Register group. 2010.

ERTMS USERS GROUP EEIG 97E267: EEIG 97E267 ODOMETER FFFIS Issue 5.

Hassan, M., Gamal, S., Louis, S.N., Zaki, G.F., Amer, H.H. (2008). Fault tolerant Ethernet network model for control and entertainment in railway transportation systems; Electron. Eng. Dept., American Univ. in Cairo. Canadian Conference on Electrical and Computer Engineering, CCECE 2008.

RAILCOM 2005–2008 FP6 Granted European Project: Electromagnetic compatibility between rolling stock and rail-infrastructure encouraging European interoperability.

Slimen, N. Ben, Deniau, V., Baranowski, S., Rioult, J., Dubalen, N., Démoulin, B. and Consortium Railcom (2007). On Board Measurements of the Railway's Electromagnetic Noise with Moving Train. Proceedings, 18th Int. Zurich Symposium on EMC, Munich 2007.

TREND 2011–2013: FP7 Granted European Project: Test of Rolling Stock Electromagnetic Compatibility for cross-Domain interoperability.

UNISIG SUBSET026. System requirement specification. Issue 2.3.0.

UNISIG SUBSET033. FIS for Man-Machine interface. Issue 2.0.0.

UNISIG SUBSET034. FIS for Train interface. Issue 2.0.0.

UNISIG SUBSET036. FFFIS for Eurobalise. Issue: 2.3.2.

UNISIG SUBSET044. FFFIS for Euroloop. Issue: 2.3.0.

UNISIG SUBSET076. ERTMS/ETCS Class 1, test plan; Subset 076, Issue: 2.3.1.

UNISIG SUBSET085. Test Specification for Eurobalise FFFIS, issue 2.2.2.

UNISIG SUBSET091. Safety Requirements for the Technical Interoperability of ETCS in Levels 1 & 2, Issue 2.5.0.

UNISIG SUBSET094. Functional Requirements for an on board Reference Test Facility. Issue 2.0.2.

UNISIG SUBSET103. Test Specification for Euroloop FFFIS, Issue 1.0.0.

Westermo (2011). The Ethernet Train, Westermo Robust Industrial Data Communications.