Measurement 67 (2015) 164–176

Contents lists available at ScienceDirect

Measurement

journal homepage: www.elsevier.com/locate/measurement

# A safety instrumented system for rolling stocks: Methodology, design process and safety analysis

David Macii [a,*], Stefano Dalpez [b], Roberto Passerone [c], Michele Corrà [d], Manuel Avancini [e], Luigi Benciolini [e]

[a] Dep. of Industrial Engineering, University of Trento, Via Sommarive, 9, 38123 Trento, Italy
[b] Fondazione Bruno Kessler (FBK), Via Sommarive, 18, 38123 Trento, Italy
[c] Dep. of Information Engineering and Computer Science, University of Trento, Via Sommarive, 9, 38123 Trento, Italy
[d] Tretec S.r.l., Via Solteri, 38, 38122 Trento, Italy
[e] Saira Electronics S.r.l., Via Fornaci, 35, 38068 Rovereto, Italy

ARTICLE INFO

*Article history:*
Available online 19 January 2015

*Keywords:*
Railway safety
Reliability
Diagnostic systems
Rail transportation
Electronic design
Field Programmable Gate Arrays (FPGAs)

ABSTRACT

Modern equipment for rail transportation has to be compliant with the reliability, availability, maintainability and safety (RAMS) requirements of both national regulations and international standards such as EN 50126-1:1999 and EN 50126-2:2007. Two critical hazards for passengers and personnel of a rolling stock may arise from accidental external doors opening and from unmanned train travelling due to the sudden incapacitation of the driver. In order to reduce the risk of such hazards to tolerable or, preferably, to negligible levels, ad hoc smart monitoring systems, typically referred to as dead-man's vigilance devices (DMVDs), are generally installed on trains. In this paper, the design process of a novel DMVD is thoroughly described with a special emphasis on safety issues. This process can be of interest for designers, engineers and practitioners developing safety and diagnostic systems for railway applications. The proposed DMVD is not only modular, flexible and able to meet the wanted safety specifications, but it is also characterized by lower development costs than other solutions available on the market, as it does not include micro-controllers (MCUs) or other programmable devices running software routines. In particular, if just hardware components and Register Transfer Level (RTL) modules synthesized in Field Programmable Gate Arrays (FPGAs) are used, the correct operation of both safety and diagnostic functions can be verified through techniques normally used for hardware-only systems. In this way, the long and expensive validation and verification strategies described in specific standards for software-based safety systems (e.g. EN 50128:2011) are no longer strictly required.

## 1. Introduction

Assuring safety integrity in railway transportation must be properly addressed throughout the whole system life-cycle. Railway safety covers several aspects. First of all, railway safety is improved by designing systems that prevent accidents and dangerous situations (e.g. safe interlocking systems), whose correctness is guaranteed by a process of simulation, testing and formal analysis [1–4]. These systems are supported by a network of sensors and actuators detecting position and speed of trains to distribute route information through appropriate signalling [5].

Another aspect is related to the detection and prevention of faults in infrastructures and to the establishment

* Corresponding author. Tel.: +39 0461 281571; fax: +39 0461 282093.
*E-mail addresses:* david.macii@unitn.it (D. Macii), stefano.dalpez@gmail.com (S. Dalpez), roberto.passerone@unitn.it (R. Passerone), michele.corra@3tec.it (M. Corrà), manuel.avancini@sairaelectronics.com (M. Avancini), luigi.benciolini@sairaelectronics.com (L. Benciolini).

http://dx.doi.org/10.1016/j.measurement.2015.01.002
0263-2241/© 2015 Elsevier Ltd. All rights reserved.

of barriers against the occurrence of hazards. In particular, it is widely recognized that deploying smart monitoring systems on trains, platforms or along railways can greatly improve safety. In this context, a number of approaches has been developed to measure quantities and to monitor events which are correlated with the onset of potentially dangerous situations, i.e. defective roller bearing [6], superstructure deformation [7], subgrade settlement [8], wheel wear and stress in the interaction with rails [9,10], train position and speed [11], and possible obstacles [12,13].

A parallel concern is related to: system design methodology and verification and validation (V&V) strategies. The purpose of these strategies is to check the compliance of a system with the *reliability*, *availability*, *maintainability* and *safety* (RAMS) requirements of widely accepted international standards, such as, for instance, EN 50126-1:1999 and CLC/TR 50126-2:2007 [14,15]. Three different approaches to analyse the safety of electronic systems for rolling stocks are described in [16], where the authors compare the policy reported in the IEC standard 61508:2010 [17], the results of a Fault Tree Analysis (FTA), and an alternative method based on Markov-chain models [18].

In this paper we present the whole design process, the main features and the safety analysis of a novel *dead-man's vigilance device* (DMVD) for railway vehicles. This kind of instruments monitors both the speed of a rolling stock and the driver's behaviour in order to lock the external doors and to detect driver's accidental incapacitation while the train is in motion [19]. Operator's monitoring in railway applications has been the subject of several studies, which are well summarised in the literature [20,21]. However, the detailed relationship between a set of *Safety Instrumented Functions* (SIFs) and the corresponding *Safety Integrity Levels* (SILs) is seldom made available to the wider public, as it is generally reported in confidential documents only.

In this paper instead all the development steps and the design choices are thoroughly described and justified from a safety-oriented standpoint in order to ensure compliance with existing standards, most notably EN 50126-1:1999, CLC/TR 50126-2:2007 and IEC 61508:2010 [14,15,17]. Moreover, this paper provides general methodological guidelines that can be applied well beyond the scope of the DMVD described in this work. The developed system is innovative, because it has been explicitly conceived to be flexible (i.e. adaptable to different types of trains and contexts) without using micro-controllers (MCUs) or other programmable devices running software routines. As known, all software-based safety-oriented systems should rely on complex V&V strategies [22–24], expensive development tools and certified third-party middleware, to meet the requirements of specific standards such as EN 50128:2011 [25]. This, in turn, results in high development costs and makes the evaluation of safety requirements difficult and sometimes even questionable. In our work the validation problem is addressed by completely avoiding the use of software routines. This can be done by implementing safety and diagnostic functions at the Register Transfer Level (RTL) in Field Programmable Gate Arrays (FPGAs). The use of FPGAs in safety–critical systems certainly is not new. For instance, in [26] the authors propose an FPGA-based safety system for the railway interlocking equipment of crossing gates.

In general, whenever a programmable logic device is configured with RTL-based, hard-coded modules without using MCU cores, the whole system can be regarded mainly as *hardware-only*, thus assuring good flexibility and expandability at reduced development costs. This is due to two main reasons. First of all, both FPGAs and Complex Programmable Logic Devices (CPLDs) offer the possibility to avoid on-line and start-up tests which instead are required by MCU-based systems [27]. A simple sanity check of the bit-stream loaded into the FPGA is generally enough to ensure that the device is configured correctly. Secondly, even if RTL module design can be a bit more time-consuming than using higher-level (i.e. behavioural) coding styles, major benefits arise because of the deterministic and parallel nature of these hardware-like components [28]. Moreover, the correct operation of individual modules can be checked as if they were purely hardware circuits. In addition, FPGAs exhibit superior real-time performances in industrial applications [29], and offer the possibility to add redundancy and diagnostic functions within the same device, as shown in the work by Girardey et al. [30]. We have indeed taken advantage of this feature to add a number of self-test functions to improve the overall diagnostic coverage of the DMVD.

A preliminary safety analysis of the DMVD described in this paper is explained in [31]. This analysis has led to the first DMVD prototype presented in [32]. However, no methodological details are reported in those papers. Moreover, the safety analysis was done *a priori* to guide the design process. In this paper instead, we provide a full *a posteriori* analysis starting from a precise definition of all hazards to prove clearly and step-by-step how and why the developed system meets the wanted SIL requirements according to the existing safety standards.

The rest of the paper is structured as follows. In Section 2, the safety problem is clearly explained. In Section 3 at first the safety specifications of the DMVD to be designed are defined; then the development process is described. Section 4 deals with the system architecture, a description of safety and diagnostic functions and some implementation issues. Finally, Section 5 reports the results of the a posteriori safety analysis in different configurations (i.e. single-channel mode, redundant-channel mode, and redundant-channel mode with diversity). Section 6 concludes the paper.

## 2. Safety problem overview

The safety problem addressed in this paper is related to two specific hazards that may occur in rolling stocks, i.e.

1. The accidental opening of external doors while the train is in motion (hazard H1).
2. The unmanned travelling of the train as a consequence of a sudden incapacitation of the driver (hazard H2).

In safety engineering the level of acceptance of any hazardous situation is often classified in a semi-qualitative way on the basis of both its frequency of occurrence and the severity of consequences [14,17]. A preliminary hazard analysis based on

- statistical data [33];
- past experience of experts working in the field of railway applications;
- the classification scheme reported in Tables 2 through 6 of Standard EN 50126-1:1999 [14];

led to the conclusion that, if no countermeasures are taken, the frequency of occurrence of hazard H1 can be classified as *probable* (e.g. from 1 in 3 months to 1 in 1.25 years), with consequences that can be ranked as *critical* (i.e. "causing a single fatality and/or severe injury" [14]). In fact, the passengers' behaviour is generally hardly predictable and, in addition, it is quite common to find people standing in the proximity of doors, e.g. because they are willing to get off shortly, or simply because the train is overcrowded.

As far as hazard H2 is concerned, the hourly probability that an apparently healthy man with an age between 18 and 59 suddenly experiences a fainting spell is in the order of $10^{-6}$ [33]. Therefore, the frequency of occurrence of hazard H2 can be conservatively classified as *remote* (i.e. "likely to occur sometimes in the system life cycle"). However, in this case the severity of consequences can be *catastrophic* (i.e. causing "fatalities and/or multiple severe injuries and/or major damage to the environment" [14]), because all passengers (and not only those standing next to the doors) can be potentially involved in a serious accident.

As a result of the classification above, according to the Standard EN 50126-1:1999, the risk levels associated with hazards H1 and H2 can be ranked respectively as *intolerable* and *undesirable*. The former hazard shall be ideally eliminated. The latter instead can be accepted only "when risk reduction is impracticable and with the agreement of the Railway Authority or the Safety Regulatory Authority, as appropriate" [14]. In practice, such Authorities require to meet specified *acceptable* safety levels, which generally depend on national or international regulations. Since these requirements may change depending on the context and the country where the train is used, in the following the values reported in Table A.1 of Standard CLC/TR 50126-2:2007 will be taken as a reference [15]. In particular, from this table it turns out that *critical* and *catastrophic* hazards (such as H1 and H2) can be regarded as *tolerable* if they are at least *improbable* (i.e. with a frequency of 1 event in 35–175 years), or *negligible* if their frequency is made smaller than 1 in 175 years assuming continuous operation. To this purpose, a *Safety Instrumented System* (SIS) is needed to decrease the original probabilities of occurrence.

Consider that if no specific a priori information is available on both the type of rolling stock and its mission profile, the *Total Hazard Rate* (THR) of either H1 or H2 when the train is in motion can be roughly assumed to be constant over time. In practice, the average THR depends also on the duty cycle of the train, namely on the number of hours travelled per day. If we conservatively assume that the train is used continuously, the THR value corresponding to 1 event in 175 years is about $6.5 \cdot 10^{-7}\ \mathrm{h}^{-1}$. However, to achieve full risk acceptability, the THR values associated with hazards H1 and H2 have to be decreased further. Evidently, a SIS addressing the safety problem above should include two SIFs, i.e.

- A function monitoring the speed of the rolling stock to lock the external doors when the train speed is different from zero (function S1).
- A function monitoring the vigilance of the operator driving the train. If no drivers' activity is detected for a significant amount of time, at first an alarm can be triggered and then the emergency brake has to be activated (function S2).

Therefore, the *safe state* is reached when the doors of the train are kept locked and the brake is activated. The Standard CLC/TR 50126-2:2007 provides a well-defined relationship between target THR values and SIL functional requirements. In particular, 4 SIL levels are defined, i.e.

- SIL 4 for $10^{-9} \leqslant \mathrm{THR} < 10^{-8}\ \mathrm{h}^{-1}$.
- SIL 3 for $10^{-8} \leqslant \mathrm{THR} < 10^{-7}\ \mathrm{h}^{-1}$.
- SIL 2 for $10^{-7} \leqslant \mathrm{THR} < 10^{-6}\ \mathrm{h}^{-1}$.
- SIL 1 for $10^{-6} \leqslant \mathrm{THR} < 10^{-5}\ \mathrm{h}^{-1}$.

Therefore, if the target THR is $6.5 \cdot 10^{-7}\ \mathrm{h}^{-1}$, at least a SIL 2 system is needed. However, only with a SIL 3 system, i.e. able to ensure a THR smaller than $10^{-7}\ \mathrm{h}^{-1}$, the wanted safety integrity is achieved with a good margin in different contexts. It is worth emphasizing that S1 and S2 are not functionally independent. In particular, function S2 is globally disabled by S1 when the railway vehicle is stock-still, in order to allow the operator to leave the commands of the train. As a consequence, if $\mathrm{THR}_{S1}$ and $\mathrm{THR}_{S2}$ denote the target THR values associated with functions S1 and S2, respectively, the following condition should be fulfilled, i.e. $\mathrm{THR}_{S1} < \mathrm{THR}_{S2} < 10^{-7}\ \mathrm{h}^{-1}$.

## 3. Methodology

### 3.1. Definition of safety specifications

The hazard analysis described in Section 2 is based on the assumption that the system of interest is a rolling stock as a whole. Indeed, SIL allocation to individual functions "without references to relevant (and general) safety requirements would be meaningless" [15]. However, the goal of this paper is to focus just on a subsystem of the rolling stock, namely a novel DMVD, which will be briefly referred to as SAFE-MOD unit in the following. The SAFE-MOD unit shall be connected to a few *external* subsystems through simple and standard interfaces. Such subsystems are: the control commands of the train (i.e. knobs, buttons or pedals), the alarm transducers on the driver's console, the unit locking/unlocking the external doors and the emergency brake. Consider that these units are vehicle-specific, as they have to be used also for purposes that are inherently different from those of functions S1 and S2.

From a methodological standpoint, the safety-oriented design of SAFE-MOD is problematic because in railway standards such as EN 50126-1:1999, CLC/TR 50126-2:2007 and EN 50129:2003, the concepts of system and function can be hardly distinguished [34]. In particular, it can be difficult to define and to allocate the safety requirements of a subsystem that implements just part of an entire function. Fortunately, this issue can be bypassed by following the general approach described in the Standard IEC 61508:2010 [17], which instead provides a clear distinction between the equipment under control (EUC), the EUC control system and the programmable electronic system (PES) that is responsible of the safety of the EUC. From this perspective, the SAFE-MOD unit can be regarded as a PES, the rolling stock is the EUC and the external subsystems listed above represent the interface between the PES and the EUC. This interface allows to exert a control action on the EUC. In the following, we will refer to *Zero Velocity Detection* (ZVD) and *Operator Vigilance Detection* (OVD) as the fractions of functions S1 and S2, respectively, which shall be implemented in the SAFE-MOD unit.

Unfortunately, if we rely just on IEC 61508:2010, a new formal problem arises, since in railway applications the SIL levels depend on the THR values, as explained in Section 2, whereas in IEC 61508:2010 they are defined respectively in terms of [17]:

- average *probability of a dangerous failure on demand* (PFD) in low-demand modes of use;
- *probability of a dangerous failure per hour* (PFH) in high-demand modes of use.

The relationship between PFD/PFH and THR is not trivial in general and it is analysed in detail in [34]. However, the SAFE-MOD unit has to monitor *continuously* both the speed of the rolling stock and the vigilance of the driver when the train is in motion. Therefore, the SAFE-MOD unit definitely operates in high-demand mode. In situations of this kind, it is shown in [34] that the THR associated to a SIF basically coincides with the PFH of the entire system implementing the SIF. Therefore, the SIL levels specified in the IEC 61508:2010 as a function of the PFH intervals are the same as those reported as a function of the THR intervals in the EN 50126 series of standards, but under the implicit assumption that a given system fully implements the wanted SIF. In our case, this condition does not hold exactly, since, as explained above, the SAFE-MOD unit implements just part of functions S1 and S2. Thus, if we denote with $PFH_Z$ and $PFH_O$ the PFH values of functions ZVD and OVD, respectively, we must ensure that $PFH_Z < THR_{S1}$ and $PFH_O < THR_{S2}$, with $PFH_Z < PFH_O$ because ZVD also affects OVD, as already explained in Section 2. Since the subsystems of the train that are *external* to the SAFE-MOD unit implement just a small fraction of functions S1 and S2, from a design perspective, we can just ensure that $PFH_Z < PFH_O < THR_{S2}$ with a reasonable margin. In particular, if the condition above holds for $THR_{S2} = 10^{-7}$, then the SAFE-MOD unit can potentially meet the requirements of SIL 3.

It is worth emphasizing that this condition is necessary, but not sufficient for full SIL 3 compliance, since other qualitative and quantitative requirements have to be fulfilled. In terms of hardware fault tolerance, for instance, SIL 3 requires that a complex, non-redundant electronic system has a *Safe Failure Fraction* (SFF) index larger than 99% [17]. This means that full diagnostic coverage is needed during normal operation. However, if redundant architectures able to provide one-fault or two-fault tolerance are used, smaller SFF values are acceptable, i.e. ranging between 90% and 99% and between 60% and 90%, respectively. During system development, the two-fault tolerance solution was not taken into consideration because too complex and expensive. The zero-tolerant and one-tolerant configurations instead are compared in Section 5.

### 3.2. Development process

The design process of the SAFE-MOD unit is summarised in the flow-chart shown in Fig. 1. This process is general and can be applied to the development of other safety-related electronic systems for railway applications. The safety specifications of the system (see Section 3.1) result from the preliminary hazard analysis reported in Section 2. At first, we prepared a document called *safety concept* to identify the perimeter of the SAFE-MOD unit (i.e. the features of inputs and outputs in normal operating conditions) and to define its main constitutional blocks along with the relationship between them (functional and architectural breakdown). Afterwards, we performed a semi-qualitative FTA to identify the individual faults and conditions that, within the previously defined perimeter, can cause the two main hazardous events, i.e. (i) wrong zero-velocity detection and (ii) missing operator's vigilance detection. A simplified version of the FTA is shown in Fig. 2. To make the picture readable, homogeneous kinds of faults have been grouped together. For instance, the nodes labeled as "front-end hardware breakdown" can be expanded into subtrees, thus identifying more clearly individual faults at the hardware level. Note that wrong zero-velocity detection may lead to the impossibility to monitor the operator's behaviour.

The top-down FTA was followed by a preliminary coarse-grained *Failure Modes, Effects, and Criticality Analysis* (FMECA) at the architectural level. Unfortunately, the FMECA details cannot be reported for space reasons. The results of the FMECA can be used to

- to define more precisely how the faults previously identified by the FTA can turn into failures;
- to evaluate the impact of each failure both locally (i.e. within one of blocks defined in the safety concept) and globally (i.e. on the SAFE-MOD unit as a whole);
- to provide a qualitative assessment of the severity of each failure (from 1 – insignificant to 4 – catastrophic).
- to guide architectural and implementation choices during hardware design, including possible corrective actions;
- to define a list of measures aimed at reducing the risk and/or the impact of each failure. These include both the additional built-in self-testing functions that enhance the diagnostic coverage of the system and the off-line functional tests of individual modules for detecting and removing possible systematic faults in

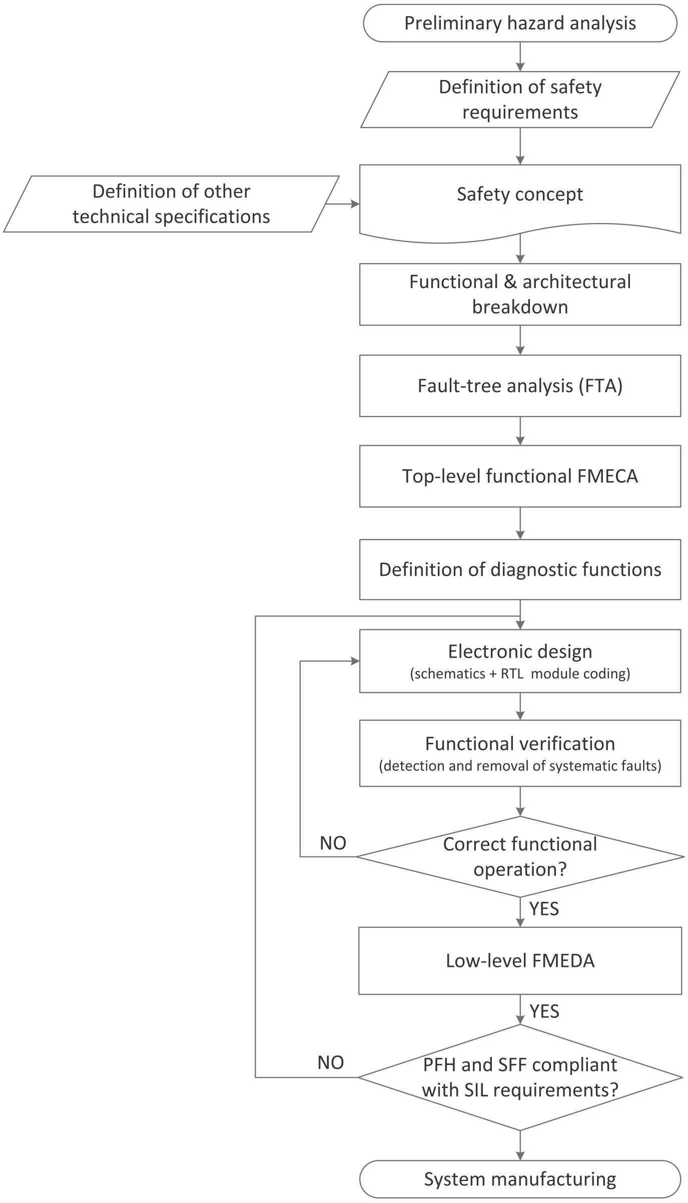
Preliminary hazard analysis
Definition of safety requirements
Definition of other technical specifications
Safety concept
Functional & architectural breakdown
Fault-tree analysis (FTA)
Top-level functional FMECA
Definition of diagnostic functions
Electronic design
(schematics + RTL module coding)
Functional verification
(detection and removal of systematic faults)
NO
Correct functional operation?
YES
Low-level FMEDA
YES
NO
PFH and SFF compliant with SIL requirements?
System manufacturing

**Fig. 1.** Process for the development of the SAFE-MOD unit.

the electronic/logic design. The results of such functional tests have to be properly and orderly documented.

In order to reduce the probability of common-cause failures due to both random and systematic faults, two different teams of engineers developed two boards, with the same architecture, similar components, but a different implementation (see Section 4.3).

As shown in Fig. 1, the design and verification steps were repeated a few times, thus leading to subsequent refinements. In order to meet the PFH and SFF specifications described in Section 3.1, the preliminary, top-level functional FMECA was transformed into a low-level *Failure Modes, Effects and Diagnostic Analysis* (FMEDA) [35]. The final values of PFH and SFF are based on the methodology proposed in [36]. The system was changed and improved a few times in order to meet the requirements of SIL 3. Further details about the safety evaluation of the system in different modes of use are reported in Section 5.

## 4. System description

### *4.1. General overview*

The role of the SAFE-MOD unit on board of a generic railroad vehicle is qualitatively shown in Fig. 3. The SAFE-MOD unit is connected to the following subsystems of the train:

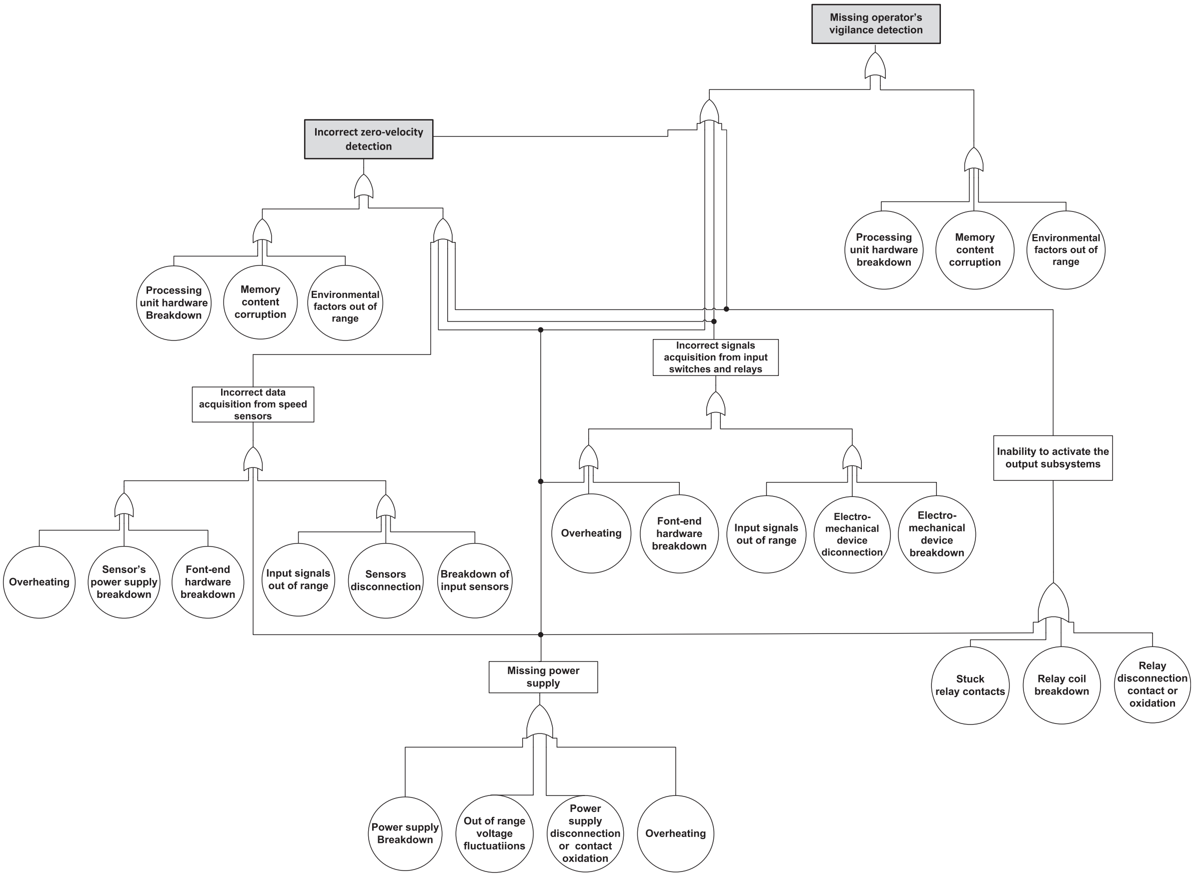
Missing operator's vigilance detection
Incorrect zero-velocity detection
Processing unit hardware Breakdown
Memory content corruption
Environmental factors out of range
Processing unit hardware breakdown
Memory content corruption
Environmental factors out of range
Incorrect signals acquisition from input switches and relays
Incorrect data acquisition from speed sensors
Inability to activate the output subsystems
Overheating
Font-end hardware breakdown
Input signals out of range
Electro-mechanical device diconnection
Electro-mechanical device breakdown
Overheating
Sensor's power supply breakdown
Font-end hardware breakdown
Input signals out of range
Sensors disconnection
Breakdown of input sensors
Missing power supply
Stuck relay contacts
Relay coil breakdown
Relay disconnection contact or oxidation
Power supply Breakdown
Out of range voltage fluctuatiions
Power supply disconnection or contact oxidation
Overheating

**Fig. 2.** Simplified Fault Tree Analysis (FTA) of the SAFE-MOD unit.

- One input switch with two contacts enabling general system operation (e.g. activated by the ignition key of the train).
- One or two control commands (i.e. pedals, buttons or knobs, each one equipped with two contacts with opposite polarity) used by the operator to drive the train.
- The emergency brake.
- An audio alarm module that is triggered when no operator's activity is detected for some time.
- An alarm module showing to the operator if a failure is detected.
- An output unit locking/unlocking external doors.
- The Event Recorder (ER) of the train, namely the "black box" that records all relevant data of a travelling rolling stock (including emergency or failure conditions detected by the SAFE-MOD unit) into a crash-hardened memory module.

Fig. 4 shows the perimeter of the system, its basic internal structure (consisting of up to two redundant safety channels, denoted with A and B, respectively), and the train subsystems that are connected directly to the SAFE-MOD unit. In Fig. 4 the stripe-patterned blocks denote the subsystems that are external to the SAFE-MOD unit. Therefore, such components do not have to be included in the final safety evaluation described in Section 5. The solid lines in Fig. 4 represent the safety–critical connections. The dashed lines denote instead the communication links used for diagnostic purposes only.

In principle, either safety channel can work as a stand-alone DMVD. In fact, redundancy is not strictly needed from the functional point of view and the communication between channels A and B can be simply disabled. However, redundancy ensures one-fault tolerance and relaxes the SFF requirements for SIL 3 systems. Of course, in redundant mode, the two channels have also to be powered by two external and independent power-supply units (PSUs). At start-up the two channels are activated by two independent general enable lines that are linked directly to the contacts of the ignition key of the locomotive. In redundant mode, each channel sends to the other: (i) a ZVD flag to inform the other channel about the status of motion of the train; and (ii) a failure clock signal that stops toggling if some failure is detected. Observe that pairs of outputs controlling the same external subsystems can be simply wired in series to have a "one out of two with diagnostics" (1oo2D) voting scheme. The details of the diagnostics functions are explained next.

### *4.2. Architectural breakdown and diagnostic functions*

Fig. 5 shows the architecture of either safety channel. This consists of several elementary modules represented by gray or white blocks. The difference between them lies

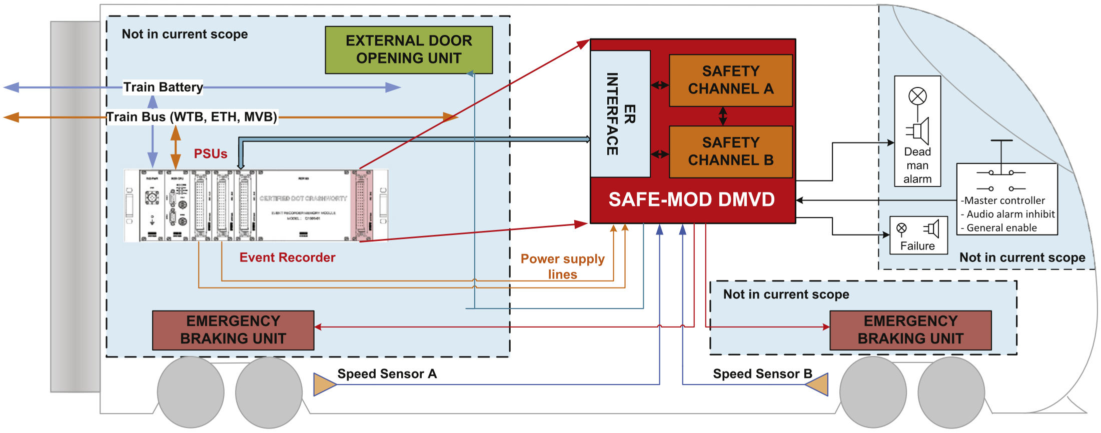

**Fig. 3.** Qualitative role of the SAFE-MOD unit. The SAFE-MOD unit has to be installed into the Event Recorder (ER) of the rolling stock to be protected from harsh environmental and electromagnetic conditions and to log safety–critical data into the crash-hardened memory module of the ER.

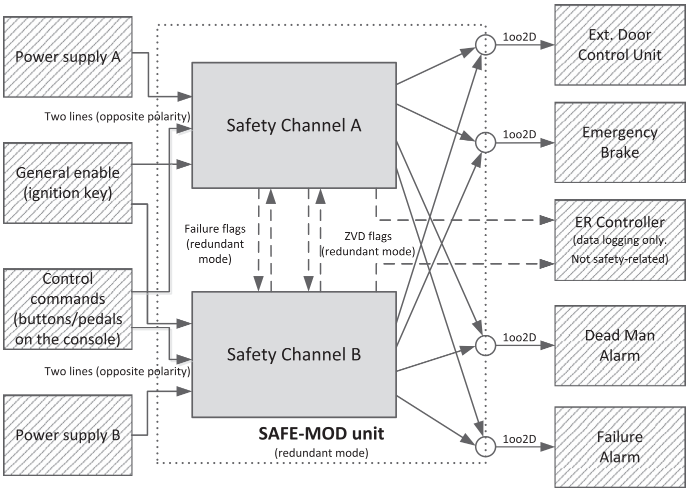
Power supply A
Two lines (opposite polarity)
General enable (ignition key)
Control commands (buttons/pedals on the console)
Two lines (opposite polarity)
Power supply B
Safety Channel A
Failure flags (redundant mode)
ZVD flags (redundant mode)
Safety Channel B
SAFE-MOD unit
(redundant mode)
1oo2D
1oo2D
1oo2D
1oo2D
Ext. Door Control Unit
Emergency Brake
ER Controller (data logging only. Not safety-related)
Dead Man Alarm
Failure Alarm

**Fig. 4.** Perimeter and top-level architecture of the SAFE-MOD unit in redundant mode.

in the fact that the gray blocks include additional functions for self-testing and diagnostic coverage, whereas the white ones do not have such features. The stripe-patterned block in this case refers to the *channel status logging unit*, which serves as an interface between each safety channel and the ER controller. This module is part of the system, but it performs read-only operations and it does not affect the ZVD and OVD functions. Therefore, it can be excluded from the safety analysis. Like in Fig. 4, solid and dashed connection lines denote safety–critical and diagnostic links, respectively.

By following the paradigm defined in the Standard IEC 61508:2010 [17], the various architectural modules are grouped into three main subsystems, i.e. the *sensor subsystem* (SS, which also comprises the front-end signal acquisition circuitry), the *logic subsystem* or *logic solver* (LS), where all the input signals are combined and processed, and the *final element subsystem* (FE) that contains mainly the output relays.

With reference to Fig. 5, S1X–S5X, L1X–L3X and F1X–F4X denote the modules belonging to the SS, LS and FE subsystems, respectively, of safety channel X (with X being A or B). In the following, the role of these modules within each subsystem will be briefly described. The diagnostic functions (DFs) identified during the preliminary FMECA and implemented inside the grey blocks are instead orderly listed in Table 1. Each DF is conceived to detect different potential hardware failures. For instance, by checking if the signals coming from the same input electromechanical device (e.g. the same pedal) have the same polarity, we can detect both abnormal input disconnections and failures in the front-end acquisition circuitry. Thus, Table 1 is a useful tool to support the low-level FMEDA mentioned in Section 3.2.

Quite importantly, most of the DFs are repeated cyclically every 500 ms. Whenever one of the DF detects an abnormal condition, the failure alarm is triggered.

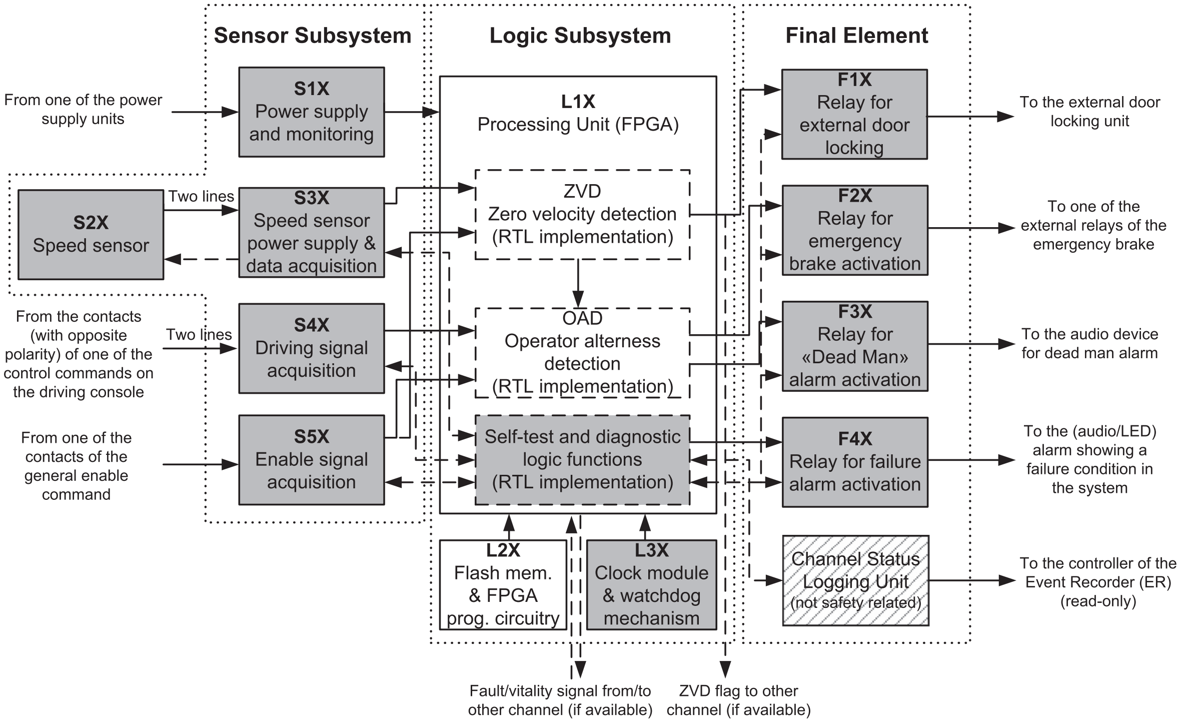
Sensor Subsystem
Logic Subsystem
Final Element
From one of the power supply units
S1X Power supply and monitoring
L1X Processing Unit (FPGA)
S2X Speed sensor
Two lines
S3X Speed sensor power supply & data acquisition
ZVD Zero velocity detection (RTL implementation)
From the contacts (with opposite polarity) of one of the control commands on the driving console
Two lines
S4X Driving signal acquisition
OAD Operator alterness detection (RTL implementation)
From one of the contacts of the general enable command
S5X Enable signal acquisition
Self-test and diagnostic logic functions (RTL implementation)
L2X Flash mem. & FPGA prog. circuitry
L3X Clock module & watchdog mechanism
F1X Relay for external door locking
To the external door locking unit
F2X Relay for emergency brake activation
To one of the external relays of the emergency brake
F3X Relay for «Dead Man» alarm activation
To the audio device for dead man alarm
F4X Relay for failure alarm activation
To the (audio/LED) alarm showing a failure condition in the system
Channel Status Logging Unit (not safety related)
To the controller of the Event Recorder (ER) (read-only)
Fault/vitality signal from/to other channel (if available)
ZVD flag to other channel (if available)

**Fig. 5.** Safety channel architecture (symbol X in all blocks can be either A or B).

**Table 1**
Overview of the diagnostic functions (DFs) implemented in the SAFE-MOD unit.

| No. | Diagnostic function (DF) | Modules implementing the DF | Modules covered by the DF |
|---|---|---|---|
| DF1 | General power supply monitoring | S1X | S1X |
| DF2 | FPGA voltage supply monitoring | S1X | L1X |
| DF3 | Speed sensor power supply monitoring | S3X | S2X |
| DF4 | Speed sensor disconnection (e.g. high-impedance condition) | S3X | S3X |
| DF5 | Consistency check between the logic values forced on S3X inputs and the corresponding values collected by L1X | S3X + L1X | S3X |
| DF6 | Detection of inconsistencies in the number of pulses collected from the two outputs of the same speed sensor | S2X + S3X + L1X | S2X |
| DF7 | Consistency check between the high/low logic values forced on S4X and S5X inputs and those collected by L1X | S4X + L1X<br>S5X + L1X | S4X<br>S5X |
| DF8 | Detection of inconsistencies in the logic state of the contacts (with opposite polarity) of one of the control commands | S4X + S5X + L1X | S4X |
| DF9 | Detection of inconsistencies between the control values produced by L1X to drive the output relays in FE and their actual boolean state | L1X + F1X<br>L1X + F2X<br>L1X + F3X<br>L1X + F4X | F1X<br>F2X<br>F3X<br>F4X |
| DF10 | Detection of bit-stream loading errors (e.g. due to flash memory corruption) | L1X | L2X |
| DF11 | Detection of a lack of vitality in LS through clock signal monitoring | L3X | L1X<br>L3X |

*4.2.1. Sensor subsystem (SS)*

The role of the SS in each safety channel is threefold, i.e.

1. powering the channel's module and monitoring the critical voltage levels (block S1X);
2. powering a speed sensor (one for each channel) and collecting the pulses generated by the sensor itself (blocks S2X and S3X);
3. collecting the signals from the other electromechanical input devices, particularly the control commands used to drive the rolling stock (block S4X) and the general enable signal linked to the ignition key (block S5X).

S1X is designed to generate power levels compatible with the electrical characteristics of the input sensors, the input front-end for signal acquisition, the processing section and the output relays. A 5-V DC input coming from the external PSUs is used to power both the relay coils inside the FE and the acquisition front-end circuitry in S3X, S4X and S5X. Two further 3.3 V and 1.2 V DC lines generated by suitable DC/DC converters are used to power the LS. Such voltage levels have to be monitored. When one of them falls below 3.07 V (for FPGA I/O blocks) or 1.12 V (for the FPGA core), respectively, a reset signal is asserted and sent to the FPGA. The same reset signal also opens the output relays, but it does not reset the FPGA configuration memory, as this feature is managed directly by the on-chip power-on reset circuitry.

Block S2X refers to a dual-output encoder (e.g. a LENORD + BAUER GEL 2475 or a similar sensor) which generates pulses with amplitude between 0 V and 15 V and frequency between 0 Hz and 20 kHz, depending on train speed. A dedicated 5–15 V DC/DC converter inside S3X is used to power the sensor. A circuit monitoring the power drain of the sensor is also included. If the sensor current drain is larger than 32 mA or if the supply voltage is lower than 10 V, a sensor power failure flag is detected by the diagnostic circuitry inside the FPGA. In addition, S3X detects whether the inputs from S2X are in a high-impedance state and collects the encoder samples through a galvanic insulator. The S3X circuitry is able to withstand large surges and bursts in compliance with the requirements of Standard IEC 61000-4-5 [37], and it also includes Schmidt triggers to reduce the probability of spurious logic transitions.

The circuitry of blocks S4X and S5X for the acquisition of the signals from the electromechanical devices located on the driver's console has similar features, although the operating range is different. Indeed, the logic values of such signals may switch between 0 V and $U_n$, where $U_n$ is the nominal voltage of the main battery of the train. In railway applications, acceptable values of $U_n$ are 24 V, 48 V, 72 V and 110 V, with a permitted tolerance range of $[0.6U_n, 1.4U_n]$ over 1 s [38]. In blocks S3X, S4X and S5X a pull-up/pull-down stage can be enabled by the FPGA to force a known logic level (either low or high) at all inputs in order to check periodically the correct operation of the input circuitry (see diagnostic functions DF5 and DF7 in Table 1).

#### 4.2.2. Logic subsystem (LS)

The LS of the SAFE-MOD unit consists of just three main architectural elements, i.e. the FPGA-based processing unit (L1X), a flash-based module to boot the FPGA (L2X) and a clock generator (L3X). The FPGA runs the ZVD and OVD functions implemented at the RTL level through a set of counters and comparators coordinated by two simple Finite State Machines (FSMs). The ZVD function measures the speed of the vehicle by counting the number of encoder pulses collected over a suitably long time interval. The value of the zero-velocity flag signal at the end of the $k$th interval is

$$F_k = \begin{cases} 1 & F_{k-1} = 0 \wedge v_k \leqslant V_1 \\ 0 & F_{k-1} = 1 \wedge v_k \geqslant V_2 \\ F_{k-1} & \text{otherwise} \end{cases} \qquad (1)$$

where thresholds $V_1$ and $V_2$ are different to prevent multiple switches due to noise or vibrations. When the train is moving, but the number of counted pulses is smaller than $V_1$, the train is considered to be still. Conversely, if the train is initially still, but the number of pulses exceeds $V_2$ the train is considered to be in motion. Counting resolution and threshold values can be changed only during maintenance (i.e. not at run-time) and depend on the type of rolling stock. For example, assuming to monitor a locomotive equipped with 80-teeth wheels of 711 mm of nominal diameter, $V_1 = 10$ pulses and $V_2 = 22$ pulses over 400-ms observation intervals correspond to 3 km/h and 6 km/h, respectively. Note that the result of (1) is used to enable/disable the vehicle-specific door locking unit and the OVD function.

Vigilance detection relies on the measurement of the time intervals between two consecutive switches of one of the signals coming from one of the input electromechanical devices used by the operator to move the rolling stock. These signals, properly acquired by S4X, are sampled at a rate of about 10 Hz. Consider that possible signal switches faster than 5 Hz are incompatible with the behaviour of a human driver. Therefore, they can be regarded as noise and filtered. When an operator is incapacitated, typically the switch or pedal is either permanently released or kept pressed. If the time interval between the moment when the input electromechanical device is released (pressed) and when it is pressed (released) again exceeds a maximum threshold $T_1$ ($T_2$), the dead-man's alarm is activated. If, in spite of this alarm, no operator's activity is detected for a further time interval $T_3$, then also the emergency brake is triggered to stop the vehicle. Once the vehicle is still, the emergency brake can then be disabled, so that the rolling stock can start moving again. The values of parameters $T_1, T_2$ and $T_3$ depend on the requirements of the chosen working environment (e.g. national regulations). However, they can be changed only during maintenance and never at run-time.

The ZVD and OVD configuration parameters $V_1, V_2, T_1, T_2$ and $T_3$ stored in the FPGA internal memory are protected by a standard 1/3 Forward Error Correction (FEC) scheme. The FPGA is completely reset and configured at power-on or whenever the voltage supply values are below the minimum tolerable thresholds specified in Section 4.2.1. The L1X module includes also (partially or totally) the diagnostic functions DF5-DF11 listed in Table 1.

The L2X module is used just to load the bit-stream from the flash memory into the FPGA. Upon loading, a sanity checksum is performed on the bit-stream. Afterwards, the flash memory is no longer used while the SAFE-MOD unit is in operation.

Module L3X generates the clock signal for L1X. The central component of L3X is a 20-MHz 3.3-V vibration-resistant crystal oscillator for industrial applications. This frequency value is much lower than the speed grade of the chosen FPGA, thus assuring good signal integrity and low power consumption, which reduces the risk of overheating. Finally, the vitality of both L1X and L3X is monitored by a watchdog timer in either channel. If no vitality (i.e. clock toggling) is detected on two L1X and L3X output pins for more than 1 s, then the failure alarm is triggered.

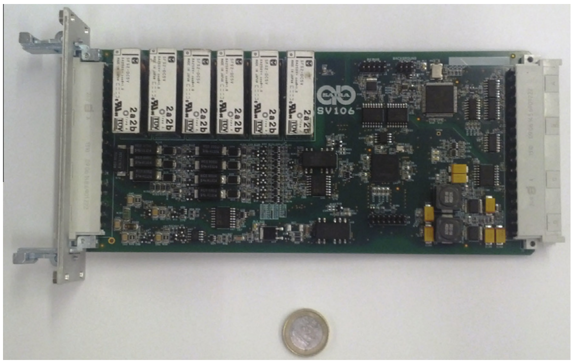

**Fig. 6.** The board SV106 implementing one of the safety channels of the SAFE-MOD unit.

### 4.2.3. Final element subsystem (FE)

The FE subsystem consists of four identical blocks, denoted as F1X–F4X. Each of them essentially relies on an electro-mechanical relay with insulation and temperature specifications compliant with the Standard EN 50155 [38]. Over-voltage protection on contacts is ensured by transils (e.g. Vishay Transzorbs). Each relay is provided with two pairs of forcibly guided contacts [39]: two normally-open (NO), and two normally-closed (NC). The former are linked to one of the external subsystem shown in Fig. 4. In redundant mode, the relays corresponding to the same output are wired in series to have a 1oo2D voting scheme. The relay sanity check is performed by a diagnostic function implemented in the FPGA. In particular, the NC contacts of each relay are linked to the FPGA to detect possible inconsistencies between the logic values applied by L1X and the actual logic state of the relays. If the FPGA outputs controlling the relay coils are in a high-impedance state (e.g. because some failure affects the FPGA itself or simply because at power-on the FPGA has not been configured yet), the relays inputs are pulled down to open all contacts, thus driving the system towards the safe state.

### 4.3. Other implementation issues

Two different versions of safety channels A and B, called SV105 and SV106, respectively, have been produced by Saira Electronics S.r.L., Rovereto, Italy. One of these boards is shown in Fig. 6. Both SV105 and SV106 are built on a Eurocard 3U Printed Circuit Board (PCB) of size 100 × 220 mm equipped with two I/O DIN41612 connectors. The rear connector is used to power the channel, to exchange failure and ZVD flags with the other channel (in redundant mode), and to send data to the ER controller through a serial link based on a proprietary protocol. The front connector is used instead to connect the safety channel to the external subsystems of the train.

To mitigate the risks of failures caused by harsh and out-of-range environmental and electromagnetic conditions (as highlighted by the FTA), the form factor of the SAFE-MOD unit is chosen to fit into the protected chassis or cabinet of the ER developed by Saira Electronics.

Both SV105 and SV106 consist of 5 galvanically insulated areas. Even if they have an identical architecture and the SS and FE subsystems rely on the same hardware components, the boards and the FPGA modules were designed by two different teams of engineers to ensure adequate diversity in redundant mode. Moreover, the LS subsections are based on two different, although similar, industrial-grade FPGAs, i.e. an Altera Cyclone II (SV105) and a Xilinx Spartan 6 XA (SV106). The configuration bitstream of either FPGA is loaded directly from a special flash memory equipped with on-chip loading features, i.e. without using MCUs. As explained in the introduction, no software routines are used to implement the safety functions and no MCU cores are synthesized in the FPGAs. All FPGA modules of both channels are implemented at the RTL level and have been tested functionally through test-bench programs relying on long sequences of input stimuli covering all possible input binary configurations.

## 5. Safety parameters evaluation

The evaluation of the safety-related parameters of the ZVD and OVD functions implemented in the SAFE-MOD unit relies on a two-step process. In the first one, a fine-grained FMEDA of boards SV105 and SV106 has been performed to determine the failure rates of the individual architectural modules. In the second step, such rates have been conservatively combined together to compute the total PFH and SFF values of each safety function.

As known, the FMEDA is an essential step to meet the requirements of the Standard IEC 61508:2010. The purpose of the FMEDA is to provide a realistic classifications of the hardware failure rates belonging to the following categories: safe detected (SD), safe undetected (SU), dangerous detected (DD), dangerous undetected (DU). In our case, at first the failure rates of all components are extracted from relevant and well-known sources such as MIL-HDBK-217f [40] and IEC TR 62380:2004 [41]. Due to the specific context in which the SAFE-MOD unit is supposed to operate, we have relied mainly on the data collected in ground mobile environments. If data from multiple sources are available, the most conservative failure rates are used in the analysis.

For each electronic component, at first the most relevant failure modes (e.g. open circuit, short circuit, open supply, changes in value) are identified and then their probability of occurrence is estimated on the basis of the statistical information and data found in [42].

The distinction between dangerous and safe failures as well as the diagnostic coverage (DC) of each component are based on the analysis of the circuits implementing the DFs reported in Table 1. In particular, the following DC values are used to partition the failure rates of the electronic components into SD, SU, DD and DU [35]:

- 0% if a failure cannot be detected;
- 50% if a failure can be detected only in specific conditions or modes of operation;
- 75% when the main part of a failure can be detected;
- 100% if a failure can always be detected.

For each category, the individual failure rates of the components belonging to the same architectural module are conservatively added together.

In order to clarify the adopted approach, we report a simple but significant example relative to the output modules F1X–F4X. Their reliability is particularly critical, since they include electromechanical components: the relays with forcibly guided contacts. The details of the FMEDA of one of these blocks are reported in Table 2. The analysis of the other blocks is similar, and is not shown for space reasons. The part failure rate $\lambda$ listed in the third column of Table 2 refers to different types of components. In our case, they are extracted from Standard MIL-HDBK-217f (in ground mobile conditions) and take into account the quality of the components actually employed (PiQ factors). The individual $\lambda$ values are at first partitioned proportionally to the probability of occurrence of different failure modes drawn from [42] (fifth column of Table 2). Afterwards, the safe detected, safe undetected, dangerous detected and dangerous undetected failure rates of each component (denoted as $\lambda_{SD}, \lambda_{SU}, \lambda_{DD}$, and $\lambda_{DU}$, respectively) result from the classification of the various failure modes (dangerous or safe) and depend on the ability of the built-in DFs to detect them, as described above. The values belonging to homogeneous categories are at first multiplied by the number of devices of the same type (second column) and then they are finally added together, as if they were functionally in series. This simplistic approach does not take into consideration the actual circuit topology, but it is classically used to have a conservative reliability estimate, which is preferable when safety functions are involved.

Table 3 summarises the FMEDA results of all modules and subsystems of one of the developed boards (i.e. SV106). The results related to the other board are almost identical, since most of the hardware components are the same. Symbols $\bar{\lambda}_i, \bar{\lambda}_{SD_i}, \bar{\lambda}_{SU_i}$, $\bar{\lambda}_{DD_i}$, and $\bar{\lambda}_{DU_i}$ denote the total, safe detected, safe undetected, dangerous detected and dangerous undetected failure rates of the $i-$th module, for $i = 1, \ldots, 13$. For instance, the values of $\bar{\lambda}_9, \bar{\lambda}_{SD_9}, \bar{\lambda}_{SU_9}, \bar{\lambda}_{DD_9}$, and $\bar{\lambda}_{DU_9}$ refer to module F1X ($i = 9$) and result from Table 2 according to the procedure explained above. The last row of the table (i.e. PCB) refers instead to an "extra" virtual module that includes all connectors and PCB traces. The rightmost column of Table 3 reports also the total diagnostic coverage of each module, defined as $\overline{DC}_i = \frac{\bar{\lambda}_{DD_i}}{\bar{\lambda}_{DD_i} + \bar{\lambda}_{DU_i}}$. The shadowed rows show the different categories of total failure rates as well as the diagnostic coverage associated with the whole SS, LS and FE subsystems. Again, such failure rates are simply and conservatively given by the sum of the corresponding modules' values building each subsystem.

In order to compute the PFH values associated to the ZVD and OVD safety functions, the results of the FMEDA have to be properly combined. To this purpose, in this paper we rely on the Reliability Block Diagram (RBD) methodology [36]. This approach allows us to evaluate the PFH of individual functions by considering just the reliability of the modules involved in their implementation. Thus, assuming that one channel only is used in the SAFE-MOD unit (1oo1D architecture), the PFH of each safety function simply coincides with the total rate of the dangerous undetected failures. In particular, if we denote with $\mathscr{M}_Z = \{1, 2, 3, 5, 6, 7, 8, 9, 13\}$ and with $\mathscr{M}_O = \{1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 13\}$ the sets of modules needed to implement functions ZVD and OVD, respectively, if follows that

$$PFH_x = \bar{\lambda}^x_{DU} = \sum_{i \in \mathscr{M}_x} \bar{\lambda}_{DU_i} \qquad (2)$$

where $x \in \{Z, O\}$ depending on whether the ZVD or the OVD function is considered. If the overall safe detected ($\bar{\lambda}^x_{SD}$), safe undetected ($\bar{\lambda}^x_{SD}$), and dangerous detected ($\bar{\lambda}^x_{DD}$) failure rates of each function are computed with a similar

**Table 2**
An example of FMEDA for blocks F1X–F4X. The various failure modes are classified as dangerous (D) or safe (S) and they are used along with the diagnostic coverage (DC) values to compute the safe detected, safe undetected, dangerous detected and dangerous undetected failure rates of each type of components.

| Component | Quantity | $\lambda$ (h$^{-1}$) | Failure mode | Failure prob. | Failure effect | DC (%) | $\lambda_{SD}$ (h$^{-1}$) | $\lambda_{SU}$ (h$^{-1}$) | $\lambda_{DD}$ (h$^{-1}$) | $\lambda_{DU}$ (h$^{-1}$) |
|---|---|---|---|---|---|---|---|---|---|---|
| SMD resistors | 6 | $1.3 \cdot 10^{-8}$ | Short-circuit | 5% | D | 100 | 0.0 | 0.0 | $6.6 \cdot 10^{-10}$ | 0.0 |
| | | | Open circuit | 59% | S | 100 | $7.8 \cdot 10^{-9}$ | 0.0 | 0.0 | 0.0 |
| | | | Change in value | 36% | S | 0 | 0.0 | $4.8 \cdot 10^{-9}$ | 0.0 | 0.0 |
| Ceramic capacitors | 2 | $1.9 \cdot 10^{-8}$ | Short-circuit | 49% | D | 100 | 0.0 | 0.0 | $9.4 \cdot 10^{-9}$ | 0.0 |
| | | | Open circuit | 22% | S | 100 | $4.2 \cdot 10^{-9}$ | 0.0 | 0.0 | 0.0 |
| | | | Change in value | 29% | S | 0 | 0.0 | $5.6 \cdot 10^{-9}$ | 0.0 | 0.0 |
| MOSFET | 1 | $9.4 \cdot 10^{-9}$ | Short-circuit | 73% | D | 100 | 0.0 | 0.0 | $6.8 \cdot 10^{-9}$ | 0.0 |
| | | | Open circuit | 27% | D | 100 | 0.0 | 0.0 | $2.5 \cdot 10^{-9}$ | 0.0 |
| Transient suppressor, transil | 2 | $2.2 \cdot 10^{-8}$ | Short-circuit | 49% | D | 100 | 0.0 | 0.0 | $1.1 \cdot 10^{-8}$ | 0.0 |
| | | | Open circuit | 36% | D | 0 | 0.0 | 0.0 | 0.0 | $7.9 \cdot 10^{-9}$ |
| | | | Parameter change | 15% | S | 50 | $1.6 \cdot 10^{-9}$ | $1.6 \cdot 10^{-9}$ | 0.0 | 0.0 |
| General purpose diodes | 1 | $1.0 \cdot 10^{-8}$ | Short-circuit | 49% | D | 100 | 0.0 | 0.0 | $5.0 \cdot 10^{-9}$ | 0.0 |
| | | | Open circuit | 36% | D | 100 | 0.0 | 0.0 | $3.7 \cdot 10^{-9}$ | 0.0 |
| | | | Parameter change | 15% | S | 50 | $7.6 \cdot 10^{-10}$ | $7.6 \cdot 10^{-10}$ | 0.0 | 0.0 |
| Forcibly guided relays | 1 | $1.5 \cdot 10^{-6}$ | Fails to trip | 55% | D | 100 | 0.0 | 0.0 | $8.2 \cdot 10^{-7}$ | 0.0 |
| | | | Spurious trip | 26% | D | 75 | 0.0 | 0.0 | $2.9 \cdot 10^{-7}$ | $9.8 \cdot 10^{-8}$ |
| | | | Short-circuit | 19% | D | 100 | 0.0 | 0.0 | $2.9 \cdot 10^{-7}$ | 0.0 |

**Table 3**
Summary of the FMEDA results for all modules and subsystems of SV106.

| Module no. | Module name | $\bar{\lambda}_i$ ($h^{-1}$) | $\bar{\lambda}_{SD_i}$ ($h^{-1}$) | $\bar{\lambda}_{SU_i}$ ($h^{-1}$) | $\bar{\lambda}_{DD_i}$ ($h^{-1}$) | $\bar{\lambda}_{DU_i}$ ($h^{-1}$) | $\overline{DC}_i$ (%) |
|---|---|---|---|---|---|---|---|
| 1 | S1X | $7.5 \cdot 10^{-7}$ | $1.9 \cdot 10^{-7}$ | $3.6 \cdot 10^{-7}$ | $1.9 \cdot 10^{-7}$ | $1.8 \cdot 10^{-8}$ | 91 |
| 2 | S2X | $2.7 \cdot 10^{-8}$ | 0.0 | 0.0 | $2.3 \cdot 10^{-8}$ | $4.0 \cdot 10^{-9}$ | 85 |
| 3 | S3X | $4.7 \cdot 10^{-6}$ | $9.9 \cdot 10^{-7}$ | $1.1 \cdot 10^{-6}$ | $2.3 \cdot 10^{-6}$ | $2.3 \cdot 10^{-7}$ | 91 |
| 4–5 | S4X-S5X | $2.1 \cdot 10^{-6}$ | $3.4 \cdot 10^{-7}$ | $3.0 \cdot 10^{-7}$ | $1.4 \cdot 10^{-6}$ | $6.1 \cdot 10^{-8}$ | 96 |
|  | Sensor subsystem (SS) tot. | $9.7 \cdot 10^{-6}$ | $1.9 \cdot 10^{-6}$ | $2.1 \cdot 10^{-6}$ | $5.4 \cdot 10^{-6}$ | $3.7 \cdot 10^{-7}$ | 94 |
| 6 | L1X | $7.3 \cdot 10^{-7}$ | $1.8 \cdot 10^{-7}$ | $1.7 \cdot 10^{-7}$ | $3.7 \cdot 10^{-7}$ | $2.2 \cdot 10^{-8}$ | 94 |
| 7 | L2X | $4.6 \cdot 10^{-7}$ | $5.9 \cdot 10^{-8}$ | $5.0 \cdot 10^{-8}$ | $3.4 \cdot 10^{-7}$ | $1.4 \cdot 10^{-8}$ | 96 |
| 8 | L3X | $3.6 \cdot 10^{-7}$ | $2.3 \cdot 10^{-8}$ | $1.4 \cdot 10^{-8}$ | $2.3 \cdot 10^{-7}$ | $8.9 \cdot 10^{-7}$ | 72 |
|  | Logic subsystem (LS) tot. | $1.6 \cdot 10^{-6}$ | $2.6 \cdot 10^{-7}$ | $2.3 \cdot 10^{-7}$ | $9.4 \cdot 10^{-7}$ | $1.3 \cdot 10^{-7}$ | 88 |
| 9–12 | F1X–F4X | $1.7 \cdot 10^{-6}$ | $5.9 \cdot 10^{-8}$ | $4.4 \cdot 10^{-8}$ | $1.5 \cdot 10^{-6}$ | $1.1 \cdot 10^{-7}$ | 93 |
|  | Finite Element Subsystem (FE) tot. | $6.7 \cdot 10^{-6}$ | $2.4 \cdot 10^{-7}$ | $1.8 \cdot 10^{-7}$ | $5.9 \cdot 10^{-6}$ | $4.5 \cdot 10^{-7}$ | 93 |
| 13 | PCB | $1.7 \cdot 10^{-7}$ | $5.2 \cdot 10^{-8}$ | $5.2 \cdot 10^{-8}$ | $2.3 \cdot 10^{-8}$ | $4.3 \cdot 10^{-8}$ | 35 |

approach, then the respective Safe Failure Fraction values $SFF_Z$ and $SFF_O$ can be obtained from

$$SFF_x = \frac{\bar{\lambda}^x_{SD} + \bar{\lambda}^x_{SU} + \bar{\lambda}^x_{DD}}{\bar{\lambda}^x_{SD} + \bar{\lambda}^x_{SU} + \bar{\lambda}^x_{DD} + \bar{\lambda}^x_{DU}} \quad \text{with } x \in \{Z, O\}. \tag{3}$$

When the SAFE-MOD unit relies on a redundant 1oo2D architecture, the situation is different because the probability of a dangerous failure per hour associated to either function results from [17]

$$\begin{aligned} PFH_x = {} & 2(1-\beta)\bar{\lambda}^x_{DU}[(1-\beta)\bar{\lambda}^x_{DU} + (1-\beta_D)\bar{\lambda}^x_{DD} + \bar{\lambda}^x_{SD}]t_{CE} \\ & + \beta_D\bar{\lambda}^x_{DD} + \beta\bar{\lambda}^x_{DU} \end{aligned} \tag{4}$$

where $\beta$ and $\beta_D$ represent the fraction of undetected and detected common-cause failures, respectively, and $t_{CE}$ is the channel equivalent mean down time given by

$$t_{CE} = \frac{\bar{\lambda}^x_{DU}(\frac{\tau_1}{2} + MTTR) + (\bar{\lambda}^x_{DD} + \bar{\lambda}^x_{SD})MTTR}{\bar{\lambda}^x_{DU} + \bar{\lambda}^x_{DD} + \bar{\lambda}^x_{SD}} \tag{5}$$

with $\tau_1$ and MTTR being the proof-test interval and the mean time to restoration, respectively. In railway applications typical values for these parameters are: MTTR = 0.5 h and $\tau_1$ = 5120 h (which corresponds to 16 h of service per day and 320 days of operation per year). Such values are derived from practical experience.

Table 4 reports the values of $PFH_Z$ and $PFH_O$ for different configurations of the SAFE-MOD unit, i.e. 1ooD, 1oo2D with two identical boards, and 1oo2D when two different boards (i.e. both SV105 and SV106) are used together. In the first case the values obtained from (2) are clearly out of the SIL 3 boundaries. However, in the contexts where a *tolerable* risk of hazards H1 and H2 is allowed according to the standard EN 50126:1999, the single-channel system could be used because the PFH values are compatible with SIL 2 specifications. Moreover, the values of $SFF_Z$ and $SFF_O$ obtained from (3) are both equal to 95%.

**Table 4**
PFH values associated to the ZVD and OVD functions of the SAFE-MOD unit in different configurations. The numbers in bold are compliant with SIL 3 specifications.

|  | 1oo1D | 1oo2D | 1oo2D with diversity |
|---|---|---|---|
| $PFH_Z$ ($h^{-1}$) | $5.9 \cdot 10^{-7}$ | $\mathbf{7.8 \cdot 10^{-8}}$ | $\mathbf{4.0 \cdot 10^{-8}}$ |
| $PFH_O$ ($h^{-1}$) | $8.8 \cdot 10^{-7}$ | $1.3 \cdot 10^{-7}$ | $\mathbf{6.6 \cdot 10^{-8}}$ |

The results in redundant mode are obtained from (4), but they differ because two distinct pairs of $\beta$ and $\beta_D$ values are used, i.e. 2% and 1% in the case without diversity, and 1% and 0.5% in the case with diversity. Such values result from the scoring-based approach described in Annex D of IEC 61508-6. Observe that only when redundancy and diversity are used together both PFH values are smaller than $10^{-7}$ $h^{-1}$, as it is required for SIL 3 compliance. Moreover, in both cases the total diagnostic coverage is also compliant with SIL 3, as $SFF_Z$ and $SFF_O$ lie in the range 90–99%.

## 6. Conclusion

Smart monitoring and safety-oriented diagnostic systems play a key role in railway applications. In this paper we have described the full design process of a novel dead-man's vigilance device (DMVD) implementing two safety functions. The proposed system is modular, flexible (i.e. suitable to different types of trains and contexts) and able to meet the wanted safety requirements. In addition, it is characterized by lower development costs than other existing solutions, as it does not include programmable devices or cores running software routines, which would require long and expensive validation and verification activities. We have thoroughly described and justified all the development steps and the design choices from a safety-oriented standpoint, in order to meet the target Safety Integrity Level (SIL). The built-in self-testing functions provide a high diagnostic coverage at run-time. The final *a posteriori* safety analysis is based on the evaluation of the probability of a dangerous failure per hour (PFH) and of the Safe Failure Fraction (SFF) in different configurations: single-channel mode, redundant-channel mode, and redundant-channel mode with diversity. The paper provides also general methodological guidelines that can be applied well beyond the scope of the DMVD presented in this work. The system is on the way to be certified by international safety authorities. Future work will be focused on extensive testing activities to verify system reliability on the field.

## Acknowledgments

The activities and results presented in this paper are part of the project "Event recorder" co-funded by Far Systems S.p.A, Saira Electronics S.r.L. and the "Provincia Autonoma di Trento."

## References

[1] C. Xiangxian, H. Yulin, H. hai, A component-based topology model for railway interlocking systems, Math. Comput. Simul. 81 (9) (2011) 1892–1900.

[2] V. Hartonas-Garmhausen, S. Campos, A. Cimatti, E. Clarke, F. Giunchiglia, Verification of a safety–critical railway interlocking system with real-time constraints, Sci. Comput. Program. 36 (2000) 53–64.

[3] A. Ferrari, G. Magnani, D. Grasso, A. Fantechi, Model checking interlocking control tables, in: E. Schnieder, G. Tarnai (Eds.), Proceedings of FORMS/FORMAT 2010, Springer, Berlin, Heidelberg, 2011, pp. 107–115.

[4] P. James, A. Lawrence, F. Moller, M. Roggenbach, M. Seisenberger, A. Setzer, K. Kanso, S. Chadwick, Verification of solid state interlocking programs, in: S. Counsell, M. Núe~z (Eds.), Software Engineering and Formal Methods, Lecture Notes in Computer Science, Springer International Publishing, 2014, pp. 253–268.

[5] K. Kanso, F. Moller, A. Setzer, Automated verification of signalling principles in railway interlocking systems, Electron. Notes Theor. Comput. Sci. 250 (2) (2009) 19–31 (proceedings of the Eighth International Workshop on Automated Verification of Critical Systems (AVoCS 2008)).

[6] C. Wang, F. Kong, Q. He, F. Hu, F. Liu, Doppler effect removal based on instantaneous frequency estimation and time domain re-sampling for wayside acoustic defective bearing detector system, Measurement 50 (2014) 346–355.

[7] B. Akpinar, E. Gülal, Railway track geometry determination using adaptive Kalman filtering model, Measurement 46 (1) (2013) 639–645.

[8] J. Yang, Q. bo Feng, A new method for measuring subgrade settlement in high-speed railway by using a linear CCD, Measurement 46 (5) (2013) 1751–1756.

[9] D. Milković, G. Simić, Ž. Jakovljević, J.T.V. Lučanin, Wayside system for wheelrail contact forces measurements, Measurement 46 (9) (2013) 3308–3318.

[10] F. Attivissimo, A. Danese, N. Giaquinto, P. Sforza, A railway measurement system to evaluate the wheel–rail interaction quality, IEEE Trans Instrum Measur 56 (5) (2007) 1583–1589.

[11] T. Engelberg, Design of a correlation system for speed measurement of rail vehicles, Measurement 29 (2) (2001) 157–164.

[12] L. Angrisani, D. Grillo, R.S.L. Moriello, G. Filo, Automatic detection of train arrival through an accelerometer, in: Proc. Instrumentation and Measurement Technology Conference, Austin, TX, 2010.

[13] J.J.D. Garcia, J.U. Urena, A.A. Hernandez, M.Q. Mazo, J.F. Vazquez, M.-J. Diaz, Multi-sensory system for obstacle detection on railways, in: Proc. Instrumentation and Measurement Technology Conference (IMTC), 2008, pp. 2091–2096.

[14] EN 50126-1:1999, Railway applications – the specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 1: Basic requirements and generic process, 1999.

[15] CLC/TR 50126-2:2007, The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – Part 2: Guide to the application of EN 50126-1 for safety, 2007.

[16] M. Catelani, L. Ciani, M. Mugnaini, V. Scarano, R. Singuaroli, Definition of safety levels and performances of safety: applications for an electronic equipment used on rolling stock, in: Proc. Instrumentation and Measurement Technology Conference Proceedings (IMTC), Warsaw, Poland, 2007, pp. 1–4.

[17] IEC 61508, Functional safety of electrical/electronic/programmable electronic safety-related system, parts 1–7, 2010.

[18] T. Winkovich, D. Eckardt, Reliability analysis of safety systems using markov-chain modelling, in: Power Electronics and Applications, 2005 European Conference on, Dresden, Germany, 2005, pp. P.1–P.10.

[19] R. Foot, G. Doniol-Shaw, Questions raised on the design of the deadman device installed on trams, Cognition Technol. Work 10 (1) (2008) 41–51. Springer-Verlag.

[20] W.I. Hamilton, T. Clarke, Driver performance modelling and its practical application to railway safety, Appl. Ergonomics 36 (6) (2005) 661–670. special Issue: Rail Human Factors.

[21] S. Lal, S.J. Lal, P. Fisher, T. Penzel, J. Agbinya, Brief overview of technology and applications in railway operator safety, in: Broadband and Biomedical Communications (IB2Com), in: 2011 6th International Conference on, Melbourne, VIC, 2011, pp. 252–258.

[22] A. Bondavalli, A. Ceccarelli, L. Falai, M. Vadursi, A new approach and a related tool for dependability measurements on distributed systems, IEEE Trans Instrum Measur 59 (4) (2010) 820–831.

[23] D. Cancila, S. Dalpez, R. Passerone, F. Terrier, An industrial case study using an MBE approach: from architecture to safety analysis, in: Proc. IEEE Int. Workshop on Model-Based Engineering for Real-Time Embedded Systems Design (MoBE-RTES), Carmona, Spain, 2010.

[24] D. Cancila, R. Passerone, T. Vardanega, M. Panunzio, Toward correctness in the specification and handling of non-functional attributes of high-integrity real-time embedded systems, IEEE Trans Indus Inform 6 (2) (2010) 181–194.

[25] EN 50128:2011, Railway applications – communications, signalling and processing systems – software for railway control and protection systems, 2011.

[26] R. Dobias, H. Kubatova, FPGA based design of the railway's interlocking equipments, in: Proc. of the Euromicro Symposium on Digital System Design (DSD), Rennes, France, 2004, pp. 467–473. http://dx.doi.org/10.1109/DSD.2004.1333312.

[27] G. Griessnig, R. Mader, C. Steger, R. Weiss, A CPLD-based safety concept for industrial applications, in: Proc. IEEE Int. Symp. on Industrial Electronics (ISIE), 2010, pp. 3027–3032.

[28] F. Salewski, A. Taylor, Systematic considerations for the application of FPGAs in industrial applications, in: Proc. IEEE Int. Symp. on Industrial Electronics (ISIE), 2008, pp. 2009–2015.

[29] S. Dalpez, R. Passerone, A. Penasa, A. Vaccari, Design of an innovative proximity detection embedded-system for safety application in industrial machinery, in: Proc. of the 17th IEEE Intern. Conf. on Emerging Technologies and Factory Automation (ETFA), Kraków, Poland, 2012.

[30] R. Girardey, M. Hübner, J. Becker, Safety aware place and route for on-chip redundancy in safety critical applications, in: Proc. IEEE Computer Society Annual Symposium on VLSI (ISVLSI), 2010, pp. 74–79. http://dx.doi.org/10.1109/ISVLSI.2010.51.

[31] D. Macii, S. Dalpez, M. Avancini, L. Benciolini, M. Corrá, R. Passerone, A safety system for zero velocity detection and operator alertness monitoring in rolling stock, in: Proc. 13th IMEKO TC10 Workshop on Technical Diagnostics, Warsaw, Poland, 2014, pp. 151–156.

[32] D. Macii, S. Dalpez, M. Avancini, L. Benciolini, M. Corrá, R. Passerone, Design of a redundant FPGA-based safety system for railroad vehicles, in: Proc. 2014 17th Euromicro Conference on Digital System Design, Verona, Italy, 2014, pp. 683–686.

[33] P.L. Clemens, System Safety Scrapbook, Jacob Sverdrup, Tullahoma, TN, USA, 2000.

[34] J. Braband, R. vom Hvel, H. Schbe, Probability of failure on demand the why and the how, in: B. Buth, G. Rabe, T. Seyfarth (Eds.), Computer Safety, Reliability, and Security, Lecture Notes in Computer Science, vol. 5775, Springer, Berlin, Heidelberg, 2009, pp. 46–54.

[35] M. Catelani, L. Ciani, V. Luongo, The FMEDA approach to improve the safety assessment according to the IEC61508, Microelectron. Reliabil. 50 (911) (2010) 1230–1235.

[36] M. Catelani, L. Ciani, V. Luongo, A simplified procedure for the analysis of safety instrumented systems in the process industry application, Microelectron. Reliabil. 51 (911) (2011) 1503–1507.

[37] IEC 61000-4-5:2005, Electromagnetic compatibility (EMC) Part 4–5: Testing and measurement techniques Surge immunity test, 2005.

[38] EN 50155:2007, Railway applications – electronic equipment used on rolling stock, 2007.

[39] EN 50205:2002, Relays with forcibly guided contacts, 2002.

[40] USA Department of Defense, MIL-HDBK-217f: Reliability Prediction of Electronic Equipment, Department of Defense of United States of America, 1991.

[41] IEC TR 62380:2004, IEC TR 62380. Reliability data handbook universal model for reliability prediction of electronics components. PCBs and equipment (emerged from UTEC 80–810 or RDF 2000), 2004.

[42] W. Fields, J. Reade, D. Mahar, Reliability Information Analysis Center (U.S.), Failure Mode/Mechanism Distributions 2013, Reliability Information Analysis Center (RIAC), 2012.