13th IMEKO TC10 Workshop on Technical Diagnostics
Advanced measurement tools in technical diagnostics for systems' reliability and safety
June 26-27, 2014, Warsaw, Poland

A Safety System for Zero Velocity Detection and Operator Alertness Monitoring in Rolling Stock

D. Macii[1], S. Dalpez[2], M. Avancini[3], L. Benciolini[3], M. Corrà[4], R. Passerone[5]

[1]*DII – University of Trento (Via Sommarive 9, Trento, Italy)*
[2]*REET Group – Fondazione Bruno Kessler (Via Sommarive 18, Trento, Italy)*
[3]*Saira Electronics S.r.l. (Via Fornaci 35, Rovereto, Italy)*
[4]*Tretec S.r.l. (Via Solteri 38, Trento, Italy)*
[5]*DISI – University of Trento (Via Sommarive 9, Trento, Italy)*

Abstract **–** Modern railroad applications must fulfill proper reliability, availability, maintainability and safety (RAMS) specifications in compliance with the requirements of widely accepted international standards such as EN 50126-1:1999 and EN 50126-2:2007. In rolling stock two complementary hazards with potential critical consequences for passengers and personnel arise from the inability to determine if a vehicle is in motion and from the inability to detect if the operator driving the train is incapacitated. While the probability of occurrence of both events is remote, the level of risk of such hazards is generally not tolerable. To assure an adequate safety integrity level (SIL) depending on the target application, ad-hoc smart monitoring systems, typically referred to as *dead-man's vigilance devices* (DMVD), are generally installed on board of rolling stocks. In this paper the safety analysis and the design procedure of a novel DMVD are described. The main elements of novelty of the proposed solution lay in its implementation, which relies on a hardware-only, potentially redundant FPGA architecture.

I. Introduction

Assuring safety integrity in transportation based on railways is a well-known issue that must be properly addressed throughout the whole system life-cycle, e.g., by following the so-called V-shaped model [1][2]. The V-shaped representation assumes that system verification and validation (V&V) strategies aimed at checking compliance with standard requirements and functional specifications are constantly and intrinsically linked to the development activities (left side of the V) as well as to assembly and installation activities (right side of the V). In this respect, the role of measurement techniques and diagnostic tools is essential at every step of system life-cycle, i.e., from design to maintenance. In particular, it is widely recognized that deploying smart monitoring systems on trains, platforms or along railways can greatly improve safety. The scientific and technical literature reports plenty of examples and solutions to enhance safety in railway applications, e.g., to detect if a train is approaching [3],[4], to track rolling stock movements in real-time [5], to measure the quality of wheel-rail interaction [6], to analyze and to avoid grade-crossing crashes [7], or simply to detect obstacles [8]. Three different approaches for safety analysis of electronic systems in rolling stock are described in [9], where the authors compare the policy described in the standard IEC 61508 [10], a Fault Tree Analysis (FTA) and an alternative method based on Markov-chain modelling [11]. In this paper, starting from an FTA and a Failure Mode, Effect and Criticality Analysis (FMECA), a novel system able to monitor the behavior of the machinist is presented. Systems of this kind are usually called *dead-man's vigilance devices* (DMVD). The primary purpose of a DMVD is to detect an abnormal lack of operator's activity when the rolling stock is in movement. Often, a DMVD is embedded in the so-called *Event Recorder* (ER) (informally referred to also as "black box"), which stores the values of all the main operating parameters of a railroad vehicle into a crash-hardened memory, so as to enable authorities to investigate on causes and responsibilities of an accident. The DMVD proposed in this paper implements a set of safety-instrumented functions (SIF) and has been developed by following the recommendations and the requirements of Standards IEC 61508 [10], EN 50126 [1], [2], EN 50129 [12], and EN 50155 [13], with the purpose of achieving a flexible trade-off between safety integrity and V&V costs.

II. General Overview

In [1] safety integrity is defined as "the likelihood that a system satisfactorily performs the required safety functions under all the stated conditions within a stated period of time." In the case considered, the main functions of interest are basically two, i.e.,

- *Zero velocity detection* (ZVD), namely the ability of the system to monitor the speed of the vehicle to detect if it is moving or not;
- *Operator's alertness detection* (OAD), i.e., the ability to detect if the driver is incapacitated, while the

vehicle is in motion.

Evidently, the ZVD function affects also the OAD function, since the latter is disabled when the railroad vehicle is detected to be stock-still. Even if no univocal safety integrity levels are assigned to these functions (as they also depend on the type of rolling stock), a SIL 2 level is often indicated in technical specifications. A preliminary hazard analysis (PHA) based on EN 50126-1 pointed out that the consequences to persons and environments of any failure affecting these two functions can be regarded as critical (i.e., potentially causing 0.625 equivalent fatalities/event), but remote (i.e., with a probability ranging between 1 in 7 years and 1 in 35 years). To mitigate the risk of such consequences and to make it compatible with at least SIL 2 requirements, a proper set of SIFs is necessary. However, for marketing reasons, products assuring higher SIL levels (i.e., SIL 3 or SIL 4) are generally recommended. A DMVD device is conceived to implement such SIFs. In particular, a DMVD does not include ZVD and OAD functions only, but shall be able to perform additional safety-oriented tasks. First of all, it must prevent the opening of the external doors while the train is in motion (be it intentional, unintentional or accidental) to avoid that people or objects fall off the vehicle and to allow passengers to get on/get off the train only when the vehicle is stock-still. In addition, a DMVD must prevent unmanned vehicle traveling if the operator is suddenly incapacitated, thus avoiding potential serious consequences for passengers and staff such as train derailment or collisions. This can be done by triggering a dedicated alarm and, if no further activity is detected, by braking the rolling stock automatically. The vehicle reaches indeed the safe state when the external doors are locked and the emergency brake is activated. Finally, the system should be able to detect if any of the functions above is affected by some fault or if some failure occurs.

The SAFE-MOD must be functionally autonomous (namely independent from other subsystems except the specified input and the output), but can be located in the chassis of existing ERs for convenience and can be assumed to be powered by the same backplane bus as the ER. The SAFE-MOD unit is connected to various sensors and actuators in order to detect the operating conditions and drive the rolling stock towards the safe state. The device receives its input from: two speed sensors (i.e., encoders) typically installed on two different wheels of the vehicle; a switch, pedal or button with two electro-mechanical contacts having an opposite polarity (one normally closed and the other normally open) used by the operator to move the vehicle; and a general-enable, double-contact switch activated by the ignition key of the train. An additional single-contact switch can be used to let the operator disable the audio alarm manually. On the output side, the SAFE-MOD unit is connected to: two external redundant relays (powered by the battery of the vehicle) enabling the emergency brakes; an audio alarm module that is triggered when no operator’s activity is detected for a given, user-defined time; another alarm module showing if some failure is detected inside the SAFE-MOD unit as well as on its inputs or outputs; and a unit which locks/unlocks the external doors of the rolling stock. Finally, the SAFE-MOD unit is supposed to be connected to the ER controller, which stores its status into the ER crash-hardened memory module.

At the core of the system are the detection algorithms, which periodically receive the digital data coming from the speed sensors on the wheels and from the switches typically located in the control console of the train. The ZVD algorithm uses two distinct (and adjustable depending on the final applications) speed thresholds (e.g., 3 km/h and 6 km/h) to detect when the vehicle is still or when it is moving. Using two thresholds assure a reasonable hysteresis that prevents multiple switching due to vibrations or noise. The OAD algorithm measures the time intervals between subsequent changes in the logic state of the switch, pedal or button used by the operator to drive the train, and raises suitable flag signals to activate the alarm or to stop the rolling stock when the measured time interval exceeds proper user-defined thresholds (typically in the order of some seconds).

III. Safety Analysis

According to our PHA based on the Standard EN 50126-1, the main hazardous situations for the proposed system derive from the risks of *false* zero-velocity detection and *missed* dead’s man detection. Such risks can be classified as *undesirable* from a safety perspective, as they may have critical consequences on both passengers and personnel. It is worth noting that the risk of *false* zero-velocity detection is not only critical per se (e.g., train external doors could be accidentally opened when the train is travelling), but it also affects the risk of *missed* dead’s man detection, because the ZVD algorithm disables the OAD algorithm when the vehicle is detected to be still. This is reasonable because in normal conditions an operator is allowed to leave the control of the train once it stops. In order to find what faults could lead to such hazardous situations, a qualitative FTA has been developed. A simplified, but well readable version of the FTA is shown in Fig. 1.

Starting from the coarse results of the qualitative FTA, a bottom-up Failure Mode, Effects, and Criticality Analysis (FMECA) has been performed to better catalogue initiating faults, to cross-check their potential effects on individual functions and at the system level and to define suitable measures for risk mitigation. The FMECA details cannot be reported for space reasons. However, the FMECA results have been used to define a general system architecture including both the main safety functions and the related risk control measures at the design level. The main features of the proposed architecture are described in the following.

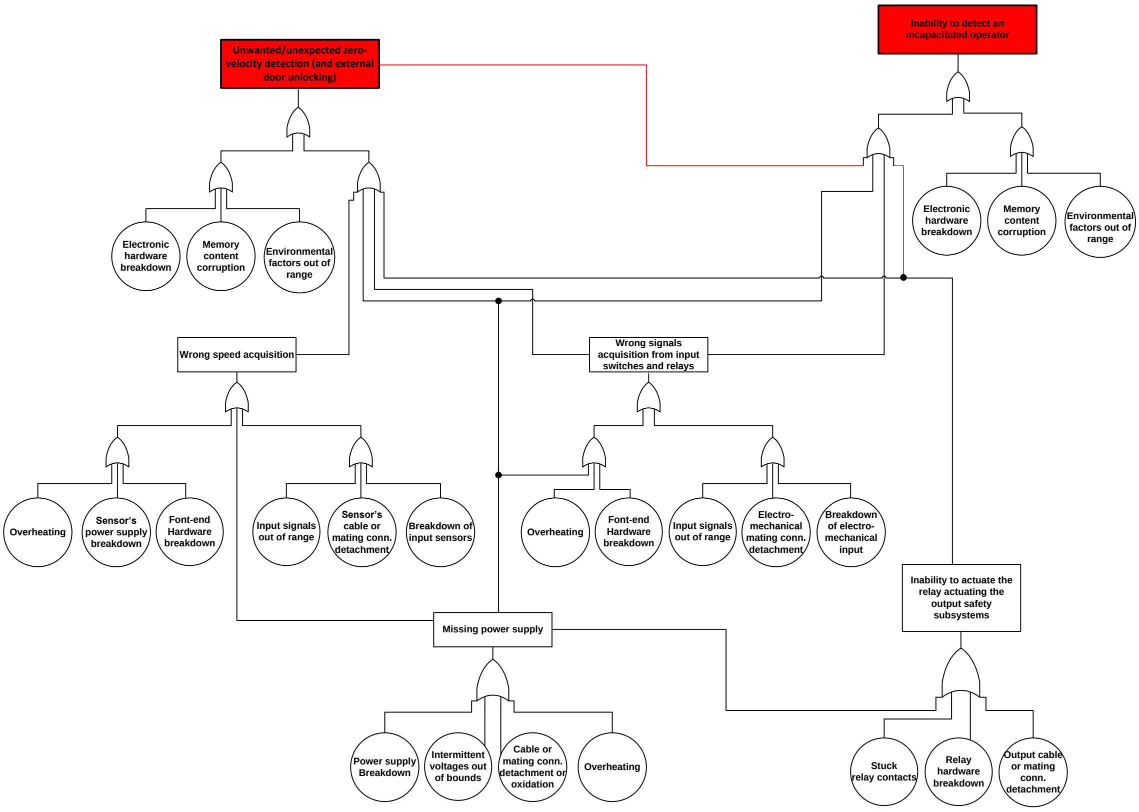

Figure 1. Simplified fault tree analysis (FTA) of a DMVD device.

- **Power supply and monitoring module**: this module 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 relays enabling the external output units. Since any power failure may lead to intermittent or permanent system shutdown and that an unexpected shutdown will certainly disrupt the ZVD and/or OAD functions, out-of-range voltage or current levels shall be properly detected. In addition, all internal power lines shall be galvanically insulated from the input power supply main line.
- **Input front-end module for signal acquisition**: this module collects signals from speed sensors and other input electromechanical devices, such as switches and external relays. Failing to collect correct input data could lead to both wrong or missed zero-velocity detection, and wrong or missed operator inactivity detection. Resilience against these failures can be obtained by means of over-voltage protection circuitry and industry-grade or automotive-grade electronic components, use of independent wiring and parallel circuitry, and self-testing modules. As required by the Standard EN 50155 [13], the outputs of this module shall be galvanically insulated from the train signal area.
- **Input front-end diagnostic module**: this module, tightly coupled with the input front-end module, implements the self-testing functions described above. In particular, it has the role of checking if the front-end circuitry is working properly, by forcing periodically known digital levels (both low and high) to all inputs, regardless of the values actually coming from sensors and electro-mechanical devices.
- **Clock generator module**: this module just generates the clock signal(s) for the processing section.
- **Processing section**: this module is mainly used to implement the ZVD and OAD functions. Obviously, any fault affecting such functions is critical because it may result in improper locking/unlocking of the external doors and/or no emergency braking when needed. Again, the safety risks can be mitigated by means of protection circuitry, industry-grade or automotive grade components, and cyclic self-testing. In addition, some kind of watchdog mechanism should be implemented to check if the processing section is active. In order to avoid completely the safety problems due to software faults, a fully hardware implementation of the processing section is envisioned [e.g., using FPGAs programmed at the Register Transfer Level (RTL)].
- **Memory**: the memory on-board of the SAFE-MOD unit shall be read-only (e.g., a Flash memory) and shall be used just to store the data for a proper initial system setup (e.g., the FPGA bit-streams). After loading the initialization data and after checking their validity, the memory shall not be used while the SAFE-MOD unit is in operation, to avoid any risk related to memory data corruption.

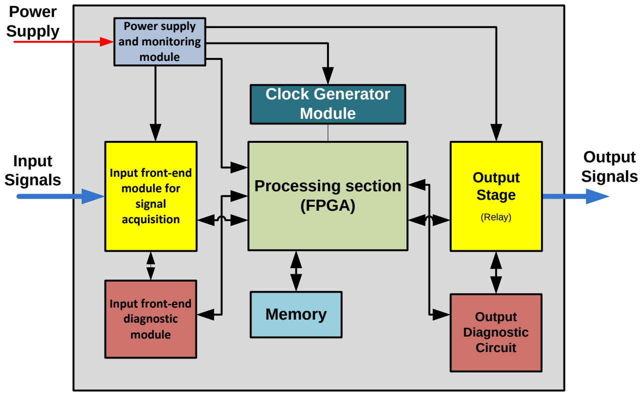

Figure 2. Architectural overview of the SAFE-MOD unit.

- **Output stage**: this module consists of independent relays controlling the various output units described in Section II. Relay inputs shall be galvanically insulated from the train signal area as recommended in [13]. Relay failures can be due to mechanical or electrical breakdown, stuck contacts, accidental disconnection of cables and/or mating connectors. Such failures may lead to the inability of the system to activate/deactivate one or more output units, with severe consequences if the operator is incapacitated or if passengers open the doors while the vehicle is in motion. These safety risks can be mitigated by high-reliability and redundant relays with forcibly guided contacts, and by using an additional diagnostic module. Relays shall have normally open contacts and shall be connected in such a way that, when they are not powered (because of some breakdown), the unit keeps the doors locked and activates the emergency braking unit.
- **Output diagnostic module**: this module is used to check if the output relays work correctly, namely if the actual logic state of each relay corresponds to the value applied to the respective control input.

A block diagram of the system is shown in Fig. 2. It is clear from the system description above, that the device has to monitor continuously both the speed of a rolling stock and the vigilance of the driver. Thus, in accordance with the Standard IEC61508-4 [10], these systems operate in a *high-demand or continuous mode*. Therefore, the quantitative safety analysis must be performed in terms of the probability to have a dangerous failure per hour (PFH). In the case of SIL 2 systems, the target PFH must lie in the interval $10^{-7} \leq PFH_D < 10^{-6}$. Before starting with component selection and hardware design, it is recommended to allocate a minimum reliability target for each block to simplify the design procedure. In our case, from a safety and reliability point of view, all modules listed above are considered as necessary to run the wanted safety functions. This means that, any failure in any module could be potentially harmful and has to be regarded as dangerous. Under this pessimistic assumption, the total PFH_D just results from the sum of the PFH_{Di} of the various modules, i.e. [10]

$$PFH_D = \sum_{i=module_i} PFH_{Di} = \sum_{i=module_i} \frac{\lambda_i}{2}(1 - DC_i) \qquad (1)$$

where λ_i and DC_i are the failure rates (per hour) and the diagnostic coverage levels (in %) associated with the *i*-th module of the system. The results of a preliminary evaluation of the target values of these parameters (assuming that no components are replaced for the whole system lifetime) are reported in Table 1. The values of λ_i are based on experience, previous reliability analyses of similar systems and data sheets of typical components for railroad applications. The values of DC_i instead have been obtained using the method reported in Standard IEC61508-4 [10]. Observe that the target PFH_D is $8.5 \cdot 10^{-7}$ [h^{-1}] with a total diagnostic coverage level greater than 80%, which is compliant with SIL 2 requirements. Therefore, the subsequent hardware design is expected to meet the requirements of Table 1. The analysis summarized above suggests also that a redundant system consisting of two parallel *safety channels* (each one meeting the reliability and architectural requirements reported in Fig. 2 and Table 1) could be designed to achieve higher SIL levels, particularly SIL 4 that requires a single-fault tolerance for any failure of the system. Of course, each channel should be functionally independent from the other and should be implemented in a different way (and with different electronic components) to improve diversity at the design level, thus reducing the probability of common-cause failures. Moreover, in order to reach a SIL4 level, each channel has to be equipped with additional diagnostic functions, able to detect possible fault conditions in the other channel and a detailed maintenance and overhaul program is need. Pairs of safety-critical outputs associated with the same function on either channel (e.g., external door unit enable, emergency braking, etc.) can be simply wired together in series. In this way, if any output incongruity is detected, then the system shall drive the rolling stock towards the safe state. As reported in the Standard IEC61508-6 [10] , a system of this kind is referred to as a “one out of two with diagnostic” (1oo2D) system.

Module	λ_i [h^{-1}]	DC_i	PFH_{Di}
Power supply and monitoring module	$1.3 \cdot 10^{-6}$	85%	$9.8 \cdot 10^{-8}$
Input front-end module for signal acquisition	$1.6 \cdot 10^{-6}$	90%	$8.0 \cdot 10^{-8}$
Input front-end diagnostic module	$1.0 \cdot 10^{-6}$	90%	$5.1 \cdot 10^{-8}$
Clock generator module	$5.5 \cdot 10^{-7}$	60%	$1.1 \cdot 10^{-7}$
Memory	$4.5 \cdot 10^{-7}$	60%	$9.1 \cdot 10^{-8}$
Processing section	$1.1 \cdot 10^{-8}$	70%	$1.7 \cdot 10^{-9}$
Output stage	$1.6 \cdot 10^{-5}$	95%	$4.0 \cdot 10^{-7}$
Output diagnostic module	$8.0 \cdot 10^{-7}$	95%	$2.0 \cdot 10^{-8}$
Total	$\mathbf{2.2 \cdot 10^{-5}}$	**81%**	$\mathbf{8.5 \cdot 10^{-7}}$

Table 1 – Preliminary evaluation of failure rates, diagnostic coverage and dangerous failures per hour.

The overall PFH_D of a redundant 1oo2D system can be evaluated as follows [10]:

$$PFH_D = 2(1-\beta)\lambda_{DU}[(1-\beta)\lambda_{DU} + (1-\beta_D)\lambda_{DD} + \lambda_{SD})]t_{CE} + \beta_D\lambda_{DD} + \beta\lambda_{DU} \qquad (2)$$

where:

- the values of β (the fraction of undetected common-cause failures), β_D (which represents the fraction of detected common-cause failures) and *DC* (diagnostic coverage level), can be set equal to 5%, 2% and 81%, respectively, as customary in redundant systems with a high level of diversity and diagnostic coverage [10];
- t_{CE} is the channel equivalent mean down time given by

$$t_{CE} = \frac{\lambda_{DU}\left(\frac{T_1}{2}+MTTR\right)+(\lambda_{DD}+\lambda_{SD})MTTR}{\lambda_{DU}+\lambda_{DD}+\lambda_{SD}}, \qquad (3)$$

  where constants T_1 = 5120 h (which means 16 h of service per day and 320 days of operation per year) and MTTR = 0.5 h are common values in railway applications and are derived from practical experience.
- Parameters $\lambda_{SD} = \frac{\lambda}{2}DC$, $\lambda_{DU} = \frac{\lambda}{2}(1-DC)$ and $\lambda_{DD} = \frac{\lambda}{2}DC$ are functions of the target reliability λ of either channel and are reported in [10].

To reach a SIL 4 level, a functional test at the beginning of each service and two overhaul per year are required. Due to space limitations, the impact of such actions on reliability is not analyzed in the paper. However, we expect that a single channel, under these conditions, could reach a rate of failure so low as $8.5 \cdot 10^{-7}$ [h^{-1}].
Using both the values in Table 1 and the data reported above, the total PFH_D achievable with a redundant system is $9.6 \cdot 10^{-9}$ [h^{-1}], which is compatible with SIL 4 requirements.

IV. System Implementation

As a result of the safety analysis described in Section III, two different versions of the SAFE-MOD unit, called SV105 and SV106, respectively, have been designed and produced by Saira Electronics S.r.L., Rovereto, Italy. Both units can work independently, but they can also be linked together to have a 2-channel 1oo2D system. If SV105 and SV106 are used together, they have to be powered by two external, independent (i.e., redundant) power-supply units (PSUs). The outputs relays of both channels are simply wired in series in pairs. Both SV105 and SV106 consist of 5 galvanically insulated areas implemented in a Eurocard 3U Printed Circuit Board (PCB) of size 100 × 220 mm equipped with two I/O DIN41612 connectors. The rear connectors are used to power the channels, to exchange fault condition and zero-velocity flags between safety channels (in redundant mode), and to read channel information from the ER controller through a serial link based on a proprietary protocol. The front connectors are used instead to connect the units to the external I/O subsystems.
The processing sections are based on an Altera Cyclone II FPGA (SV105) and on a Xilinx Spartan 6 XA (SV106) to provide adequate diversity. Both FPGAs are programmed at the RTL level and belong to the class of components for industrial applications, i.e. able to work in the temperature range [-40°,100°]. Also, the ZVD and OAD algorithms have been implemented with two different Finite State Machines (FSMs) designed by two different engineers. To avoid using external microcontroller units (MCU), the FPGA configuration bit-streams are loaded directly from dedicated flash memories. ZVD and OAD configuration parameters stored in the FPGA internal memory are protected by a standard 1/3 Forward Error Correction (FEC) scheme. Because no software routines are used to implement the safety functions and no soft-cores are implemented in the FPGAs, firmware development as well as the V&V activities do not need to comply with the requirements of Standard EN 50128 [14]. The FPGA also contains the self-test and diagnostic circuitry, which is activated cyclically (every 500 ms) to detect impending failures on all inputs and outputs. In particular, the self-test functions of each channel monitor: i) vitality and fault conditions in the other channel (redundant mode only), ii) consistency between the

actual logic state of the output relays and the respective relay control inputs, iii) consistency between the actual and the expected logic values of the inputs, iv) consistency of the speed values measured by two speed sensors installed on two different wheels, v) high impedance conditions on the inputs and vi) abnormal power drain of the speed sensors. Besides sensor power supply circuitry, the acquisition front-end stage includes analog filters and protections capable to withstand large surges and bursts in compliance with the requirements of Standard IEC 61000-4-5 [15], and Schmidt triggers to reduce the probability of spurious high-to-low or low-to-high transitions. All output relays have insulation and temperature specifications compliant with the Standard EN 50155 [13], and are provided with forcibly guided contacts in compliance with the requirements of the Standard EN 50205 [15]. Protection from large voltage swings is assured by proper transils (e.g. Vishay Transzorbs). Each relay has two normally-open contacts, and two normally-closed contacts. The first are linked to one of the external units to be controlled. The corresponding normally-closed contacts instead are read back by the FPGAs. If the FPGA outputs controlling the relay coils are in a high-impedance state (e.g., because some fault affects the FPGA or when the FPGA is not yet configured), the relays inputs are pulled down to open all contacts.

V. Conclusions

In this paper, a diagnostic safety system for rolling stock is described. The goal of the system is to detect if a railroad vehicle is in motion and if an operator is actually driving the train. System design results from a preliminary hazard analysis and a following safety analysis. The minimum target safety integrity level is SIL 2. However, a redundant and slightly modified version of the same system and a more frequent maintenance could meet the requirements of SIL 4 applications. The system has been fully implemented in hardware to reduce the complexity of V&V activities and has been developed in accordance with the specifications, recommendations and requirements of specific Standards dealing with railway applications.

References

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

[2] 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.

[3] K. Futsuhara, M. Mukaidono, “Realization of a fail-safe train wheel sensor using electromagnetic induction,” *IEEE Trans. on Instrumentation and Measurement*, vol. 38, no. 2, pp. 421-427, Apr. 1989.

[4] L. Angrisani, D. Grillo, R.S.L. Moriello, G. Filo, “Automatic detection of train arrival through an accelerometer,” Proc. *Instrumentation and Measurement Technology Conference*, Austin, TX, May 2010.

[5] A. Rubaai, “A neural-net-based device for monitoring Amtrak railroad track system,” *IEEE Transactions on Industry Applications*, vol. 39, no. 2, pp. 374-381, Mar./Apr. 2003.

[6] F. Attivissimo, A. Danese, N. Giaquinto, P. Sforza, “A Railway Measurement System to Evaluate the Wheel–Rail Interaction Quality,” *IEEE Transactions on Instrumentation and Measurement*, vol. 56, no.5, pp.1583-1589, Oct. 2007.

[7] Zu Whan Kim, T.E. Cohn, “Pseudoreal-time activity detection for railroad grade-crossing safety,” *IEEE Transactions on Intelligent Transportation Systems*, vol. 5, no. 4, pp. 319-324, Dec. 2004.

[8] 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,” Proc. *Instrumentation and Measurement Technology Conference* (IMTC) pp. 2091-2096, May 2008.

[9] 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,” Proc. *Instrumentation and Measurement Technology Conference* (IMTC), Warsaw, Poland, pp.1-4, May 2007.

[10] IEC 61508-0-1-2-3-4-5-6-7:2010, Functional safety of electrical/electronic/programmable electronic safety-related systems.

[11] T. Winkovich, D. Eckardt, “Reliability analysis of safety systems using Markov-chain modelling,” Proc. *European Conference on Power Electronics and Applications*, Dresden, Germany, pp. 1-10 Sep. 2005.

[12] EN 50129:2003, Railway applications – Communication, signalling and processing systems – Safety related electronic systems for signalling.

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

[14] EN 50128:2011, Railway applications – Communications, signalling and processing systems - Software for railway control and protection systems.

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

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