2014 17th Euromicro Conference on Digital System Design

Design of a Redundant FPGA-based Safety System for Railroad Vehicles

David Macii
DII – University of Trento
Trento, Italy
Email: david.macii@unitn.it

Manuel Avancini, Luigi Benciolini
Saira Electronics S.r.l.
Rovereto (TN), Italy
Email: manuel.avancini@sairaelectronics.com

Stefano Dalpez
REET – Fondazione Bruno Kessler (FBK)
Trento, Italy
Email: stefano.dalpez@gmail.com

Michele Corrà
Tretec S.r.l.
Trento, Italy
Email: michele.corra@3tec.it

Roberto Passerone
DISI – University of Trento
Trento, Italy
Email: roby@disi.unitn.it

***Abstract*—This paper deals with the design of a safety-critical embedded system for railroad vehicles usually referred to as "dead-man's vigilance device" (DMVD). A DMVD monitors the activity of the operator driving a train to detect his/her possible incapacitation while the vehicle is traveling. The system relies on a redundant and diverse FPGA-based architecture (without using micro-controllers, soft-cores or other software programmable components) to assure good flexibility and to avoid complex and expensive validation and verification activities of software modules, as typically required in safety-oriented applications. The first tests conducted on a prototype confirm that the system behaves correctly both in normal operating conditions and in the presence of single faults.**

***Keywords-Railway engineering, railway safety, field programmable gate arrays (FPGAs), redundancy, fault diagnosis*.**

I. Introduction

A *dead-man's vigilance device* (DMVD) is a safety system monitoring if the driver of a rolling stock is incapacitated while the train is traveling. Often, a DMVD is incorporated within the alerter or in the *Event Recorder* (ER), namely the "black box" that saves all data related to railroad vehicle operation when it is in motion [1]. The DMVDs available on the market today often rely on custom embedded platforms, with most of the safety functions implemented in software. While this approach is preferable in terms of flexibility and portability, software compliance with the requirements of safety standards, such as the EN 50128 [2], demands complex and expensive validation and verification (V&V) strategies [3]. For instance, in [4] Cancila et al. discuss ways of representing failures in software systems for railroad vehicles as non-functional annotations for safety analysis.

In this work, one of the main objectives is to avoid using software modules in the implementation of the safety functions of a DMVD device. To this purpose, safety and diagnostic functions are implemented at the Register Transfer Level (RTL) in Field Programmable Gate Arrays (FPGAs). RTL-based modules can be indeed typically regarded as *hardware* rather than *software* components, thus greatly simplifying V&V activities. In fact, Griessnig et al. [7] observe that both FPGAs and Complex Programmable Logic Devices (CPLDs) require minor software development due to the small amount of RAM and the possibility to avoid using on-board microprocessors, which would require on-line and startup tests. Salewski et al. highlight that system development based on hardware programmable devices can be more complex in safety industrial applications, but it offers clear benefits due to their performance and the parallel nature of these components [8]. Dalpez et al. employed an FPGA to achieve the required performance in the design of safety-related functions in industrial machinery [9]. In the specific context of railway applications, Dobias and Kubatova developed an FPGA-based safety system for railway interlocking equipment, to be employed at the crossing gate [8]. Conmy and Bate show how to derive the failure properties to be used in a possible safety analysis [6]. A similar approach has been applied to our case to drive a less pessimistic design. Programmable logic also promotes the implementation of on-chip redundancy and diagnostic functions [10]. We have specifically taken advantage of this feature to detect a number of critical faults identified through the preliminary safety analysis described in [11].

II. Functional Overview

The structure of our DMVD device (shortly called SAFE-MOD unit in the following) is shown in Figure 1. The two main safety functions are:

- *Zero velocity detection* (ZVD): the system must detect whether the vehicle is moving in order to lock/unlock the external doors and to enable/disable the operator's alertness detection function;
- *Operator's alertness detection* (OAD): the system must detect any prolonged lack of operator's activity while the vehicle is in motion, in order to trigger at first an audio alarm and then, if no further activity is detected, the emergency brake of the train.

The *safe state* of the vehicle is reached when the external doors are locked and the emergency brake is activated. The SAFE-MOD unit described in this paper is conceived to be functionally autonomous and independent, even if it is located in the chassis of an existing ER for convenience.

978-1-4799-5793-4/14 $31.00 © 2014 IEEE
DOI 10.1109/DSD.2014.96

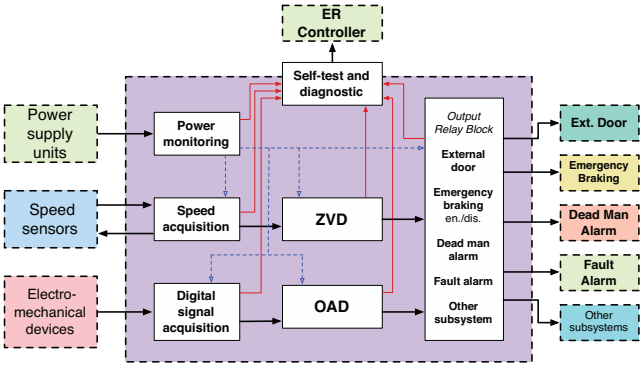

Figure 1. Functional overview of the SAFE-MOD unit

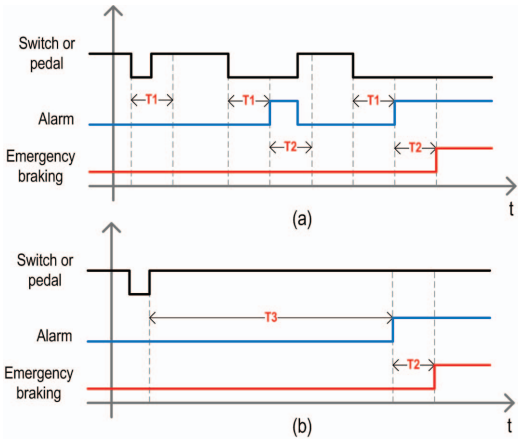

Figure 2. Timing diagram of the dead-man's device activation mechanism in the case of (a) prolonged lack of pressure on the pedal/switch, and (b) prolonged uninterrupted pressure on such commands.

In our case, the SAFE-MOD unit is powered through the backplane bus of the ER by two independent power supply units (PSU). The inputs to the system come from: two speed sensors (i.e., encoders) typically installed on two different wheels of the vehicle; a switch or pedal with two electro-mechanical contacts of opposite polarity (one normally closed and the other normally open) used by the operator to drive the rolling stock; a two-contact switch linked to the ignition key enabling the system at start-up. An additional input is used to let the operator disable the alarms, once a dead's man condition is detected and handled properly.

On the output side, the SAFE-MOD unit is connected to two external 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 some time; a failure alarm and a system which locks/unlocks the external doors. Finally, the SAFE-MOD is connected to the controller of the ER which saves information about emergency conditions or failures into the crash-hardened memory module.

At the core of the system are the detection algorithms that receive periodically the data from input sensors and switches. The ZVD function counts the pulses generated by the input speed sensors over a suitably long time interval. Two speed thresholds are used to assure a reasonable hysteresis, thus preventing multiple spurious switches due to vibrations or noise. The value of the zero-velocity flag signal at the end of the ith interval is therefore given by the following expression:

$$S_i = \begin{cases} 1 & S_{i-1} = 0 \wedge v_i \leq V_1 \\ 0 & S_{i-1} = 1 \wedge v_i \geq V_2 \\ S_{i-1} & \text{otherwise} \end{cases} \quad (1)$$

where V_1 and V_2 are the speed thresholds. 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 still, but the number of pulses exceeds V_2 the train is detected to be in motion. The values of V_1 and V_2 are expressed in terms of number of pulses and must be configurable during maintenance (depending on the type or railroad vehicle) without changing the core of the system. The duration of each observation interval must be long enough to assure adequate counting resolution when the train moves at low speeds. For instance, if 400-ms observation intervals and 80-teeth wheels with a nominal diameter of 711 mm are used, $V_1 = 10$ pulses and $V_2 = 22$ pulses correspond to 3 km/h and 6 km/h, respectively. The result of (1) is used to enable/disable the OAD function and the relays driving the unit locking/unlocking the external doors.

The OAD function measures the time intervals between two consecutive changes of the logic state of those controls (e.g. pedals, buttons, switches) normally activated by the operator to drive the train. All signals from the input electromechanical devices are sampled at a rate of about 10 Hz. Possible signal switches faster than 5 Hz are indeed incompatible with human driving behavior. So they can be regarded as noise and filtered. Two possible situations may occur if the operator is suddenly incapacitated. They are shown in Fig. 2(a) and 2(b), respectively, where:

- T_1 represents the maximum duration of the time interval between the moment when the switch or the pedal is released and when it is pressed again. If T_1 is exceeded, the dead-man's alarm signal is activated;
- T_2 is the duration of the following maximum time interval after which the emergency braking unit is triggered if no operator's activity is detected;
- Finally, T_3 is the maximum duration of the time interval between the moment when the switch or the pedal is pressed and when it is released again. If time T_3 is exceeded, the dead-man's alarm signal has to be activated. Again, if no operator activity is detected after an additional interval of duration T_2, the emergency brake is activated.

Of course, once the vehicle is detected to be still, the emergency brake can be disabled, so that the train can start moving again. Parameters T_1, T_2 and T_3 can be

configured depending on the requirements of the chosen working environment (e.g., national regulations). Possible default values are $T_1 = 2$ s, $T_2 = 2$ s and $T_3 = 10$ s.

III. System Architecture

The SAFE-MOD unit has been designed to assure an appropriate safety integrity level (SIL) that depends on the operating scenario in which the system is used. While SIL 2 was the minimum target, according to the Standard IEC 61508 [12], the highest SIL level is SIL 4. In high demand or continuous mode of operation, SIL 4 requires that the probability of a dangerous failure per hour (PFH) lies between 10^{-9} and 10^{-8}. In addition, the design, testing and maintenance strategies have to be properly defined and several different types of actions and measures are needed. In particular, at the design level, both *redundancy* and *diversity* play an essential role [13]. For this reason, the SAFE-MOD unit consists of two independent channels working in parallel and referred to as *safety channel A* and *safety channel B*, respectively. Each channel is implemented in a Eurocard 3U Printed Circuit Board (PCB) of size 100×220 mm. Either board is equipped with two I/O DIN41612 connectors. The rear plugs are used to connect the module to the ER backplane bus, to power the system, to exchange failure and zero-velocity flags between safety channels A and B, 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 link the safety channels with the field-side I/O devices, namely two speed sensors, the train console controls (ignition, pedal and switches), the dead-man's alarm disable switch, the dead-man's and failure audio alarms, the unit locking/unlocking external doors and the emergency brake relays. A *one-out-of-two with diagnostic* (1oo2D) policy is implemented in the system [12]. To this purpose, pairs of homogeneous safety-critical outputs of both channels are wired in series. In this way, the external doors are kept unlocked and the emergency brake is not enabled provided that the output logic values of both channels agree.

Both safety channels consist of 5 galvanically isolated areas to protect the internal circuitry. In order to ensure the proper physical diversity and to reduce the probability of common-cause failures, each channel uses a different style of implementation and also partially relies on different hardware components.

A 5-V DC supply in either channel is used to power the output relay coils, the signal acquisition front-end circuitry and to generate two DC sources at 3.3 V and 1.2 V, respectively, which supply the FPGA-based processing sections. These voltage levels are monitored: when either one falls below 3.07 V (for FPGA I/O blocks) or 1.12 V (for FPGA core), the FPGA is reset. A dedicated 5-15 V DC/DC converter on either channel powers one of the input speed sensors. In addition, the acquisition front-end includes analog filters and protections capable to withstand large surges and bursts in compliance with the requirements of Standard IEC 61000-4-5. Suitable Schmidt triggers partially remove spurious high-to-low or low-to-high transitions. An ad-hoc analog circuit monitors the power drain of the speed sensors (one per channel) and asserts and alarm flag if the current drain is larger than 32 mA or if the supply voltage is lower than 10 V. The same circuit also checks whether the input lines are in a high-impedance state as a result of a sensor or connection failure.

The processing sections of the SAFE-MOD unit are based on an Altera Cyclone II FPGA (channel A) and on a Xilinx Spartan 6 XA (Channel B), respectively. Both FPGAs belong to the class of components for industrial applications, i.e. able to work in the temperature range [-40°,100°]. The firmware modules inside either FPGA have been developed at the Register Transfer Levels (RTL) by two teams of designers. To avoid using external micro-controllers or other booting devices, the FPGA configuration bit-streams are loaded directly from dedicated flash memories. To ensure better signal integrity, lower power consumption and overall better reliability, the FPGAs are clocked at a much lower frequency (20 MHz) than their nominal speed grade. Since no software routines of any kind run in the FPGAs, no validation and verification activities compliant with Standard EN 50128 are strictly needed [2], thus making the system potentially cheaper than other solutions available on the market. All the safety-critical inputs coming from the acquisition front-end (except the speed sensors) pass through a bank of anti-bounce filters (ABF) removing spurious logic transitions occurring on the contacts of the electromechanical devices. The FPGAs also include self-test and diagnostic modules that are activated periodically (every 500 ms) to detect impending failures. The self-test functions provide an extensive diagnostic coverage of the system (larger than 80%). In fact, i) they monitor the vitality and the state of the other channel, ii) check if the logic states of the output relays correspond to the expected values driven by the ZVD and OAD functions, iii) detect out-of-range input signals and power levels, and iv) check possible inconsistencies between the speed values associated with sensor 1 and sensor 2. Moreover, a pull-up/pull-down stage is used by the FPGA to force periodically all inputs to a known logic level (both high and low). In this way, the correct operation of the acquisition circuitry can be checked.

The output relays have isolation and temperature specifications compliant with the Standard EN 50155, and are provided with forcibly guided contacts in compliance with the requirements of the Standard EN 50205. 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 normally-open contacts are linked to one of the external units to be controlled. The corresponding normally-closed contacts

instead are read back by the FPGAs to check for the consistency between actual and expected logic levels. If the FPGA outputs controlling the relay coils are in a high-impedance state (e.g., because some fault affects the FPGA or because the FPGA is reset and not yet configured), the relays control inputs are pulled-down by default to assure that all contacts are open.

IV. Testing Results

In order to verify the correct operation of the system prototype in a variety of possible conditions (both normal and anomalous), a suitable test-bench has been set up. This consists of the equipment under test (EUT), a variable power supply, a waveform generator able to emulate both the speed sensors and the operator's behavior, and a jig board with LEDs and switches to visually display and to control the status of the SAFE-MOD unit.

The tests have initially verified the correct functionality of the system under normal circumstances. For instance, by varying the frequency of the waveform generator we checked the operation of ZVD and OAD functions, as the speed of the train varies across thresholds V_1 and V_2. Similarly, alarms and emergency brake activation have been tested whenever the train controls are not operated for time intervals of duration T_1, T_2 and T_3. The tests have also verified that the alarms are not set off when the operator's active presence is detected.

A second round of functional tests has been conducted to verify the ability of the system to detect the expected faults on input devices (i.e. speed sensors, switches) and output relays.

Finally, multiple type tests have been conducted to measure signal integrity (e.g., in the case of over- and under-voltages of both power supply and digital inputs), electromagnetic compatibility (in terms of both radiated and conducted emissions, as well as immunity to radiated, conducted, surge and electrostatic disturbances), and climatic and insulation properties, in compliance with Standards EN 50155 and IEC 61000-4-5.

V. Conclusion

This paper describes the main features of a *one-out-of-two with diagnostic* (1oo2D) FPGA-based redundant safety system for zero-velocity and dead man's vigilance detection in railroad vehicles. Since the FPGAs are programmed at the RTL level, the safety functions do not rely on software modules running on soft-cores or micro-controllers. Therefore, the complex and expensive techniques typically required for embedded software validation and verification (in accordance with the Standard EN 50128) can be replaced by less involved, hardware-oriented methods. As a result, the proposed system is expected to be flexible and cost-effective compared with other solutions available on the market.

References

[1] R. Foot and G. Doniol-Shaw, "Questions raised on the design of the "dead-man" device installed on trams," *Cognition, Technology & Work, Springer-Verlag*, vol. 10, no. 1, pp. 41–51, 2008.

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

[3] E. Joung, C. Lee, H. Lee, and G. Kim, "Software safety criteria and application procedure for the safety critical railway system," in *Proc. Transmission Distribution Conference Exposition: Asia and Pacific*, Oct. 2009, pp. 1–4.

[4] D. Cancila, S. Dalpez, R. Passerone, and 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, May 2010.

[5] R. Dobias and H. Kubatova, "FPGA based design of the railway's interlocking equipments," in *Proc. of the Euromicro Symposium on Digital System Design (DSD)*, Rennes, France, Aug.- Sept. 2004, pp. 467–473.

[6] P. Conmy and I. Bate, "Component-based safety analysis of FPGAs," *IEEE Transactions on Industrial Informatics*, vol. 6, no. 2, pp. 195–205, May 2010.

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

[8] F. Salewski and A. Taylor, "Systematic considerations for the application of FPGAs in industrial applications," in *Proc. IEEE Int. Symp. on Industrial Electronics (ISIE)*, Jun.-Jul. 2008 2008, pp. 2009 –2015.

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

[10] R. Girardey, M. Hu andbner, and 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)*, Jul. 2010, pp. 74 –79.

[11] D. Macii, S. Dalpez, M. Avancini, L. Benciolini, M. Corrà, and 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 – Advanced measurement tools in technical diagnostics for systems' reliability and safety*, Warsaw, Poland, Jun. 2014.

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

[13] G. Corradi, R. Girardey, and J. Becker, "Xilinx tools facilitate development of FPGA applications for IEC61508," in *Proc. NASA/ESA Conf. on Adaptive Hardware and Systems (AHS)*, Jun. 2012, pp. 54–61.