A Step Toward Safe Unattended Train Operations: A Pioneer Vital Control Module

Giovanni Mezzina[1*], Arturo Amendola[2], Mario Barbareschi[3], Salvatore De Simone[2], Grazia Mascellaro[1], Alberto Moriconi[2], Cataldo Luciano Saragaglia[1], Diana Serra[2], Daniela De Venuto[1]

[1] *Dipartimento di Ing. Elettrica e dell'Informazione – Politecnico di Bari, 70125 Bari, Italy*
[2] *Rete Ferroviaria Italiana SpA, 80021 Afragola (NA), Italy*
[3] *Dipartimento di Ing. Elettrica e delle Tecnologie dell'Informazione - Università Degli Studi di Napoli Federico II, 80125 Napoli, Italy*
{name.surname}@poliba.it, mario.barbareschi@unina.it, amendola.arturo@yahoo.com, a.moriconi@rfi.it, sa.desimone@rfi.it, d.serra@rfi.it

Abstract— **Although the Automatic Train Operation (ATO) is consolidated in urban railways, its use on mainlines is still unexplored. Currently, the first prototypes of train with ATO capable of running on mainlines equipped with specific control systems (e.g., ETCS/ERTMS in Europe) have been realized. However, they require the active presence of staff on board. Recent research in innovative solutions for railway efficiency has opened to the possibility of extending the ATO concept to the Unattended Train Operation (UTO), i.e., the full automation of infrastructures and vehicles. In this context, a project based on synergistic collaboration between academia and the national railway industry has led to the definition of a new Vital Control module (VC). VC includes a PCB, managed by a reliable and safe hard Real-Time Operating System (RTOS). The hardware consists of a Eurocard-sized PCB that houses an Ultrazed-EG System on Module as computing core and embeds several communication interfaces to favor the inclusion in existing apparatus. The VC RTOS runs an application logic that acts as a real-time control core for the assessment of the on-cabin equipment operativity. VC is also responsible for detecting UTO-related hazardous situations by intervening with emergency braking. Both VC hardware and software are developed to be compliant with related safety standards. The proposed VC has been included in an automatic testbed to recreate real-time hazardous scenarios. In this context, VC system has proven to be able to mitigate these scenarios ~2 times faster than current ATO protection system.**

Keywords— Automatic Train, Safety, Vital Control, RTOS

I. Introduction

Although Automatic Train Operations (ATO) have been used in urban railways for decades with excellent results, the railway sector started investigating ATO applications on mainlines only recently [1]. The reason lies in heterogeneous traffic, various stop distances, complex track layouts, network size, open environment, and multi-operator involvement [1].

ATO is an on-board/trackside control system able to automatically manage the train movements, by respecting the journey indications/constraints. ATO is characterized by its level of automation, defined as Grade of Automation (GoA) by IEC62290-1. GoA ranges between 0 (absence of automation) to 4 (fully automated, unmanned). An ATO with GoA4, is also named Unattended Train Operation (UTO). ATO is part of a broader framework, the Automatic Train Control (ATC). The ATC includes the Automatic Train Protection (ATP) system which supervises the ATO operations safety. In Europe, the standard ATP system is the European Rail Traffic Management System / European Train Control System (ERTMS/ETCS). It consists of on-board equipment and trackside infrastructure. The described ATC architecture is known as ATO-over-ETCS [1]. Currently, ATO-over-ETCS integration prototypes are limited to the GoA 1 and 2 [2], because the related standard [3] still considers the presence of the on-board human driver mandatory. The reason lies in the low percentage of routes equipped with ETCS, e.g., only 3400 km out of 16800 in Italy. Currently, the X2Rail4 European project started defining specifications for ATO GoA 3 and GoA 4 [4]. To this aim, novel ATP modules for UTO should be introduced in the ATC, aiming to supervise vital and safety-critical functions currently ignored by ETCS. To expand these capabilities, Politecnico di Bari and Rete Ferroviaria Italiana collaborated to design and implement a novel on-board Vital Control (VC) module. VC consists of a multi-layer PCB, embedding a performant computation core (i.e., Ultrazed EG by Avnet), and several communication interfaces toward existing on-board equipment. The VC core executes a hard real-time operating system (RTOS), integrating an application logic layer that has been designed in Simulink/Stateflow with a model-based approach. VC is designed to supervise the working status of the on-board equipment, identify potential hazards, and intervene to secure the autonomous train.

Ultimately, the innovation points of the VC module are:

- a *compact* PCB design, addressing cabin space limits, and the ability to interface pre-existing on-board equipment both related to ETCS and national systems.
- the ability to evaluate in real-time the operation of equipment real-time of the on-board equipment working status.
- the VC capability in enabling safe autonomous navigation of the train (via ATO) even in the absence of or with faulty ETCS [5, 6].
- the possibility of carrying out supervised remote movements to permit remote routes maintenance, diagnostics missions, shunting or in depots operations, and in-line train recovery.
- the transparency (no interferences) to nominal ETCS operation, while extending its GoA4 ATP functions.

The paper is organized as follows. Sec. II provides an overview of the VC hardware architecture. Sec. III outlines the VC application logic. Sec. IV presents and discusses the experimental results. Sec. V concludes the paper.

II. The VC module Hardware

A. VC Module: PCB Implementation

Fig. 1 shows the realized VC module in terms of PCB implementation and hardware architecture [7, 8].

Processing Unit. The VC computation core is an Ultrazed-EG SoM based on Zynq Ultrascale+ MPSoC by Xilinx. This core runs a reliable and safe RTOS, which integrates the VC logical layer. It manages the communication drivers to interface with other cabin modules and provides access to pin banks that allow the I/O access to lines from Processing System (PS) and FPGA Programmable Logic (PL).

Communication. The VC module interfaces most of the other cabin submodules via SPI, CAN, RS-485, RS-422.

The VC provides six SPIs to interface equipment such as the

978-3-9819263-7-8/DATE23/© 2023 EDAA

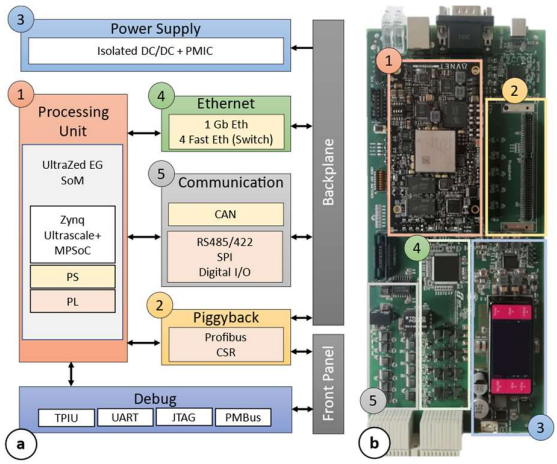

Fig. 1. Vital Control (VC) Module. (a) VC module architecture ; (b) VC PCB implementation;

Balise Transmission Module, and for the Inter-Processor Communication (IPC) in a voting architecture [7]. Two RS-485 and RS-422 have been included to interface the Multi-Vehicle Bus. CAN is used to communicate with the odometry board and watchdogs. SPI and RS-4xx drivers are integrated via PL, while CAN exploits the PS [8].

Ethernet. VC module implements 5 Ethernet interfaces, 1 Gigabit Ethernet (GbE) and 4 Fast Ethernet (100 Mbps), for data logging. The GbE exploits on-SoM media access control and the physical layers, while the 4 Fast Ethernet interfaces are obtained via a dedicated GbE Switch.

Piggyback. The VC module must communicate with the ATO onboard via Profibus according to Subset-058 [8]. In this respect, the VC module provides a piggyback slot to house a Profibus DP Master device, or the Italian train driving control system, the Continuous Signal Repetition.

Power Management. The VC is supplied with +24V. The VC power delivery network consists of an isolated DC/DC converter to step down the +24V to +12V, followed by a programmable Power Management Integrated Circuit able to extract all the SoM working voltages (i.e., +5V, +3.3V, +1.8V, +0.85V, +1.8V linear).

Debug. The VC board provides several standard debug interfaces (i.e., UART, JTAG) and a parallel Trace Port Interface Unit (TPIU) to export trace data of ARM cores.

B. Breakthrough Points

Compact Solution. The VC module functionalities (typically distributed on several boards into a rack) are condensed in a 10-layers PCB (Fig. 1.b) with a Eurocard footprint (100 mm × 220 mm) and 4 HP height. The hardware is compliant with the standards EN 50124-1 and EN 50155 [7-9].

Interchangeable. The piggyback section is designed to house two independent modules with minimum hardware variations (i.e., zero-ohm resistors) and an automatic software recognition of the piggyback. To minimize the hardware variation, a custom DB-15 receptacle is included.

III. The VC Module Software

A. VC Module: Software Stack

Starting from the lower level, the VC software stack is composed of: (1) the hard RTOS, (2) the middleware, and (3) the application logic.

RTOS. The hard RTOS schedules the tasks of the middleware and application logic. Architectural design principles of implemented RTOS are available at [10]. Specifically, the RTOS is based on a micro-kernel architecture with fixed priority scheduling. Drivers are executed in isolated applications and interface other applications via a message-passing mechanism [11].

Middleware. The middleware is responsible for the encapsulation and the information and hardware complexity hiding between the low-level functions of the communication buses and the high-level application logic.

B. VC Module: Application Logic

The VC application logic has been designed via a model-based approach by employing Simulink and Stateflow. The model has been assessed via the Simulink Model Advisor toolkit to be fully compliant with MISRA C:2012 and EN50128. The VC application logic C-language code has been automatically generated via the Embedded Coder and validated through Code Advisor for standards compliance.

The application logic is organized in three dedicated tasks as reported in Fig. 2. The implemented tasks do not share resources, but inter-communicate via non-blocking IPCs [12].

Task A manages the generation of a series of periodic fixed messages constituting the communication channel among VC, on-board equipment and ATO on-board. The messages include six requests: (i) ATO Vitality; (ii) Operator Vigilance; (iii) Emergency Brake (EB) Release Confirmation; (iv/v) ETCS Insertion/Isolation Confirmation; (vi) EB Rearm Confirmation. *ATO Vitality* permits the assessment of the working status of the ATO subsystems. *Operator Vigilance* returns the active presence of the remote operator in the trackside control room. *EB Release Confirmation* provides the operator with the ability to remotely activate the EB, while *ETCS Insertion/Isolation Confirmation* permits the remote switching off/on of the ETCS. *EB Rearm Confirmation* allows the operator to proceed with safe recovery operations.

Task B exploits connections with the ATO, odometry board, EB and ETCS power control systems to assess functional safety. Task B cyclically checks the EB and ETCS systems. The digital input from the EB indicates the braking system availability, while the signal from the ETCS system returns information about its insertion/isolation (*Cyclic Monitor* - Fig. 2). Task B periodically receives and elaborates tachometer sensors data from the odometer board [13], to estimate train speed and position. When the odometer board sends usable information, Task B can extract the train speed, the standstill condition and perform safety supervision of the speed profile. In presence of not usable data and isolated ETCS Task B sets a braking flag [6], recognizing a hazardous situation.

Another main function of Task B concerns the answers

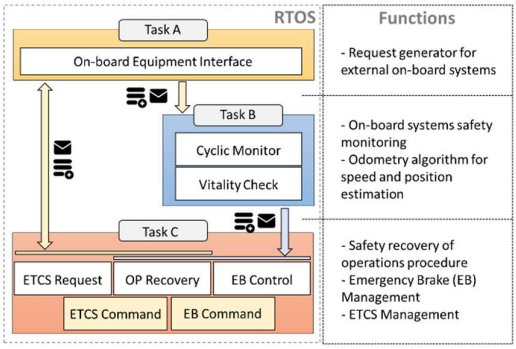

Fig. 2. Tasks organization of VC module application logic

checking for the requests generated via Task A. Specifically, the *Vitality Check* routine of Task B considers only the responses concerning the ATO Vitality, Operator Vigilance, and EB Release Confirmation requests. Task B acts as a watchdog on ATO, by analyzing the ATO responses provided within a time limit. Task B rises the braking flag if the active operator vigilance is not confirmed when the remote operator requires emergency braking, and when ATO reaches unsafe working states (e.g., failure mode).

Task C manages procedures that activate/deactivate on-board ETCS and the EB system. First, Task C monitors the remote operator's answers. If a request for toggling the ETCS status occurs, Task C activates, manages, and verifies the isolation/insertion procedures (*ETCS Request* routine and *ETCS Command* routines in Fig. 2) by driving a radio relay. Next, Task C employs data provided by Task B to check the radio relay status and verify the command actuation.

Task C continuously monitors the braking flags, intervening by powering off the EB system. This process leads to the total block of the traction and the train deceleration (*EB Command* in Fig. 2). After EB activation, Task C monitors the train speed, waiting for the standstill condition. Upon reaching the standstill condition, Task C starts the recovery procedure, if safe conditions are verified (*OP Recovery*). This procedure is necessary to guarantee safe traction after an emergency brake event.

IV. Experimental Results

A. Experimental Setup

To validate the proposed VC module in real-life scenarios, a testbed that includes the VC board in a test loop has been realized. The testbed includes different modules that emulate the behavior of the ATO on-board and trackside (i.e., remote operator decisions), odometer board, and Train Interface. Fig. 3 shows a snapshot of the hardware testbench.

According to Fig. 3, the VC module connects a backplane via SPI, CAN, digital I/O (DI/O), and Gbe. The backplane distributes signals to the target emulators. Specifically, the Gbe connects the VC module with the Host PC, which emulates the ATO on-board. SPI and CAN interfaces are connected to a MiniZed by Avnet. The MiniZed is programmed to stream previously defined scenarios (realized via Simulink Test Harness), synchronizing (via USB connection) the operations with the Host PC that manages the overall testbed. The MiniZed is used to emulate the BTM and the odometer board functions.

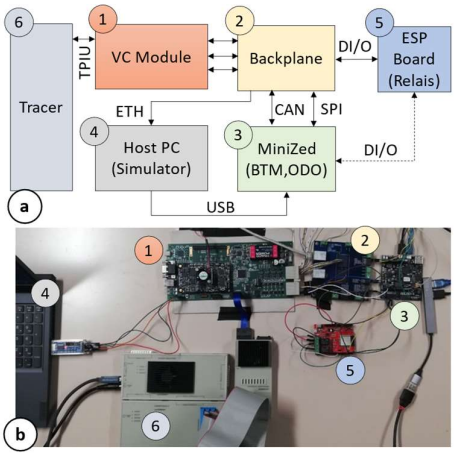

Fig. 3. Real-life Scenarios Testbed for VC module. (a) Architecture representation; (b) Testbench implementation.

The VC module also interfaces, via DI/O an ESP board, which embeds two relays to emulate EB and ETCS systems. This last board is synchronized with the MiniZed, to manage the consequences of braking operations that lead to a speed reduction readable via a dedicated odometer function. Intervention timing of the VC module has been extracted by connecting a commercial tracing tool Lauterbach PowerTrace to the TPIU interface.

B. Selected Hazardous Scenarios

VC system has been tested across 36 real-life scenarios derived from the system specification. These scenarios are representative of logic paths triggered by normal system operation and in presence of external equipment faults. Overall, 23 scenarios out of 36 lead to hazardous situations requiring VC mitigation actions. In 5 cases, the VC intervenes by issuing the EB system, allowing potential safe recovery of operations after the braking, while in 10 cases operations recovery is considered unsafe. In this latter case, the system passes in a state known as *System Decay*. This state is also reached by 8 scenarios, occurring with the train already in a standstill position (no EB intervention is needed).

To provide a complete overview of the VC module intervention capabilities, 6/23 scenarios are selected and presented: the best and the worst scenario of each above-analyzed category is reported in Fig. 4 and briefly described in the following.

According to Fig. 4, *Scenario A* concerns a direct request for emergency braking by the remote operator (via ATO).

Scenario B considers a train speed profile supervised by the odometer algorithm of the VC module with ETCS isolated. In this case, the VC module permits the train traction within a speed limit of 30 km/h. If train speed exceeds the limit, the system intervenes by commanding the EB. Scenarios A and B present safely reversible procedures that allow EB rearm.

During *Scenario C* and *Scenario D*, VC performs an emergency braking followed by the System Decay because it detects ATO on-board failure operating mode and does not receive active vigilance by the remote operator within the time limit, respectively.

The following two scenarios conclude with System Decay with the train already in a standstill position (no emergency braking is needed). During *Scenario E, the* VC module cannot toggle the isolation/insertion of ETCS after the command.

Scenario F analyzes the operator's response to a request concerning the EB rearm confirmation.

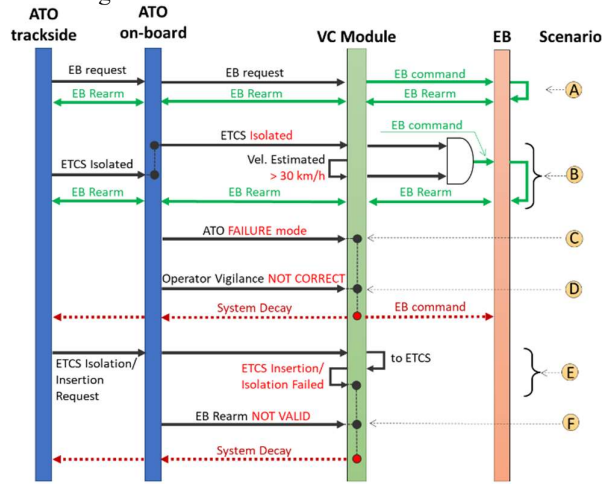

Fig. 4. Hazardous scenarios intended to lead VC module in EB and/or Decay status.

If a response is received, but it is not compliant with the standard message composition (not valid message), a System Decay condition is reached.

C. VC Module Intervention Times

To provide an overview of the VC module intervention time, it should be specified that according to the current ERTMS/ETCS performance requirements [14], the shortest intervention time required to issue an emergency brake, when a hazardous event occurs, is 1 s (most stringent case). Thus, to be concurrent, VC architecture must intervene in a period shorter than this limit.

It should be also considered that, in railway application, a standard pneumatic plates system for emergency braking, can typically depressurize the pipe (actuate the braking) in a maximum of 450 ms, leaving 550 ms for the ATP intervention. In this respect, Fig. 5 shows the architecture intervention times for those scenarios analyzed in Sec. IV.B. Specifically, Fig. 5.a shows the intervention time as the sum of the maximum delay in receiving the response (Data Exchange Time), VC module elaboration time and the time needed to depressurize the pipe (ATO-EB Intervention Time). Fig. 5.b expands the data exchange and elaboration time, regardless the EB intervention.

Considering scenarios that involve EB intervention, in the worst case (i.e., *Scenario A*), the whole intervention chain requires 540 ms to be completed (80 + 10 + 450 ms). In this case, the VC module intervenes 1.85 times faster than ETCS constraints. The best case involving an EB command (*Scenario D*) needs 452 ms. The last two scenarios (i.e., E and F) do not consider EB intervention because of System Decaying with the train already in a standstill position. The proposed ATP recognition and intervention time is, in these cases, largely below 50 ms.

V. Conclusions

New research trends in the railway sector are pushing toward fully automated infrastructure. Current solutions exploit supervision control systems based on existing ATP modules, such as the ERTMS/ETCS. However, the integration of ATO frameworks with GoA3/4 is still under investigation and additional ATP functionalities should be introduced.

In this paper, the design and implementation of a novel on-board VC module to supervise the unattended train operation have been proposed. The VC module, realized in the context of the collaboration between Politecnico di Bari and Rete Ferroviaria Italiana, expands the existing ATP functions of ETCS, permitting the continuous assessment of the on-board equipment working status, the identification of potential hazards, and the secure autonomous navigation of the train also in lines not served by ETCS or with faulty ETCS. VC module hardware consists of a Eurocard PCB, which is a first-of-a-kind compact solution capable to instantiate several communication interfaces with pre-existing in-cabin equipment, minimizing the integration impact with ETCS and national signalling system. The VC module stack software embeds a reliable and safe hard RTOS that schedules the application logic for vital control. This layer, developed as a model with Simulink/Stateflow tool, has been implemented on the Xilinx Ultrascale+ core of the PCB.

Experimental tests evaluated the VC module intervention timing in real-life scenarios. In this context, considering the worst case, tests showed that the VC architecture can issue the emergency brakes in 540 ms solving hazardous situations.

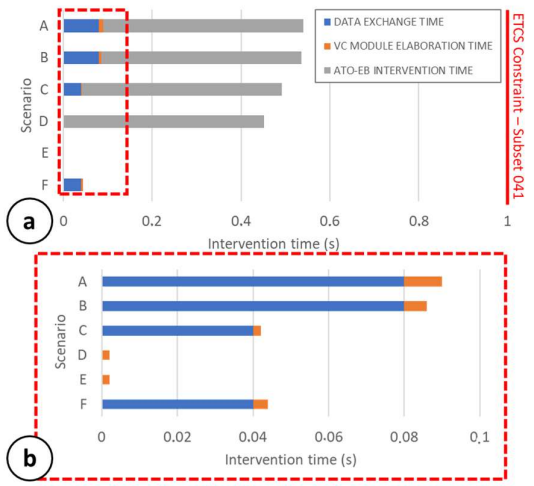

Fig. 5. VC module intervention times assessed on the selected scenarios.

This intervention time is largely below the related standard specification constraints (i.e., 1).

Another important advantage of the VC module lies in its possible use for the remote recovery of trains stopped on routes, because of ETCS system malfunctions.

Acknowledgment

This work has been realized in the frame of the ATO Project by Rete Ferroviaria Italiana S.p.A.

References

[1] Wang, Ziyulong, et al. "Assessment of architectures for Automatic Train Operation driving functions." Journal of Rail Transport Planning & Management 24 (2022): 100352.

[2] Eschbach, R. Formalizing and Analyzing System Requirements of Automatic Train Operation over ETCS Using Event-B. In: International Conference on Rigorous State-Based Methods. Springer, Cham, 2021. p. 137-142.

[3] Subset-026. ERTMS/ETCS System Requirements Specifications.

[4] Shift2Rail Project. Online available: https://projects.shift2rail.org/s2r_ip_TD_r.aspx?ip=2&td=b47388a9-b1f8-4ed8-9872-bb7708f7c08d

[5] ERTMS/ETCS - RAMS Requirements Specification

[6] S. Hayat, "Modeling of new driver assistance system for dysfunction of the signaling system ERTMS/ETCS," Proceedings of 2013 International Conference on Industrial Engineering and Systems Management (IESM), 2013, pp. 1-7.

[7] CEI EN 50124- Railway Applications - Insulation Coordination

[8] Mezzina, G., Barbareschi, M., De Simone, S., Di Benedetto, A., Narracci, G., Saragaglia, C.L., Serra, D., De Venuto, D. (2022). Applications in Electronics Pervading Industry, Environment and Society. ApplePies 2021. Lecture Notes in Electrical Engineering, vol 866. Springer, Cham. doi: 10.1007/978-3-030-95498-7_445.

[9] EN 50155 Railway applications, Rolling stock, Electronic equipment

[10] Donnarumma, Ciro, et al. "EN-50128 certification-oriented design of a safety-critical hard real-time kernel." 2019 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW). IEEE, 2019.

[11] De Venuto, D.; Mezzina, G. Spatio-Temporal Optimization of Perishable Goods' Shelf Life by a Pro-Active WSN-Based Architecture. Sensors 2018, 18, 2126. https://doi.org/10.3390/s18072126

[12] D. De Venuto, V. F. Annese, G. Mezzina, M. Ruta and E. Di Sciascio, "Brain-computer interface using P300: a gaming approach for neurocognitive impairment diagnosis," 2016 IEEE International High Level Design Validation and Test Workshop (HLDVT), Santa Cruz, CA, USA, 2016, pp. 93-99, doi: 10.1109/HLDVT.2016.7748261.

[13] M. Blagojevic, M. Kayal, M. Gervais and D. De Venuto, "SOI Hall-Sensor Front End for Energy Measurement," in IEEE Sensors Journal, vol. 6, no. 4, pp. 1016-1021, Aug. 2006, doi: 10.1109/JSEN.2006.877996.

[14] Subset 041 - UNISIG. Performance Requirements for Interoperability.