Safe Maintenance of Railways using COTS Mobile Devices: The Remote Worker Dashboard

TOMMASO ZOPPI, Dept. of Mathematics and Informatics, University of Florence, Florence, Italy
INNOCENZO MUNGIELLO, R&D Department of Rete Ferroviaria Italiana - RFI, Afragola (Naples), Italy
ANDREA CECCARELLI, Dept. of Mathematics and Informatics, University of Florence, Florence, Italy
ALBERTO CIRILLO, R&D Department of Rete Ferroviaria Italiana - RFI, Afragola (Naples), Italy
LORENZO SARTI, Dept. of Mathematics and Informatics, University of Florence, Florence, Italy
LORENZO ESPOSITO, R&D Department of Rete Ferroviaria Italiana - RFI, Afragola (Naples), Italy
GIUSEPPE SCAGLIONE and SERGIO REPETTO, R&D Department of Rete Ferroviaria Italiana - RFI, Osmannoro (Florence), Italy
ANDREA BONDAVALLI, Dept. of Mathematics and Informatics, University of Florence, Florence, Italy

The railway domain is regulated by rigorous safety standards to ensure that specific safety goals are met. Often, safety-critical systems rely on custom hardware-software components that are built from scratch to achieve specific functional and non-functional requirements. Instead, the (partial) usage of Commercial Off-The-Shelf (COTS) components is very attractive as it potentially allows reducing cost and time to market. Unfortunately, COTS components do not individually offer enough guarantees in terms of safety and security to be used in critical systems as they are. In such a context, *RFI* (Rete Ferroviaria Italiana), a major player in Europe for railway infrastructure management, aims at equipping track-side workers with COTS devices to remotely and safely interact with the existing interlocking system, drastically improving the performance of maintenance operations. This paper describes the first effort to update existing (embedded) railway systems to a more recent cyber-physical system paradigm. Our Remote Worker Dashboard (RWD) pairs the existing safe interlocking machinery alongside COTS mobile components, making cyber and physical components cooperate to provide the user with responsive, safe, and secure service. Specifically, the RWD is a SIL4 cyber-physical system to support maintenance of actuators and railways in which COTS mobile devices are safely used by track-side workers. The concept, development, implementation, verification, and validation activities to build the RWD were carried out in compliance with the applicable CENELEC standards required by certification bodies to declare compliance with specific guidelines.

CCS Concepts: • **Computer systems organization** → **Embedded and cyber-physical systems**; *Dependable and fault-tolerant systems and networks* • **Security and privacy** → *Systems security*;

Additional Key Words and Phrases: Safety, security, SIL4, railway, CPS, track-side maintenance, mobile devices, CENELEC, COTS

This work has been funded by RFI - Rete Ferroviaria Italiana S.p.A.

Authors' addresses: T. Zoppi, A. Ceccarelli, L. Sarti, and A. Bondavalli, Dept. of Mathematics and Informatics, University of Florence, Viale Morgagni 65, 50134 Florence, Italy; emails: {tommaso.zoppi, andrea.ceccarelli, lorenzo.sarti, bondavalli}@unifi.it; I. Mungiello, A. Cirillo, and L. Esposito, R&D Department of Rete Ferroviaria Italiana – RFI, Via Arena 1, 80021 Afragola (Naples), Italy; emails: {i.mungiello, a.cirillo, lo.esposito}@rfi.it; G. Scaglione and S. Repetto, R&D Department of Rete Ferroviaria Italiana – RFI, Osmannoro, Via Curzio Malaparte 50145, Florence, Italy; emails: {g.scaglione, se.repetto}@rfi.it.

2378-962X/2023/10-ART25
https://doi.org/10.1145/3607193

ACM Reference format:
Tommaso Zoppi, Innocenzo Mungiello, Andrea Ceccarelli, Alberto Cirillo, Lorenzo Sarti, Lorenzo Esposito, Giuseppe Scaglione, Sergio Repetto, and Andrea Bondavalli. 2023. Safe Maintenance of Railways using COTS Mobile Devices: The Remote Worker Dashboard. *ACM Trans. Cyber-Phys. Syst.* 7, 4, Article 25 (October 2023), 20 pages.
https://doi.org/10.1145/3607193

1 INTRODUCTION

Critical systems, whose (mis) behavior may lead to fatalities, severe injuries, or major damage to the environment, must adhere to appropriate guidelines to ensure that specific non-functional requirements are met [1, 22, 25]. In particular, their design and realization must provide safety [1], *avoiding catastrophic consequences on the user(s) and the environment*, thus being able to mitigate, manage, and isolate potential failures. Several domains have strong and straightforward safety implications, such as avionics, automotive, and railways. In these domains, components and systems are typically associated to a ***Safety Integrity Level*** (**SIL** [2, 7]), which identifies both qualitative and quantitative classes for the safety of the target component or system. In addition, attackers may craft and conduct malicious activities to harm those systems and generate cascading (safety) issues. Examples include, but are not limited to, hijacking autonomous vehicles to remotely control braking [36], the infection of the Deutsche Bahn systems by the WannaCry virus [38], and the multiple security issues in avionics that have been reported in surveys [37]. Consequently, safety-critical systems also have to deal with *security* [26, 45, 46], as they are required to guarantee *availability for authorized actions only, confidentiality, and integrity* [1].

The railway domain is based on embedded hardware-software systems that were built decades ago, and that are being maintained and updated along the evolution of the applicable standards as the ***European Rail Traffic Management System/European Train Control System*** (**ERTMS/ECTS**, [24, 27]). Indeed, recent technologies offer many additional opportunities to improve control systems by remotely providing critical functionalities in a completely safe manner. Unfortunately, railway control systems are not generally willingly updated due to (i) the reluctance of authorities and (ii) the cost and effort to design, develop, implement, verify, and validate a system that must comply with CENELEC [3, 7, 8] standards and has to be approved by a certification body before installation and operation. Moreover, **Commercial Off-The-Shelf (COTS)** components that may meet specific needs at a cheaper price are usually designed without safety in mind, and therefore cannot be employed as they are. As a result, control systems in the railway domain work properly and are maintained efficiently, but do not fully exploit novel technologies**.**

RFI **(Rete Ferroviaria Italiana)**, the company which manages railway infrastructure in Italy, has undergone a process to renew the current procedure to maintain rails, connected devices, and actuators. Maintenance activities are currently planned and coordinated via a ***Worker Dashboard*** **(WD)**, which is located in the central offices of train stations and requires track-side workers to physically move there whenever they initiate and conclude each maintenance action. The WD shows the state of actuators (e.g., railway switches) and other devices in the station as a *synoptic* diagram, often referred to as *mimic panel.* After physical access to the WD, track-side workers phone the control room operators through a dedicated and protected phone line for any information which is not available on such synoptic. Moreover, to block transit of trains in the track segment or actuator to be maintained, the workers may need to move to a separate – albeit close to the WD – room which contains the key cabinet. This cabinet contains switch-lock keys for each area or actuator in the station, which have to be removed by track-side workers before starting operations and re-inserted only when concluding maintenance.

To improve and optimize such operations, *RFI* is promoting the usage of COTS tablets and smartphones to (i) eliminate the need to physically access the WD and the key cabinet to acquire the physical token, (ii) provide remote access to the synoptic of the station to the track-side worker, and (iii) reduce the need of phone calls with the control room operator. It is worth mentioning that such an update will dramatically improve the efficiency of maintenance operations, minimize train delays and reduce workers' movements – which indeed have to be tracked [34] - between the train station and railways, with positive impact on the personal safety of the workers themselves.

To the best of our knowledge, this paper describes the first ongoing work that aims at updating existing (embedded) railway systems to a more recent cyber-physical system paradigm by using non-customized COTS components. The contribution of the paper mostly revolves around bringing mechanisms that are state-of-the-art for researchers into a real cyber-physical system that has critical safety requirements. In fact, companies are usually reluctant to upgrade their critical systems, because even a small update may require massive time and money investment for conceptualizing, implementing, and producing all the necessary documentation for certifying the system before deployment in its final environment.

As such, we introduce a SIL4 **Remote Worker Dashboard (RWD)** to support maintenance of railways, which connects and orchestrates physical components to provide the track-side worker with responsive, safe, and secure services, with clear economic benefits in the medium-long term period. According to the CENELEC EN50126 [7] lifecycle, we describe Concept, System Definition, Hazard and Risk Analysis, System Architecture, and some details on implementation and V&V activities, focusing on mechanisms to guarantee safety and/or security. We also explain how COTS mobile devices can be safely used in the RWD without customization, as it is instead common practice in other railway systems [28, 29], providing additional relevance and novelty of the concept and design of the RWD.

The paper is organized as follows: related works and applicable standards are presented in Section 2, while an overview of railway maintenance and the current procedures is described in Section 3. Section 4 provides details about the system concept and architecture, Section 5 presents the safety and security mechanism developed for the RWD system, while Section 6 elaborates on the updated maintenance procedure. Section 7 elaborates on relevant Verification and Validation activities, letting Section 8 to finally conclude the paper.

2 APPLICABLE STANDARDS AND RELATED WORKS

2.1 Safety Integrity Level

The CENELEC standards represent landmarks for the development of programmable electronics in the field of railway applications in Europe. Particularly, EN 50126 [7], EN 50128 [8], EN 50129 [21], and EN 50159 [3] specialize the general-purpose IEC61508 [2] for the railway domain: compliance with those standards guarantees a safe development of hardware-software systems for the railway domain. The likelihood that a system satisfactorily performs the required safety functions is typically called *safety integrity level* [2, 7]. When a product is developed using methods, tools, and techniques appropriate to a specific safety integrity, it is possible to claim that the product is a *Safety Integrity Level* "X" product [7]. In the railway domain [21], SILs range from SIL0 (no safety constraints exist), to SIL4, which is quantified as a probability of catastrophic failure lower than 10^{-9} per hour and is the reference level for most railway systems.

2.2 COTS Components and Safety-Critical Systems

Companies, researchers, and practitioners usually aim at reducing time-to-market and costs related to the development of the whole system. This may be achieved by adopting COTS hardware and software components [22, 23, 25] that interact with custom safety-critical applications, operating systems, or hardware to provide the desired functionalities. However, COTS hardware, boards, and components do not usually accomplish safety requirements and do not embed diagnosis strategies [17, 18] to timely identify unsafe states. Consequently, researchers and practitioners proposed multiple approaches based on wrappers [16], redundant hardware [15, 19], or diverse software [30], which can adequately manage COTS components in safety-critical systems.

2.3 Safety of Track-Side Workers

The safety of track-side workers is obviously one of the main concerns [46, 50, 52, 53] when planning maintenance activities in railways. However, "[…] the continuing requirement for people to go on to the track to place and remove red lamps and explosive detonators, as part of the arrangements for protecting engineering work on the railway", is an issue that the UK Rail Accident Investigation Branch – among others – acknowledges since decades [48].

Consequently, different strategies were proposed throughout the years and in different countries to provide a safe environment for track-side workers that can be quickly set up and disassembled once maintenance is over. Most solutions rely on proposing ad-hoc wearable devices [28, 47, 49] which went through rigorous risk assessment [51] processes before production. Each worker is equipped with a device that rings or shakes to alert the worker whenever a train is expected to pass by the area under maintenance. Noticeably, those systems need components installed in neighboring areas that observe railways through radars, lidars, GPS, webcams, and oscillometers to eventually trigger wearable devices. Wrapping up, wearable devices can enhance safety of track-side workers, but still require ad-hoc devices and the setup of train detectors in areas neighboring the maintenance site, which still require time and effort to be installed. Differently, [54] proposes the adoption of high-visibility clothing that allows workers to be visible to automatic object detectors even with scarce or adverse lighting conditions. Such an approach proves to be effective in building sites or docks, but it is not effective in railways as a train at cruising speed most likely will end up hitting the track-side worker due to the very long time it needs to stop.

Despite the relevant body of research, to the best of our knowledge, no SIL4 railway system realizes part of its safety functions through COTS smartphones and tablets. Mobile devices are often used in the railway domain, but always require ad-hoc development of safety-critical software and a rugged architecture [28, 29]. Differently, this paper presents a new step for the research and innovation in the railway domain as it presents a SIL4 system that safely orchestrates unsafe COTS components, without requiring any customization.

3 RAILWAY MAINTENANCE

Track-side workers have multiple responsibilities and have to fulfill different tasks to support the correct provision of railway services. Most of their work is carried out inside the stations, where the majority of physical actuators and almost all the software of railway ground systems (e.g., railway switches, semaphores, and crossings) are located. Workers may need to request several authorizations to block trains passing by the areas under maintenance [14]. This section describes the main actors involved in the maintenance of railways and the current procedure to conduct common maintenance operations.

3.1 Maintenance of Railways

Italian railways are managed by **RFI (Rete Ferroviaria Italiana)**, which administers and maintains approximately 2,200 stations and a total of 16,723 km (10,391 mi) of active lines, 45% of which

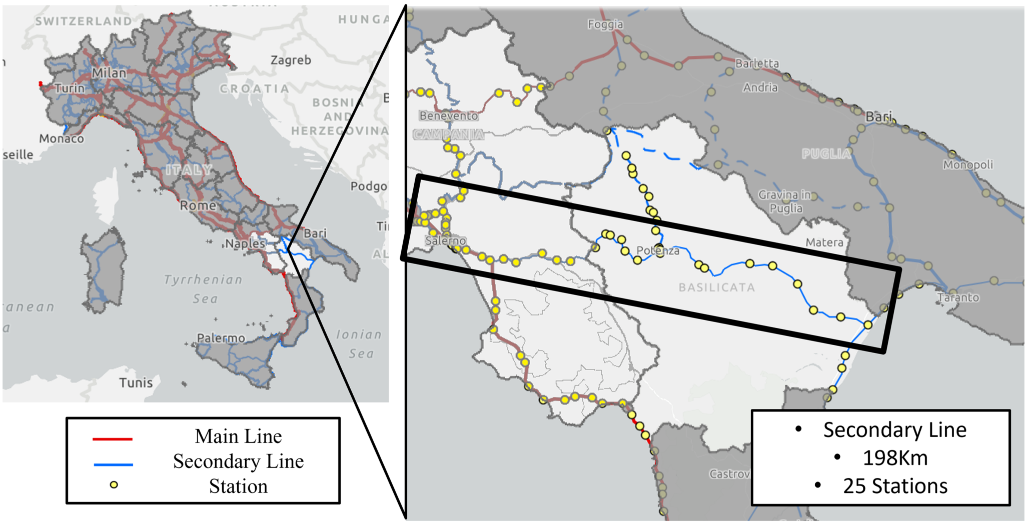


Fig. 1. Diagram of tracks, railways, and stations in Italy, highlighting a secondary line [44].

have double railway tracks [44]. The left of Figure 1 shows the current topology of the railway network, and allows identifying (i) stations, (ii) main lines, which have high traffic and good infrastructure quality, and (iii) secondary lines, which have less traffic and are responsible for connecting medium or small regional centers.

Maintaining such safety-critical and cyber-physical infrastructure poses mechanical and electrical challenges, but also has to guarantee the personal safety of track-side workers, customers, and personnel on trains, trying to minimize delays due to maintenance operations. For instance, the schedule of planned maintenance operations for a secondary line of approximately 200 km in length (e.g., see right of Figure 1, length of 198 Km), or rather the 1.18% of the overall extension of Italian railways [44], usually allocates between 450 and 500 operations per month. In one month of 2020, the following maintenance operations were planned, implemented, and decommissioned on a line similar to (the exact line cannot be revealed due to non-disclosure constraints) the one in Figure 1:

- Replacement (73/477, 15.3%), which aims at substituting, upgrading, or partially replacing components that may be degrading or too old.
- Periodic Inspection (134/477, 28.1%), which is planned periodically and aims at manually inspecting actuators or railways to identify potential mechanical or electronic issues.
- Reconditioning (65/477, 13.6%), or rather maintenance actions directed to restore a component to its original state without replacing.
- Generic Maintenance (92/477, 19.3%) and Generic Action (113/477, 23.7%) where no further details were provided by the infrastructure manager RFI.

All these 477 maintenance operations (i.e., 15.4 scheduled operations as daily average) require disconnecting one or more actuators or physical components from the railway network, temporarily preventing the transit of trains to guarantee personal safety of track-side workers. Consequently, reducing maintenance time does not only improve the throughput of those operations, but also – and more importantly - reduces potential delays due to train re-routing.

It is worth mentioning that 67% of these operations were scheduled at night-time (i.e., between 11 pm and 6 am), where the railway network is usually subject to a very low to absent traffic. Such

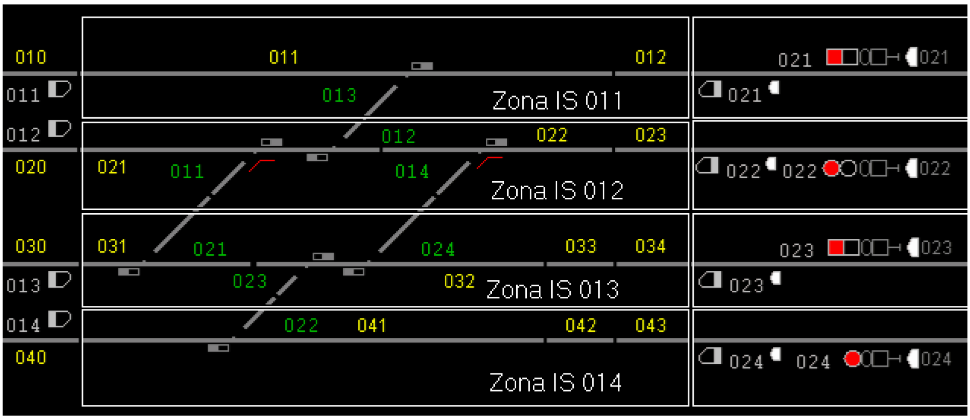


Fig. 2. Synoptic including rails, their interconnections, and several actuators and physical components.

policy allows conducting maintenance without impacting at all on train schedules. Additionally, *periodic inspections* and many *generic maintenance* operations are entirely carried out by visual inspections, thus requiring minimal maintenance time. Regardless, there were approximately five daily maintenance operations to be carried out in such secondary line during high-peak traffic hours. Roughly, we can estimate around 600 maintenance operations to be carried out daily in high peak hours in the whole infrastructure of Italian railways, which clearly motivates the need for an adequate support to optimize those operations.

3.2 Railway Stations, Synoptic and Track-Side Workers

Railway stations are usually partitioned into areas representing track segments, connected components, and actuators [14]. The state of those areas is usually depicted as a *synoptic* or mimic panel (see Figure 2), which reports on rails and components, labeled with numbers that are painted with different colors depending on their state. When an area, or an actuator, is under maintenance, its state is considered excluded, which is translated to temporarily disconnect a specific component from the railway network. Note that each area (e.g., “Zona IS” in Figure 2) is independent from the others: as a result, different actions can be simultaneously performed in two different neighbouring areas. For example, the area “Zona IS 011” in the figure may be excluded, while the neighbouring “Zona IS 012” may allow transit of trains.

Maintenance activities may be either planned or immediate, whenever facing unexpected issues. In both cases, as described in [14], track-side workers (simply *workers*, for brevity in the remainder of the paper) rely on the ***Worker Dashboard*** **(WD)**, which can be accessed only from the station *central office* with workers’ credentials. The WD enables workers to (i) observe the synoptic to check the state of actuators (e.g., rail switches can be “straight” or “diverging”), or (ii) see details about train routing. Moreover, they can also (iii) use the WD to send *commands,* which are usually directed to change the state of actuators to exclude areas and avoid train routing, allowing workers to safely reach specific areas of the station that need maintenance. For a detailed list of requirements of the Italian WD, please refer to the directive [20].

3.3 The Maintenance Procedure

Maintenance procedures in Italian stations follow a two-step process to authorize commands. First, the worker asks for a given command using the WD; then, the command is forwarded to the control room of the station where the station manager authorizes or denies it. If this authorization

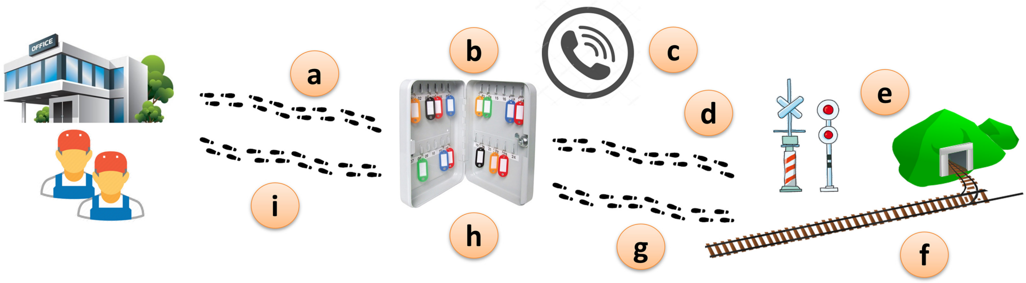


Fig. 3. Schema of the current maintenance procedure [14].

is granted, the worker may be asked to perform additional actions before starting maintenance. For example, whenever a worker has to exclude an area of the station, he/she is required to go to the WD, ask for the command, wait for the confirmation of the station manager, and, additionally, remove a switch-lock key corresponding to the area involved in maintenance from a key cabinet before starting operations.

As represented also in Figure 3, once the worker gets to the premise of the WD and the key cabinet (a), he has to authenticate to the local security personnel, then he has to turn the switch-lock key (b), call the station manager to confirm the maintenance operation (c), and turn the lock key again, removing it from the key cabinet (d). If the key corresponding to a given area is not in the key cabinet, such area is excluded from the railway network. At this stage, all the required authorizations have been granted and therefore workers can (e) reach the area under maintenance, and (f) perform the required actions. When the workers complete maintenance, they have to (g) go back to the key cabinet, (h) re-insert the key corresponding to the area and turn it on to match the initial position. This action re-connects the area to the network, completing maintenance and enabling trains to transit again in the area previously excluded. Finally, (i) workers can come back to the central office and are ready to handle further actions.

3.4 Limitations of the Current Maintenance Procedure

This procedure was adopted decades ago and still complies with the applicable railway standards, but there is room for innovation, mainly considering the following aspects:

- Access to the WD for simple operations such as viewing the synoptic requires the workers to physically move throughout the station between areas, actuators, and the central office every time.
- The central office may be physically far from the position of the workers and the maintenance site. This wastes workers time, since they have to move to get the required authorization.
- Time required for maintenance can be reduced, minimizing delays to train re-routing.

4 A REMOTE WORKER DASHBOARD

To tackle the issues above and update maintenance of railways, RFI and its academic partner defined a Remote Worker Dashboard (RWD) to be installed first in Italian stations and potentially applicable to other stations worldwide. This section summarizes the main items of our work regarding phases 1-4 of the CENELEC EN50126 [7] lifecycle, namely Concept, System Definition, Risk Analysis, and System Requirements. Those were cross-validated by a certification body that provided a SIL4-compliance certificate to CENELEC EN50126 lifecycle up to step 4 (included).

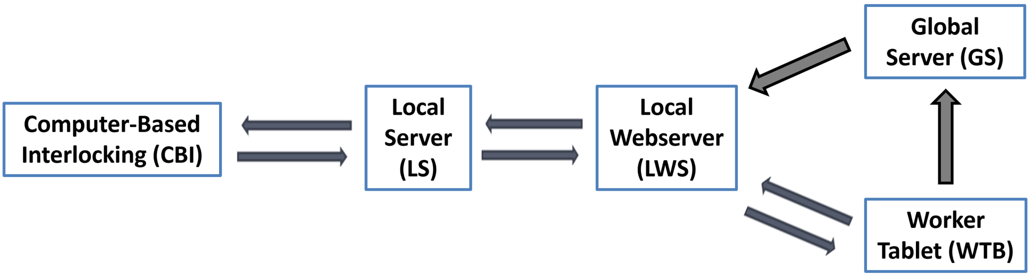


Fig. 4. Preliminary architecture of the RWD showing components and their inter-connections.

4.1 System Concept and Motivation

The RWD aims at updating the existing procedure and support systems by providing workers with a COTS tablet that displays the WD and allows a safe and secure interaction with the existing SIL4 interlocking systems when sending commands. RWD will allow workers to perform their daily operations without the necessity to physically go to the central office to ask for and execute commands. The RWD has analogous functionalities of the WD and can remotely interact with the existing interlocking machinery. Consequently, the RWD system as a whole has to conform to SIL4 [7] requirements. Since some of the components and communications are carried out in an uncontrolled and potentially hostile environment, security threats shall be accounted, as they may have severe impact on safety properties. In other words, the RWD system has to be safe, and its safety integrity should not be affected by possible security breaches or exploits of vulnerabilities.

4.2 System Definition

Functional requirements that guide a precise definition of the system overlap with the requirements of the already existing WD [20]. At this phase, the CENELEC lifecycle requires devising a preliminary system architecture that (i) serves as a baseline for the hazard analysis, and (ii) will be updated to include mitigations to identified hazards to constitute the final system architecture.

Overall, our preliminary architecture specification of the RWD ended up identifying five components, namely WTB, GS, LWS, LS, and CBI, which are depicted in Figure 4. The worker primarily relies on a tablet (Worker Tablet, WTB), which they use to gather information such as the synoptic and to send commands to the **Computer-based Interlocking (CBI)**. To such extent, we employ a webserver **(Local Webserver LWS)** specific for each station that exposes a web app to be accessed from the WTB through browsing. The worker can connect to the specific LWS through a Global Server GS which works as a single and unified access point and re-routes the worker to the LWS installed in the specific station they work in. Each LWS will execute commands asked by workers through WTB; therefore, it will safely communicate with the existing SIL4 CBI. Interfacing LWS and CBI is quite complex: therefore, we plan a **Local Server (LS)**, disconnected from the Internet but able to bridge the connection between CBI and LWS and provide additional control routines or support tasks e.g., check preconditions before applying commands.

4.3 Hazard and Risk Analysis

Hazard Analysis Techniques. The preliminary architecture specification allows conducting a ***preliminary hazard analysis*** **(PHA)** to identify and analyze *hazards* due to component failures, human mistakes, or attackers willing to damage the system, leading either to availability or safety issues. There are many different techniques for identifying criticalities and operability problems, ranging from *Checklists*, ***Fault Modes and Effects Analysis*** **(FMEA)** [6], ***Hazard and***

Operability study **(HAZOP)** [5, 51] and ***Fault Tree Analysis*** **(FTA)**. All these methods output a hazard log, or rather a list of potential threats to the system.

Likelihood, Severity, and Risk. Regardless of the domain of interest, each item of the hazard log needs to be assigned to qualitative levels of *likelihood* and *severity* that help build the *risk* function. The standard CENELEC EN50126 [7] lists severities from best to worst as *Insignificant, Marginal, Critical*, and *Catastrophic*, to be combined with *Frequent, Probable, Occasional, Rare, Improbable*, and *Highly Improbable* likelihoods. Each possible couple of <severity, likelihood> is assigned in the standard [7] to a risk, which may be *Negligible, Tolerable, Undesirable*, or *Intolerable*. The resulting risk for each hazard drives the need to identify a mitigation that may (slightly) modify the system architecture and usually aim either at decreasing likelihood or at reducing severity to lower risk associated to hazards. As a result, the identification of mitigations to hazards contributes to building the final system architecture. At this stage, the PHA has to be updated to match the final system architecture, building the final **Hazard Analysis (HA)**.

Hazard Analysis of the RWD. The industrial partner and the consultant set up hazard meetings to identify potential threats to the system through brainstorming, checklists, and more importantly by systematically applying the HAZOP [5] methodology. For each critical function of the RWD system, e.g., “worker requests a command”, the HAZOP methodology demands applying the following keywords:

- *Not*, or rather: what happens if the function is NOT executed?
- *More/Less:* what happens if the function is repeated MORE/LESS times than expected*?*
- *Part Of:* what happens if the function is only partially executed?
- *Early/Late:* what happens if the function is executed EARLIER/LATER than expected?
- *Other Than*, which points to execution of the function by means OTHER THAN expected, or with specific environmental conditions, that do not cover other options above.

As a result, potential hazards are identified in a structured way. In addition, we devise the root cause and consequences of each hazard, as well as likelihood, impact, and risk according to the categories above, and an explanation about why the residual risk is acceptable, or mitigations to be applied to make the risk tolerable.

Table 1 shows an extract of the Hazard and Risk Analysis of the RWD system.[1] The table reports five hazards related to different functionalities: H1–H4 were extracted from the PHA, while H5 only appears in the final HA as it involves a component that was added to mitigate threats in the PHA. From the top of the table, in column “hazard”, a potential threat H1 could lie in dropped message due to a malfunction of the channel or the LTE network. The impact of this hazard may be catastrophic if the message that is dropped carries critical information such as “area cannot be freed due to trains expected to pass by”. As mitigation, communication should be protected through a safe protocol (SSL/TLS itself is not enough) regulated by CENELEC EN50159 [3] that – amongst other characteristics – does not fail silent if a message is lost. Similarly, we have to be aware that WTB is a COTS tablet that is not built according to safety requirements. Therefore, the same message may be sent more than once (line H2 in Table 1) to LWS due to problems or congestion in the network adapter of WTB. This may also have catastrophic consequences if the duplicated message is an old synoptic that was previously cached, which shows an area as excluded, i.e., disconnected and safe to go for the worker, despite it being connected and ready for train routing. Here the adoption of a safe protocol is not enough even in the case of an EN50159-compliant [3]

[1] Note that mitigations to specific threats cannot be shared entirely due to non-disclosure agreements and to protect the Intellectual Property of the industrial partner (and funder) of this project.

Table 1. Items of the (Preliminary) Hazard and Risk Analysis of the RWD – HAZOP Methodology

#	Component(s)	Function	HAZOP Key	Hazard	Root Cause	Consequences	Likelihood	Impact	Risk	Mitigation
Preliminary Hazard Analysis										
H1	WTB, LWS	*Data exchange with LWS*	NOT/NO	Network packet/Message is dropped	*Channel Error*	A message is dropped. Possible loss of critical data or malfunctioning of procedure executed by the worker.	Probable	Catastrophic	*Intolerable*	Adoption of a Safe and Secure communication protocol, compliant to EN 50159 standard.
H2	WTB, LWS	*Data exchange with LWS*	MORE	Message is repeated	*Tablet Error*	Could be shown old and erroneous information (e.g., because of data caching) about critical commands (e.g., exclusion of an area).	Rare	Catastrophic	*Undesirable*	Duplicated information about commands (e.g., timestamp, actuator/component involved) must be shown in a replicated channel.
H3	WTB	*Command Request*	OTHER THAN	The worker selects a command, its execution get notified, but command actually not executed	*Malicious (Attack)*	Workers may take wrong decisions e.g., going to an area they think it is disconnected from the network, while it is not.	Probable	Catastrophic	*Intolerable*	Feedbacks about execution or failure of a command should be reported through two diverse and isolated channels.
H4	WTB	*Pressing Command Button on UI*	OTHER THAN	The worker presses the wrong button	*Worker Error*	The Worker input in the IMR System a command different from the one intended.	Occasional	Catastrophic	*Intolerable*	Each command needs additional confirmation by using also a replicated channel.
Final Hazard Analysis										
H5	WTB, WS	*Command Request*	OTHER THAN	The attacker compromises both personal devices of the worker at the same time	*Malicious (Attack)*	The attacker can act freely as a worker, asking for commands and confirming it through the both channels, with potentially catastrophic consequences.	Highly Improbable	Catastrophic	*Tolerable*	Not Needed: Tolerable risk.

protocol able to defend also against repetition attacks. Consequently, we figured out that we have to provide additional information to the worker (e.g., a timestamp to identify the "freshness" of the image) both on the WTB and on a replicated channel, which may be another device such as the personal smartphone of the worker. This mitigation would help also with the threat H3, which is caused by an attacker that installs malware on the tablet to change the content of the feedback message from LWS to harm the worker.

Similarly, it may happen that the touchscreen or the browser of the WTB do not function properly and send to the LWS the request of a command other than the one the worker wanted to execute. Also in this case, the usage of a replicated channel where LWS sends feedback by means of a device different from WTB reduces the likelihood of this hazard, which becomes "Highly Improbable" and results in a "Tolerable" risk.

Implementing Mitigations. The most frequent mitigations require all safety-critical information to be made redundant (e.g., relevant information in the synoptic will also appear as separate text in the webpages) for safety purposes, while a duplicated communication channel helps mitigating also security threats. To achieve these mitigations, we mimic an approach commonly used in online banking that requires the worker to insert in the WTB a **One-Time Password (OTP)** they get from a different device (the **Worker Smartphone WS**) to confirm the execution of a command or for other critical actions, e.g., Login. This provides coverage against failures (even malicious) of either WTB or WS devices: common mode failure/hacking still shows a Catastrophic impact in Table 1 (H5), but we consider the likelihood of this event to be Highly Improbable for this system, making the overall risk as Tolerable.

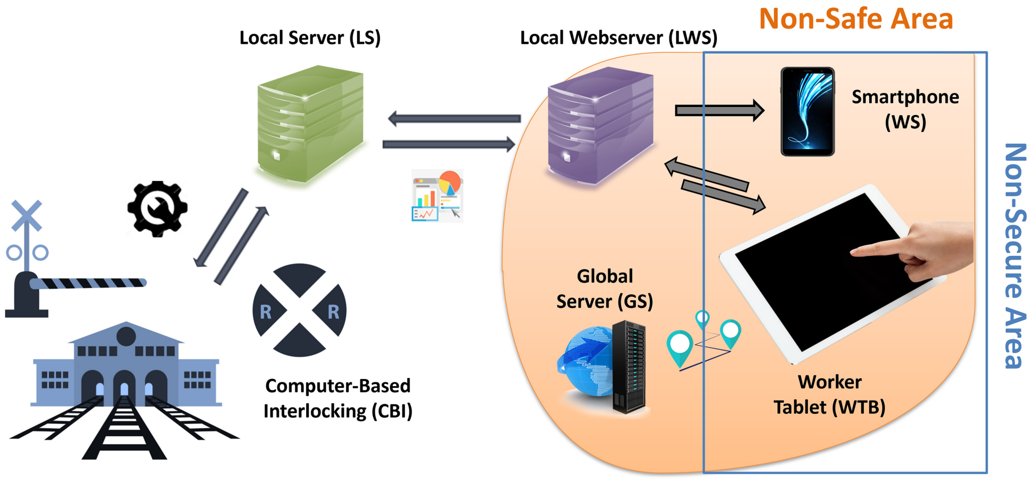


Fig. 5. Final architecture of the RWD. Components that lie in non-safe or non-secure areas do not have to comply with safety or security requirements.

4.4 System Architecture Specification

The mitigations identified during (P)HA allowed devising the final System Architecture that is reported in Figure 5. The left part of the picture depicts components (CBI, LS) that: (i) are located in a premise of the station whose access is severely controlled; (ii) are intrinsically safe as they are designed, developed, verified and validated as SIL4, and (iii) can rely on secured (wired) connections that shield them from network threats.

Instead, the right part of the picture represents devices and interconnections lying in a "non-safe area", where components are individually built without safety in mind. Therefore, they may independently fail, or may be subject to attacks, which may also impact communication channels. The non-safe region of Figure 5 embraces the global (web)server GS, the web server of the station (LWS), and two personal COTS devices available to the worker: a tablet (WTB) and a smartphone (WS). Indeed, GS and LWS are physically located in the station's premises and protected by a firewall to ensure security against network intrusions and therefore do not belong to the non-secure area.

Finally, it is worth pointing out that each worker is responsible of mobile devices WTB and WS and they have to immediately notify the IT department of the railway manager if either of the two devices is lost or unavailable. Insights on each of the six components of the RWD are provided below.

4.4.1 Computer-Based Interlocking (CBI). The Computer-Based Interlocking manages all the actuators such as railway switches, semaphores or level crossings in a semi-automatic way. It manages interlocking activities through SIL4 routines and control loops that periodically query all connected devices to check their state and (when possible) their health indicators. In the RWD system, the CBI can be accessed only by LS through a wired point-to-point channel that is managed through a safe [3] protocol.

4.4.2 Local Server(LS). LS is a SIL4 component running a Real-Time Embedded operating system with cyclic tasks. This is necessary to correctly interact with CBIs, which typically rely upon hard real-time OSs with cycles of either 350 or 500 milliseconds [40]. LS is in charge of: (i) managing workers' authentication (bridged by LWS); (ii) generating One Time Passwords through Pseudo-RNG with a periodical refresh of the seed and performing their verification; (iii) checking the applicability of the commands asked by workers and – if applicable - forward them to the CBI; and (iv) query the CBI to get the state of the physical devices to build the synoptic. Note that LS is not directly connected to the internet; instead, it has two separate point-to-point connections (see Figure 5) protected by a safe and secure protocol to interact with CBI and LWS.

4.4.3 Local Web Server (LWS). LWS runs a commercial (i.e., Apache) webserver which exposes the user interface of the RWD through webpages. Moreover, LWS acts as a proxy between LS and WTB and is in charge of (i) bridging requests and feedback of user commands requested by the worker to LS and (ii) assembling web pages with information provided by LS and the synoptic, so that they can be accessed by the worker through WTB. The LWS is physically located in the premises of the station and protected by rigorous access control and a firewall to ensure security against physical and cyber intrusions. Additionally, the communication between LWS and WTB happens by means of a safe and secure protocol [3].

4.4.4 Global Server (GS). GS stores all information (e.g., IP addresses), needed to re-route workers to specific LWS. Each station has its own LWS and WS; instead, the GS works as a unified entry point to the system that asks the worker for a first login and redirects them to the LWS of the station they are interested in. GS hosts a web server that workers can use for a username-password login which, if successful, enables the worker to be redirected to the LWS of a station and complete login. The GS lies in the “Secure Area” in Figure 5 as it has security requirements (i.e., login activities), but it is not considered an intrinsically safe component.

4.4.5 Worker Smartphone (WS). WS is a COTS smartphone that shows a textual message received through a wireless LTE network. Whenever needed, LWS sends SMSs that contain different information which include – but are not limited to – the name of the station, the requested command, a timestamp (details in Section 5.3.2).

4.4.6 Worker Tablet (WTB). WTB is a COTS tablet the worker uses to remotely access the RWD through mobile network. The worker uses this COTS tablet in conjunction with the WS to (i) first navigate to the GS to be redirected to the correct LWS; (ii) authenticate to the LWS of the station the worker has to operate, and (iii) perform the actions needed for authorization, start, and decommission of a specific maintenance procedure.

4.5 Interactions between Synchronous and Asynchronous Components

In a generic railway system, collisions between trains are avoided by never allowing more than one train to occupy a track segment at any time. Regardless of the specific protocol to avoid collisions, which is implemented in the CBI, those actions have strict hard-real-time requirements that need to be fulfilled alongside with other safety requirements. Consequently, the RWD should have at least a SIL4 component (the LS) equipped with a cyclic hard-real-time operating system. LS directly interacts with the CBI and with all the machinery required for compliance to the railway standards whenever needed. However, the WTB should be able to occupy a track segment asynchronously, when workers complete a maintenance request.

This exposes the RWD system to a potential design issue: while the LWS and WTB communicate through a client-server asynchronous paradigm, the LS, the CBI, and other railway actuators execute a cyclic and synchronous exchange of information and completion of tasks. As in Section 4.4.3, the LWS is in charge of bridging communications between LWS and LS, where only the latter is a cyclic synchronous system. Therefore, LWS implements a communication module that, every cycle:

- forwards to LS any request that was sent to LWS by WTB in the last cycle, if any;
- sends an “I am alive” default message to LS if no request was received from the WTB.

Table 2. Summary of Communications Happening in the RWD Systems, and Protocols they Rely Upon

Communication Channel	CENELEC 50159 Network Cat.	Physical Transmission Medium	Application-Level Protocol	Type	Purpose
CBI - LS	*Cat.1 Closed Transmission System*	Wired	PVS	Synch	Communications of the RWD with the interlocking railway system
LS - LWS	*Cat.1 Closed Transmission System*	Wired	Custom over PVS	Synch	Exchange of requests and data to build webpages
LWS - WTB	*Category 3 – Open Transmission System*	Wireless	Custom over HTTPS	Asynch	Exposing webpages to the tablet
WTB - GS	*Category 3 – Open Transmission System*	Wireless	HTTPS	Asynch	Managing authentication of the user and routing to the correct LWS
LWS - WS	*Category 3 – Open Transmission System*	Wireless	HTTPS	Asynch	Sending OTPs to the WS

LS reads data from the network interface with LWS once every cycle and reacts accordingly. When the request from WTB is completed, LS sends a feedback to LWS, which updates the webpage to be shown on the WTB. In case no information is received by LS for a few consecutive cycles, the LS flags the communication channel with LWS as malfunctioning, and stops accepting any request that may come from this channel until restoration. Importantly, the payload of requests from LWS to LS complies to an application-level-protocol that specifies, among others (i) the ID of the worker and the WTB, (ii) the code of the request, and (iii) additional information whenever needed. Any request that does not comply with this protocol specification is discarded before being processed: exposing a restricted set of requests provides yet another mechanism to guarantee that LS deals only with requests it is able to manage.

5 INSIGHTS ON SAFETY AND SECURITY MECHANISMS

COTS devices as WTB and WS are not customized, rugged, or run with limited privileges and therefore are affected by a multitude of threats. Consequently, interactions with other components of RWD need to be strictly regulated to avoid unsafe behaviours or potential security breaches will not propagate to the system. The rest of this section provides insights on specific mechanisms we devised to mitigate safety and security threats.

5.1 Communications between Components

Communications between components of the RWD should comply with different requirements: therefore, different communication protocols are required for different channels (see Table 2). LWS provides data to WS through a regular LTE network, and then is accessed on the WS by using a commercial messaging app. WTB and GS communicate via a regular HTTPS (SSL/TLS) protocol as no particular safety requirement involves the Global Server GS.

All the other communications between components of the RWD should instead be carried out through safe (and often secure) protocols [3]. Interactions between LS and LWS, as well as between LS and CBI, are managed through the Vital Standard Protocol (***Protocollo Vitale* Standard - PVS** [9]). PVS is a lightweight protocol that stems from the Subset-037 of ERTMS ETCS *Euroradio* FIS [11] and Subset-098 of *RBC-RBC Safe Communication Interface* [10]. It adopts techniques and algorithms that have been identified among those highly recommended in EN50159 [3]. As a consequence, *this protocol is becoming a de-facto standard for safety-related communications between cyber-physical components* in the Italian railways allowing interoperability of components produced by different manufacturers as Hitachi, Alstom and Bombardier. PVS [9] provides the *Session* and *Presentation* OSI layers over a TCP/IP transport stack and provides defences against CENELEC EN50159 [3] threats through mechanisms as *sequence number, safety codes* (extended CRC), *cryptography* (optional) through *AES* [12] and *AES-CMAC* [13], and a numerical counter that ensures "freshness" of the message called execution cycle.

Instead, communications between LWS and WTB are regulated by a custom protocol which provides safety by custom handshaking upon the standard HTTP with SSL/TLS commonly used for secured web communications. This custom protocol was deemed necessary since the PVS is meant to manage cyclic communications and does not adequately fit the client-server paradigm behind web-pages.

5.2 Safety Mechanisms

We list here safety mechanisms SaM1 to SaM6 that were employed to mitigate hazards alongside with measures to protect communications that we described in the previous section. Note that some of these mechanisms may also mitigate security threats.

5.2.1 SaM1 – Redundancy and Device Duplication (WTB and WS). Redundancy is a design pattern that is widely adopted when building safety-critical systems [41], even through diversity [42]. We apply redundancy by providing the worker with two personal COTS devices to execute commands, handling redundant information which may help to understand ongoing malfunctions. For example, a worker may see a command "exclusion of area 15" on a device, and "inclusion of area 15" on the other, detecting a malfunction and stopping operations.

5.2.2 SaM2 - Synchronization. After login, LS establishes a point-to-point connection with WTB through LWS. Then, we calculate and store the potential clock drift between LS and WTB to be used as offset when producing timestamps to be sent through web pages. This avoids misinterpretation of the "freshness" of the information (e.g., a synoptic) by the worker due to clock skew between LS and COTS devices, which may not rely on unified timings as NTP [43].

5.2.3 SaM3 – Static Webpages. Webpages generated by LWS using information received from the LS are designed to be defined server-side (PHP), easy to interpret and avoid client-side scripting (i.e., JavaScript) aside from showing current time, to minimize potential hazards due to running scripts on the potentially unsafe and insecure COTS tablets (WTB).

5.2.4 SaM4 – Generation of Images. LS gets the state of physical devices through CBI and builds the synoptic as a GIF/JPEG. Those images are then sent to LWS, which embeds them in the webpage with no further modifications. To mitigate some of the threats identified during HA, LS slightly modifies such image under specific circumstances by watermarking [31] heterogeneous information to be provided to the worker (details are not shared due to non-disclosure). Image generation is entirely performed by the SIL4 LS: therefore, the image is always generated safely, and its integrity is preserved thanks to the safe communications between LS, LWS, and WTB.

5.2.5 SaM5 – Command Filtering and Applicability Check. Once a worker selects a given area or actuator on the web app, the LS (through LWS) provides the worker with a list of applicable commands. Applicable commands are filtered by the LS according to the current state of the area/actuator: for example, it is not possible to disconnect a railway switch when it is already disconnected. Such filtering prevents the worker to ask for inapplicable commands. Nevertheless, the applicability of commands is always cross-checked by CBI before actuation, which prevents the execution of malformed or non-valid commands and guarantees safety of those operations.

5.2.6 SaM6 – Revert Commands. Commands can be reverted (e.g., re-connecting an area that was previously disconnected) only by the worker that requested it at a first stage or by the station manager in the control room. This denies a worker to re-connect an area that was previously disconnected by another worker, who may still be acting there.

5.3 Security Mechanisms

We report here the security mechanisms of the RWD that pair and synergize with the safety mechanisms and the communication protocols discussed above.

5.3.1 SeM1 - Authentication. The worker should first authenticate to the RWD through a two-step process. First, the worker accesses GS, which asks a login with something the worker *knows*: a username and a password. This enables the worker to choose a station in which they are authorized to operate. Then, the worker is automatically redirected to the LWS of the specific station, where they have to provide an OTP to complete login. Such OTP is generated by LS and sent to the WS through LWS. Workers' credentials and the phone number of the WS are stored in the LS, allowing authentication to be entirely conducted server-side, delegating all these critical actions to the SIL4 LS.

5.3.2 SeM2 - OTP. Login or command requests have to be confirmed using a One-Time-Password. In those cases, the LS (i) generates an OTP through a state-of-the-art Pseudo-Random Number Generator, (ii) associates the OTP to the ID of the worker who requested the operation and, at the same time, (iii) builds a message containing the OTP and supporting information (details are not shared due to non-disclosure), and (iv) forwards the message to LWS alongside with a phone number, to allow the LWS to send such message to the WS as SMS. After the worker types such OTP, (v) WTB forwards such OTP to LWS and LS, allowing the latter to (vi) verify the compliance of the OTP typed by the worker with the one that was generated at step (i). Similarly, to SeM1, critical tasks such as generating and checking OTP are demanded to the SIL4 LS.

5.3.3 SeM3 – Command Feedback. When a command is correctly executed by the CBI, the LS prepares an updated GIF of the synoptic in which additional information is watermarked at random coordinates without overlapping with existing information in the image. The updated synoptic is sent to the WTB, and a message is simultaneously sent to the WS, allowing the worker to check compliance of those two items. Instead, if the command is *not* executed, LS transmits to the WTB a synoptic that *does not* contain additional information, and LS *does not* transmit anything to the WS. If the worker does not get any message on WS, he can assume that the command was not executed, even if malfunctions happen on WTB.

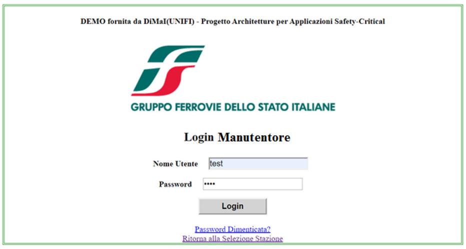
6 MAINTAINANCE PROCEDURE WITH RWD

The RWD calls for an update of the current maintenance procedure we describe below with the help of Figure 6, Figure 7, Figure 8, and Figure 9 and with a sequence diagram in Figure 10 that details the execution of a generic command.

6.1 Login and Station Selection

The worker performing maintenance on a station first connects with GS through WTB. The Global Server asks for login credentials (SeM1, Figure 6), allows the choice of the station, and redirects to the specific LWS (Station_1 in Figure 7) which completes the login asking for an OTP (SeM1, SeM2).

Once the address of the LWS is retrieved by GS, the WTB establishes a direct connection with the LWS performing the initial handshake needed for the safe and secure protocol and for clock


DEMO fornita da DiMaI(UNIFI) - Progetto Architetture per Applicazioni Safety-Critical

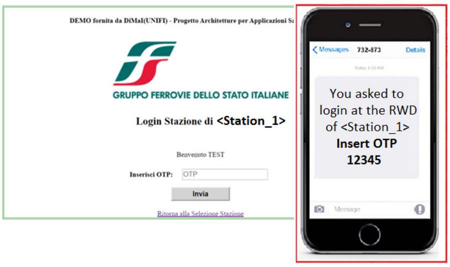
Login Manutentore

Nome Utente: test

Password: ••••

GRUPPO FERROVIE DELLO STATO ITALIANE
Login
Password Dimenticata?
Ritorna alla Selezione Stazione

Fig. 6. Login page of the GS asking for Username and Password.


DEMO fornita da DiMaI(UNIFI) - Progetto Architetture per Applicazioni Sa

Login Stazione di <Station_1>

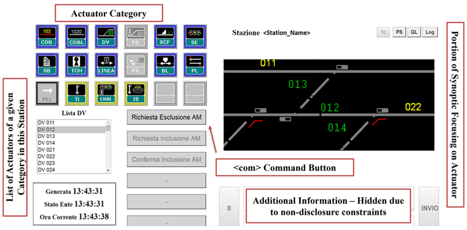
Benvenuto TEST

Inserisci OTP: OTP

You asked to login at the RWD of <Station_1>
Insert OTP
12345

GRUPPO FERROVIE DELLO STATO ITALIANE
Invia
Ritorna alla Selezione Stazione
Messages
732-873
Details
Message

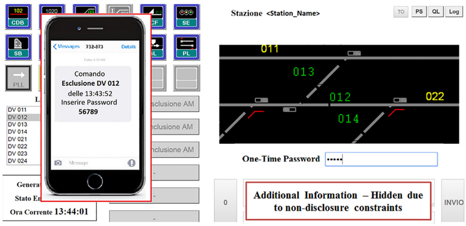
Fig. 7. Login page of the LWS, which completes the two-step login initiated by GS. It is completed by inserting the OTP the worker receives on the WS.


Stazione <Station_Name>

Lista DV: DV 011, DV 012, DV 013, DV 014, DV 021, DV 022, DV 023, DV 024

Generata 13:43:31
Stato Ente 13:43:31
Ora Corrente 13:43:38

Fig. 8. Execution of a command: step 1 – selection of railway switch DV 012.


Comando
Esclusione DV 012
delle 13:43:52
Inserire Password
56789

Stazione <Station_Name>

One-Time Password: •••••

Ora Corrente 13:44:01

Fig. 9. Execution of a command: step 3,4 – exclusion. (disconnection) of railway switch DV 012.

synchronization (SaM2). If different workers operate in different areas of the same station simultaneously, each worker will have his own WTB connected with a dedicated point-to-point channel to LWS.

6.2 Check the Synoptic

Once the worker is authenticated to the LWS, he may want to query the synoptic of the station, ask for planned train routing and review planned maintenance operations. When LS grants login to the worker, it gathers data about the state of physical components of the station through CBI, assembles the required information, and sends the image (plus textual information about specific components, whenever applicable - SaM1) back to LWS, which delivers it to the worker through a webpage (SaM3).

6.3 Execution of Commands

Once logged in, the worker may ask to remotely execute commands. Let *com* be a command the worker wants to execute, e.g., temporarily disconnect an area from the railway network. The procedure to execute the command *com*, shown as sequence diagram in Figure 10, is orchestrated as follows:

(1) The worker selects an area or an actuator category (e.g., railway switch). Then he selects the specific area/actuator (e.g., railway switch DV 012) from a dropdown list; this shows (Figure 8) the portion of the synoptic focusing on the chosen actuator alongside with available commands (SaM5). To execute the command *com* the worker presses the "com" button that is shown in the middle of the page.
(2) LS receives the command.

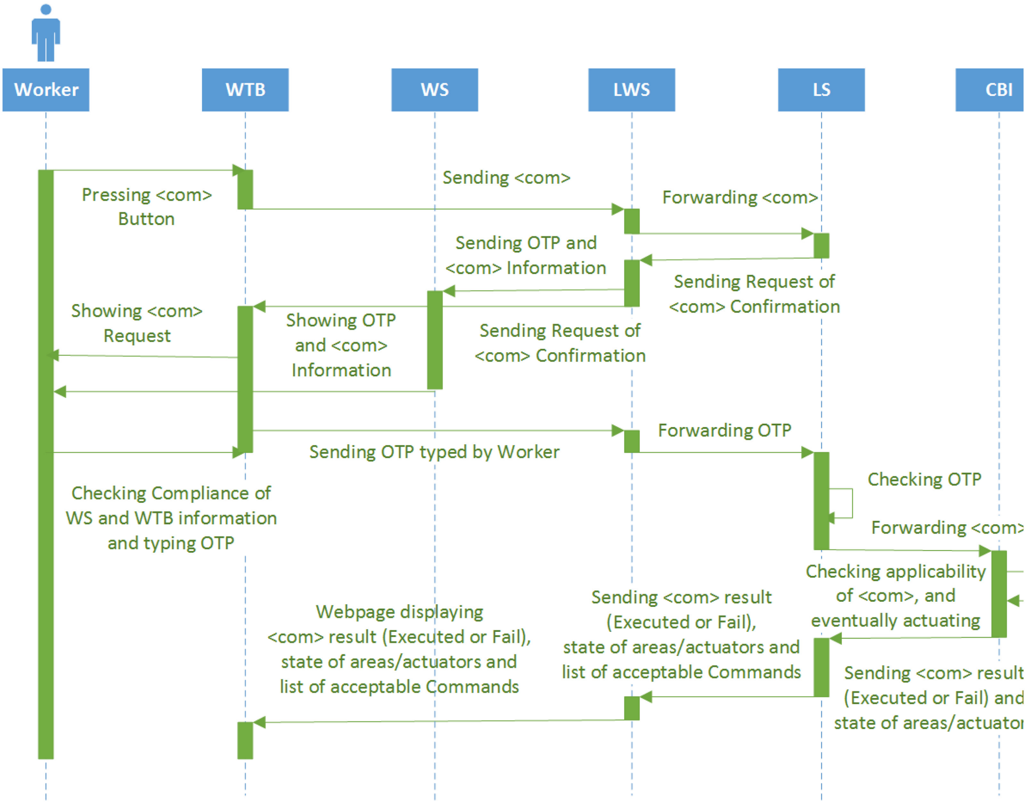

Worker
WTB
WS
LWS
LS
CBI
Pressing <com> Button
Sending <com>
Forwarding <com>
Sending OTP and <com> Information
Sending Request of <com> Confirmation
Showing <com> Request
Showing OTP and <com> Information
Sending Request of <com> Confirmation
Forwarding OTP
Sending OTP typed by Worker
Checking OTP
Forwarding <com>
Checking Compliance of WS and WTB information and typing OTP
Checking applicability of <com>, and eventually actuating
Webpage displaying <com> result (Executed or Fail), state of areas/actuators and list of acceptable Commands
Sending <com> result (Executed or Fail), state of areas/actuators and list of acceptable Commands
Sending <com> result (Executed or Fail) and state of areas/actuator

Fig. 10. Sequence diagram to execute a command <com>. Numbers match bullets in Section 6.3.

(3) LS replies via LWS: (i) to the WTB: an updated synoptic showing the area/actuator and the received command (SaM1, SaM4), and (ii) to the WS: an OTP plus additional information about the requested command (SeM2, Figure 9).
(4) The worker types the OTP received on WS in the WTB after checking compliance of additional information to confirm the command *com*.
(5) The OTP is received by LWS and forwarded to LS. After successfully verifying the validity of the OTP, LS (i) forwards the command to the CBI for actuation, and (ii) stores the requested command (and the feedback the CBI gives) in its internal storage for logging purposes.
(6) Then, LS prepares a feedback to the worker (SeM3), which is delivered through LWS. The worker may be asked to execute additional actions to confirm they correctly got the feedback, which helps mitigate specific threats.
(7) Ultimately, the RWD shows a webpage (similar to Figure 8) that contains an updated synoptic and potentially allows requesting other commands.

Various commands can be sent by the workers according to the same procedure, either if they want to re-connect the area that was previously disconnected, or if they want to disconnect a new one for the sake of maintenance. Note that *once a worker asked for disconnection of an area or an actuator, only that specific worker will be able to reconnect it (SaM6), avoiding critical personal safety problems.*

7 VERIFICATION AND VALIDATION ACTIVITIES

When developing a railway system, each phase of the development lifecycle must be conducted in compliance with CENELEC standards [3, 7, 8, 21]. Among these, EN50128 [8] specifies a set of guidelines that shall be followed for safety-related software. This translates for example into the adoption of adequate code quality metrics [32, 35], and coding standards (e.g., MISRA C [4], widely adopted in the safety-critical domain), as well as the selection and the execution of the proper **Verification and Validation (V&V)** activities. The EN50128 standard sets up best practices to be adopted to comply with a given SIL, even letting the system architect choose amongst many alternatives depending on their expertise or specific project requirements.

Specifically, V&V techniques [8] selected for the RWD are: (i) *Dynamic Analysis and Testing*, applied according to principles *Test Cases Boundary Value Analysis* and *Equivalence Classes and Input Partition Testing*; (ii) *Functional/black box testing*, performed to check the satisfaction of all the functional, safety and security requirements; (iii) *Traceability*, carried out through the filling of *traceability matrixes* to provide an immediate mapping between test case and requirement under test; (iv) *Test Coverage*, verified according to criteria *statement* and *compound condition* and, finally, (v) *Static Analysis*, performed through the use of software tool *Polyspace* [33], to verify the compliance of the source code with selected coding standard and metrics. Such activities have been performed for the LS. Other components LWS, WTB, GS, and WS instead follow specific SIL0 V&V activities, which include a subset of those mentioned above. Given the heterogeneity of the system components, different testing environments have been set up for verification and validation purposes. In particular, we used an ARM board equipped with the *FreeRTOS* [39] real-time operating system for the LS, Linux machines for GS and LWS, and Android devices for WTB and WS.

V&V activities, alongside system concept, architecture, and hazard analyses are currently been used to develop a *safety case*, which reports the compliance of the system to the selected coding standard and metrics, demonstrates the satisfaction of each requirement, and contains a user manual which describes how to deploy and use the RWD system in its operational environment.

8 CONCLUSIONS AND ONGOING WORKS

This paper presented a Remote Worker Dashboard (RWD) to enhance current maintenance of railway infrastructures. RWD allows reducing maintenance time, minimizing delays on train schedule, and increasing safety of track-side workers. The RWD will support workers in managing maintenance operations through safe and secure interaction with the existing Computer-Based Interlocking. Workers can take advantage of personal COTS mobile devices to interact with the system, with clear advantages in terms of safety and time needed to fulfil operations.

To the best of our knowledge, RWD is the first cyber-physical railway system that embeds COTS mobile devices as tablets and smartphones without requiring rugged hardware or special configurations thanks to a consistent and coordinated system engineering effort of both the system owner and the consultants.

We described the current maintenance procedures, motivating the need of an RWD to reduce time needed for such operations and to optimize the overall movements of track-side workers in the station. After recalling key items of the applicable CENELEC standards, we reported on the concept, the definition, the hazard analysis, and the final architecture of the RWD system providing insights about the most relevant safety and security-related aspects that allowed RWD to be certified as a SIL4-compliant system regarding the first four phases of the CENELEC lifecycle [21].

Current works are directed to complete the implementation and V&V of the system, which is currently targeting the LS component. Other components as the webserver LWS and all connected devices were already exercised together and proposed to a group of track-side workers, who provided interesting feedbacks about usability without raising concerns regarding safety and/or availability of the RWD system as a whole. Once implementation, verification, and validation are completed, we will come back to the certification body to complete the assessment which is mandatory to install the RWD in Italian stations.

REFERENCES

[1] Algirdas Avizienis et al. 2004. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing* 1, 1 (2004), 11–33.

[2] IEC, IEC61508. 2010. 61508 functional safety of electrical/electronic/programmable electronic safety-related systems. *International Electrotechnical Commission* (2010).

[3] CENELEC, EN. 50159. Railway applications - Communication, signalling and processing systems - Safety-related Communication in Transmission Part 2 (2011).

[4] MISRA C:2012. Guidelines for the use of C in Critical Systems, 978-1-906400-11-8, Motor Industry Research Association (2013).

[5] International Electrotechnical Commission and Technical Committee 56. 2016. Hazard and operability studies (HA- Q6 641 ZOP studies): Application guide. IEC61882:2016.

[6] D. H. Stamatis. 2003. *Failure Mode and Effect Analysis: FMEA from Theory to Execution.* ASQ Quality Press.

[7] CENELEC EN 50126. 2017. Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) – part 1 (2017).

[8] CENELEC EN 50128. 2012. Railway applications - Communication, signalling and processing systems - Software for railway control and protection systems. (2012).

[9] D. Bertieri, A. Ceccarelli, T. Zoppi, I. Mungiello, M. Barbareschi, and A. Bondavalli. 2021. Development and validation of a safe communication protocol compliant to railway standards. *Journal of the Brazilian Computer Society* 27, 1 (2021), 1–26.

[10] UNISIG, ERTMS/ETCS RBC-RBC Safe Communication Interface, Subset-098, (2012)

[11] UNISIG, UNISIG ERTMS/ETCS - Euroradio FIS, Subset 037 (2016)

[12] Joan Daemen and Vincent Rijmen. AES proposal: Rijndael. 1999.

[13] Junhyuk Song et al. The AES-CMAC algorithm. *RFC* 4493, June, 2006.

[14] RFI – Worker Dashboard, RFI DTCDNSSS SR IS 14 000 C (07/2013).

[15] Alejandro Carlos, Torres-Echeverría, Sebastián Martorell, and H. A. Thompson. 2011. Modeling safety instrumented systems with MooN voting architectures addressing system reconfiguration for testing. *Reliability Engineering & System Safety* 96, 5 (2011), 545–563.

[16] P. Popov, L. Strigini, S. Riddle, and A. Romanovsky. 2001. Protective wrapping of OTS components. In *Proc. 4th ICSE Workshop on Component-Based Software Engineering: Component Certification and System Prediction*, Toronto.

[17] M. Serafini, A. Bondavalli, and N. Suri. 2007. Online diagnosis and recovery: On the choice and impact of tuning parameters. *IEEE Trans. on Dependable and Secure Computing* 4, 4 (2007), 295–312, 2007.

[18] G. Carrozza, D. Cotroneo, and S. Russo. 2008. Software faults diagnosis in complex OTS based safety critical systems. In *2008 7th European Dependable Computing Conference.* IEEE, 25–34.

[19] F. Di Giandomenico and L. Strigini. 1990. Adjudicators for diverse-redundant components. In *Proceedings Ninth Symposium on Reliable Distributed Systems.* IEEE, 114–123.

[20] RFI, Specifica dei Requisiti del Terminale Operatore (TO), codifica RFI DTC STS SR SR SS40 001 A, 2013.

[21] CEI EN50129, Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling. (2004).

[22] Zeeshan E. Bhatti, Partha S. Roop, and Roopak Sinha. 2016. Unified functional safety assessment of industrial automation systems. *IEEE Transactions on Industrial Informatics* 13, 1 (2016), 17–26.

[23] C. Yang, C. Yang, T. Peng, X. Yang, and W. Gui. 2017. A fault-injection strategy for traction drive control systems. *IEEE Transactions on Industrial Electronics* 64, 7 (2017), 5719–5727.

[24] H. W. Lim, W. G. Temple, B. A. N. Tran, B. Chen, Z. Kalbarczyk, and J. Zhou. 2019. Data integrity threats and countermeasures in railway spot transmission systems. *ACM Transactions on Cyber-Physical Systems* 4, 1 (2019), 1–26.

[25] R. E. Bloomfield, P. Popov, K. Salako, V. Stankovic, and D. Wright. 2017. Preliminary interdependency analysis: An approach to support critical-infrastructure risk-assessment. *Reliability Engineering & System Safety* 167 (2017), 198–217.

[26] A. Khaled, S. Ouchani, Z. Tari, and K. Drira. 2020. Assessing the severity of smart attacks in industrial cyber-physical systems. *ACM Transactions on Cyber-Physical Systems* 5, 1 (2020), 1–28.

[27] Richard Bloomfield. 2006. Fundamentals of European rail traffic management system-ERTMS. (2006): 165–184.

[28] Andrea Ceccarelli et al. 2012. Design and implementation of real-time wearable devices for a safety-critical track warning system. *High-Assurance Systems Engineering (HASE), 14th Symp. on.* IEEE.

[29] Muhammad Mahtab Alam and Elyes Ben Hamida. 2014. Surveying wearable human assistive technology for life and safety critical applications: Standards, challenges and opportunities. *Sensors* 14, 5 (2014), 9153–9209.

[30] Gustav Dahll, Mel Barnes, and Peter Bishop. 1990. Software diversity: Way to enhance safety?. *Information and Software Technology* 32, 10 (1990), 677–685.

[31] S. Katzenbeisser and F. A. P. Petitcolas. 2000. *Digital Watermarking*. Artech House, London.

[32] Exida Consulting LLC, C/C++ Coding Standard Recommendations for IEC 61508, Version V1, Revision R2, 2011.

[33] Polyspace static analysis tool, MATLAB, (product description website) https://it.mathworks.com/products/polyspace.html.

[34] T. Wang, W. Wang, A. Liu, S. Cai, and J. Cao. 2018. Improve the localization dependability for cyber-physical applications. *ACM Transactions on Cyber-Physical Systems* 3, 1 (2018), 1–21.

[35] Jill Britton. (PERFORCE) - Programming Research, Which Software Quality Metrics Matter? Online at https://www.perforce.com/resources/qac/which-software-quality-metrics-matter. Accessed 11/7/2023.

[36] Andy Greenberg. 2013. Hackers Reveal Nasty New Car Attacks-With Me Behind the Wheel (Video - online). https://bit.ly/3lWRAIN.

[37] Michal Klenka. Major incidents that shaped aviation security. *Journal of Transportation Security* 12.1-2 (2019), 39–56.

[38] Deutsche Bahn attacked by Wannacry (online), https://www.railtech.com/digitalisation/2017/12/11/wannacry-virus-was-wake-up-call-for-railway-industry/.

[39] FreeRTOS reference manual: API functions and configuration options. *Real Time Engineers Limited* (2009).

[40] Zhuo Li et al. 2016. NDN-GSM-R: A novel high-speed railway communication system via named data networking. *EURASIP Journal on Wireless Communications and Networking* 2016, 1 (2016), 1–5.

[41] F. Flammini, S. Marrone, N. Mazzocca, and V. Vittorini. 2009. A new modeling approach to the safety evaluation of N-modular redundant computer systems in presence of imperfect maintenance. *Reliability Engineering & System Safety* 94, 9 (2009), 1422–1432.

[42] F. Di Giandomenico and L. Strigini. 1990. Adjudicators for diverse-redundant components. In *Proceedings Ninth Symposium on Reliable Distributed Systems.* IEEE, 114–123.

[43] D. L. Mills. 1991. Internet time synchronization: The network time protocol. *IEEE Transactions on Communications* 39, 10 (1991), 1482–1493.

[44] RFI – La Rete oggi (online) https://www.rfi.it/it/rete/la-rete-oggi.html.

[45] A. Ceccarelli, T. Zoppi, A. Vasenev, M. Mori, D. Ionita, L. Montoya, and A. Bondavalli. 2018. Threat analysis in systems-of-systems: An emergence-oriented approach. *ACM Transactions on Cyber-Physical Systems* 3, 2 (2018), 1–24.

[46] Carmen Cheh et al. 2019. Modeling adversarial physical movement in a railway station: Classification and metrics. *ACM Transactions on Cyber-Physical Systems* 4, 1 (2019), 1–25.

[47] S. Banerjee, M. Hempel, and H. Sharif. 2017. A review of workspace challenges and wearable solutions in railroads and construction. In *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC).* IEEE, 91–96.

[48] Network Rail Urged to Eliminate "Victorian Methods of Protection" (online), https://rail.nridigital.com/future_rail_oct19/getting_on_track_with_safety_for_railway_workers.

[49] M. M. Alam and E. Ben Hamida. 2014. Advances in wearable sensor technology and its applications in mobile workforce's health monitoring and safety management. In *SPE Middle East Health, Safety, Environment & Sustainable Development Conference and Exhibition.* Society of Petroleum Engineers.

[50] S. Kliuiev, I. Medvediev, and N. Khalipova. 2020. Study of railway traffic safety based on the railway track condition monitoring system. In *IOP Conference Series: Materials Science and Engineering.* IOP Publishing 985, 1 (2020), 012012.

[51] N. Noorudheen, M. McClanachan, Y. Toft, and G. Dell. 2013. Keeping track workers safe: A socio-technical analysis of emerging systems and technology. *Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit* 227, 5 (2013), 517–528.

[52] C. Baldry and J. Ellison. 2006. Off the rails: Factors affecting track worker safety in the rail industry. *Employee Relations.*

[53] J. M. Sanne. 2008. Framing risks in a safety-critical and hazardous job: Risk-taking as responsibility in railway maintenance. *Journal of Risk Research* 11, 5 (2008), 645–658.

[54] R. Mosberger, H. Andreasson, and A. J. Lilienthal. 2013. Multi-human tracking using high-visibility clothing for industrial safety. In *2013 IEEE/RSJ International Conference on Intelligent Robots and Systems.* IEEE, 638–644.

Received 2 August 2022; revised 14 April 2023; accepted 29 June 2023