



SEMOR: Miglioramento della Sicurezza per gli Operatori di Manutenzione nei Cantieri Ferroviari

SEMOR: Safety Enhancement of Maintenance Operators in Railway worksite

Paolo CESARIO ^(*)

Ivan COLLA ^(*)

Matteo SCIUTTO ^(*)

Filippo SUGLIANO ^(*)

David GOMEZ CASCO ^(**)

Fabrizio TAVANO ^(***)

Tiziano COSSO ^(****)

Michal FALTA ^(*****)

(<https://www.medra.org/servlet/view?lang=it&doi=10.57597/IF.09.2023.ART.2>)

Sommario - La sicurezza nei cantieri ferroviari è una questione cruciale per garantire che i lavoratori non corrano pericoli durante la costruzione e la manutenzione delle infrastrutture ferroviarie.

Il sistema SEMOR migliora le dotazioni di sicurezza del personale che opera nei cantieri, e dei mezzi da loro utilizzati, fornendo il posizionamento in tempo reale degli stessi, supportando il ruolo dell'agente avvisatore.

L'obiettivo del progetto è quello di centralizzare in un Sistema Centrale di Supervisione (CSS) portatile la localizzazione di tutti gli operatori e di tutti i mezzi (con particolare riguardo alle parti mobili che potrebbero invadere il binario attiguo) di uno scalo ferroviario. Per fare ciò, operatori e mezzi vengono dotati di un dispositivo individuale portatile di localizzazione e segnalazione finalizzata alla sicurezza degli operatori, e alla protezione dei treni in transito, dei passeggeri e del personale sugli stessi (per questo si equipaggiano i mezzi d'opera).

Per rilevare la posizione in tempo reale, precisa e robusta, è stata sviluppata una strategia basata su un ricevitore GNSS multi-costellazione e un dispositivo INS (*Inertial Navigation System*).

Summary - Safety on railway working sites is a crucial issue in ensuring that sentinels are not put at risk during the construction and maintenance of railway infrastructure.

The SEMOR system improves the safety equipment of personnel working on working sites, and the vehicles they use, by providing real-time positioning of them, supporting the role of the covering agent.

The objective of the project is to centralize in a portable Central Supervisory System (CSS) the location of all sentinels and vehicles (with particular regard to moving parts that could encroach on the adjacent track) of a railway yard.

To achieve this, operators and vehicles are equipped with an individual portable localization and signaling device aimed to ensuring the safety of operators and the protection of trains in transit, passengers, and personnel on board (which is why the work vehicles are equipped).

A strategy based on a multi-constellation GNSS receiver and an INS (*Inertial Navigation System*) device was developed to detect the position in real time, accurately and robustly.

^(*) Si Consulting.

^(**) European Space Agency (ESA).

^(***) Rete Ferroviaria Italiana (RFI).

^(****) Gter.

^(*****) LEVEL System.

^(*) Si Consulting.

^(**) European Space Agency (ESA).

^(***) Rete Ferroviaria Italiana (RFI).

^(****) Gter.

^(*****) LEVEL System.

1. Introduzione

Le autorità ferroviarie definiscono, a livello nazionale, i requisiti di sicurezza per la protezione dei lavoratori adoperando sia norme e regolamenti, sia tecnologie, al fine di prevenire incidenti e di gestire rischi.

In Italia, in seguito alla pubblicazione della Direttiva ANSF n. 1/dir/2012, l'Agenzia Nazionale per la Sicurezza delle Ferrovie (oggi ANSFISA), ha demandato a RFI, il compito di adeguare le proprie norme in funzione delle modifiche indotte al RCT (Regolamento per la Circolazione dei Treni). Pertanto, il Decreto n. 16/2010 [1], riguardante il regolamento dei regimi di esecuzione dei lavori, emanato dall'ANSF, non è più di competenza dell'Agenzia stessa ma fa parte del Sistema di Riferimento sulla base del quale gli operatori ferroviari possono elaborare ed emanare le proprie disposizioni e prescrizioni in materia di sicurezza della circolazione.

Rete Ferroviaria Italiana, per regolare la circolazione dei treni e in generale l'intero processo di esercizio in sicurezza dell'infrastruttura ferroviaria nazionale, aggiorna costantemente il proprio apparato di norme di esercizio, tra cui istruzioni [2] e linee guida [3][4] per la protezione dei cantieri.

La norma per la sicurezza dei cantieri ferroviari (IPC [2]), prescrive l'interruzione della circolazione dei treni lungo i binari interessati dai lavori; all'articolo 10 viene prescritta quale misura di protezione l'interruzione anche sui binari attigui o, ove possibile, l'approvazione delle misure indicate all'articolo 12; l'articolo 12 indica le modalità per consentire la circolazione sul binario attiguo a quello in lavorazione, fra queste vi è l'uso di sistemi quali l'ATWS per automatizzare le procedure di avvistamento con agente di copertura e l'uso di barriere per rendere chiaramente identificabile l'area interessata ai lavori.

La proposta definita nel presente articolo non ha come obiettivo quello di risolvere il problema della riconduzione al regime di "assenza di circolazione treni" sul binario attiguo, bensì di garantire una maggiore sicurezza nel caso di circolazione su tale binario sotto specifiche prescrizioni. Oggi, nel caso di mancanza delle condizioni di sicurezza sul cantiere, la sicurezza dell'arresto del treno è oggi garantita tramite il sistema SCMT (Sistema di Controllo della Marcia dei Treni) o ERTMS.

D'altra parte, il treno è abilitato a passare per decisione umana: la decisione è demandata all'agente di copertura, sulla base della sua osservazione di tutti i lavoratori, i.e. la certezza delle condizioni di sicurezza in cantiere, è quindi soggetta al fattore umano.

La soluzione SEMOR si occupa pertanto di questo aspetto, supportando il ruolo dell'agente avvisatore introducendo nel processo di avvistamento e protezione da parte dell'agente di copertura coadiuvato da ATWS, quello di individuazione, tramite "barriera virtuale", della zona dove i lavoratori possono restare senza rischi, definita come "area sicura".

1. Introduction

The railway authorities define at national level, the safety requirements for the protection of workers using both standards and regulations, as well as technology, in order to prevent accidents and manage risks.

In Italy, following the publication of the ANSF Directive No. 1/dir/2012, the National Agency for the Railway Safety (today ANSFISA), has entrusted RFI with the task of adapting its regulations according to the changes brought about by the RCT (Regulations for the Circulation of Trains). Therefore, according to the Decree No. 16/2010 [1], concerning the regulation of the works execution regimes, issued by the ANSF, it is no longer the responsibility of the Agency itself but it is part of the Reference System on the basis of which railway operators can elaborate and issue the own regulations and standards about traffic safety.

Rete Ferroviaria Italiana, in order to regulate the railway traffic and in general the entire process of safe operation of the national railway infrastructure, constantly updates its system of operating rules, including instructions [2] and guidelines [3][4] for the protection of working sites.

The national norm for the safety in railway working sites (IPC [2]) prescribes the suspension of train circulation along the tracks affected by the works. Article 10 prescribes as a protective measure the suspension of circulation on adjacent tracks as well, or, if possible, the implementation of the measure indicated in Article 12. Article 12 outlines the procedure to allow circulation on the track adjacent to the one under works, including the use of system such as ATWS, to automate the "observation" procedures with a "covering agent" and the use of physical barriers to clearly identify and separate the area affected by the works.

The purpose of the proposal defined in the present paper is not to support the management of the "no train running" regime on the adjacent track, but to ensure the best safety in the case that running on that track is allowed under specific prescriptions. Today, in the event of unsafe conditions for the workers on the working site, the safety is guaranteed by the signalling system (SCMT – the Italian Train Running Control System or ERTMS by stopping the approaching train.

On the other hand, the train is enabled to pass by human decision: the decision is delegated to the covering agent, based on his observation of all the workers, i.e. the certainty of safety conditions on the working site, is still subject to the human factor.

The SEMOR solution addresses this aspect by supporting the role of the covering agent by introducing into the process of alerting and protecting the workers by a covering agent assisted by ATWS, that of identification, through a "virtual barrier", of the area where the workers can stay without risks, defined as a "safe area".

SEMOR is able to detect the presence of the operators of the safe area in relation to its boundaries and thus to ensure the safe state of every operator.

SEMOR è in grado rilevare la presenza degli operatori del cantiere rispetto ai confini di tale area e quindi di garantirne lo stato sicuro.

2. Contesto applicativo

Gli operatori dei siti di lavoro ferroviari sono esposti a rischi connessi alla circolazione quando il traffico ferroviario, sul binario attiguo a quello in lavorazione, non è completamente interrotto.

Il passaggio del treno sui binari adiacenti può essere consentito se viene attivata una protezione su avvistamento oppure se viene installata temporaneamente una barriera fisica per impedire di invadere l'area di pericolo.

L'installazione di barriere richiede però tempi la cui durata deve risultare irrilevante rispetto alla durata dei lavori stessi e tale operazione. Di conseguenza, viene prevista solo nel caso di lavorazioni di lunga durata.

Alternativamente, al fine di avvisare gli operatori di cantiere che lavorano lungo la tratta, il treno in avvicinamento viene prontamente segnalato grazie a procedure regolate dall'IPC [2] tramite avvistamento con agente di copertura coadiuvato da ATWS.

L'uso di SEMOR si inserisce nelle procedure definite dall'IPC [2] fornendo all'avvisatore ulteriore conferma dello stato sicuro della localizzazione di tutti i lavoratori del cantiere anche quando le condizioni di visibilità potrebbero essere ostacolate (presenza di macchine operatrici ingombranti, etc.). In particolare permangono le limitazioni di velocità sul binario attiguo in relazione alle distanze consentite agli operatori durante in transito del treno definite al comma 1 dell'articolo 10 dell'IPC: tali distanze vengono infatti utilizzate per imporre il confine dell'area sicura di SEMOR durante la fase di predisposizione del cantiere.

In passato, le fasi del processo adottate per ridurre il rischio di incidenti sul binario attiguo a quello in lavorazione erano tutte basate su intervento umano: avvistamento del treno in arrivo da una postazione in linea molto lontana dal cantiere, inoltro dell'informazione al cantiere, avviso ai lavoratori di mettersi in condizione sicura, verifica dello stato sicuro dei lavoratori e comunicazione ad un secondo addetto in una postazione intermedia dal cantiere di consentire il passaggio del treno (questo doveva rimuovere una bandiera rossa posta fra i binari in modo che il macchinista non venisse allertato alla frenatura).

Oggi, la tecnologia ATWS (*Automatic Track Warning Systems*) [5] si inserisce nel processo per supportare le mansioni umane. Tale sistema rappresenta infatti un'applicazione automatica di mansioni esecutive (avvistamento e avviso) e consente di mitigare il rischio di incidenti che possono coinvolgere attività svolte dall'umano. L'ATWS mette a disposizione tecnologie basate su un livello di integrità per la sicurezza SIL3 e/o SIL4 definito in base agli standard [6], [7]; tali tecnologie coprono tutte le

2. Background

Operators of railway work sites are exposed to traffic hazards when train traffic on the track adjacent to the one being worked on is not completely interrupted.

Train passage on adjacent tracks may be permitted if a guard on sight is activated or if a physical fence is temporarily installed to prevent encroachment into the danger area.

However, the installation of barriers requires a time-frame that must be deemed negligible in relation to the duration of the actual works. Therefore, this operation is only envisaged in cases of long-duration construction activities.

Alternatively, in order to notify the construction workers operating along the track, the approaching train is promptly signaled through regular procedures by the IPC [2] via sighting agent and covering agent assisted by ATWS.

The use of SEMOR is integrated into the procedures defined by the IPC [2], proving the warning agent with additional confirmation of the safe status and location of all construction workers, even when visibility conditions may be hindered (presence of bulky operating machinery, etc.). In particular, speed restriction on the adjacent track remains in relation to the distances allowed for workers during train transit, as defined in paragraph 1 of Article 10 of IPC: these distances are indeed used to establish the boundary of SEMOR's safe area during the construction setup phase.

In the past, the process steps taken to reduce the risk of accidents on the track adjacent to the one being under works, were all based on human intervention: sighting the incoming train from a very far position along the line, forwarding the information to the working site, warning the workers to get them into a safe condition, checking the workers' safe status and informing a second operator along the line, at intermediate distance from the working site, to allow the train to pass (he had to remove from the track a red flag, so the train driver is not alerted to brake).

Today, Automatic Track Warning Systems (ATWS) technology [5] is introduced into the process to support human tasks. In fact, such a system represents an automatic application of executive tasks (sighting and warning) and makes it possible to mitigate the risk of accidents that may involve the human operation. The ATWS provides technologies based on a safety integrity level SIL3 and/or SIL4 defined according to standards [6][7]; such technologies cover all stages of the process described above except that of ensuring the safe status of all workers and machines on the site.

The decision to consider the danger area cleared and to allow the train to pass remains the responsibility of the covering agent, who in a few seconds must assess, on the basis of what he sees and of his perception of the risk, whether all the workers and working machines are in the safe area.

The level of safety provided by the current procedures is certainly adequate, but the fact remains that incidents

fasi del processo sopra descritto ad eccezione di quella di garanzia del raggiunto stato sicuro di tutti i lavoratori e di tutti i mezzi del cantiere.

La decisione di considerare sgombra l'area di pericolo e di consentire il passaggio del treno rimane di competenza dell'agente avvisatore, che in pochi secondi deve valutare, sulla base di ciò che vede e della sua percezione del rischio, se tutti i lavoratori e i macchinari/mezzi d'opera siano in posizione di sicurezza.

Il livello di sicurezza che le procedure in vigore è sicuramente adeguato, ma sta di fatto che incidenti nei cantieri continuano, sporadicamente, a verificarsi. D'altra parte il processo che garantisce al treno l'accesso sul binario attiguo utilizza da un lato il supporto di apparecchiature SIL3 o SIL4 (ATWS) nella gestione dell'avvistamento e dell'avviso, ma nel momento in cui occorre garantire il rientro dei lavoratori in area sicura e la presa visione di tale stato, tali azioni ricadono completamente nel fattore umano.

Purtroppo le fatalità occorrono, seppure raramente, nella ragione di un incidente ogni due o tre anni [8], e sono spesso dovute ad eccesso di zelo associato ad eccesso di fiducia in sé stesso (il lavoratore continua la lavorazione in presenza di allarme), come ad altri fattori quali errori di comunicazione o distrazione.

Il modo più semplice per ottenere una minimizzazione dell'impatto del fattore umano è quello di garantire un supporto tecnologico anche per le altre fasi del processo, ovvero non solo per l'avvistamento e l'avviso (supporto garantito tramite ATWS), ma anche per la messa in sicurezza degli operatori e dei mezzi.

Con questo obiettivo Si Consulting, insieme a Rete Ferroviaria Italiana, LEVEL System e Gter, ha proposto ad ESA (European Space Agency) un progetto di ricerca e sviluppo atto a ridurre ulteriormente il rischio nella protezione dei cantieri ferroviari.

Si può quindi affermare che la soluzione SEMOR (*Safety Enhancement of Maintenance Operators in Railway worksite*) integra gli attuali sistemi di sicurezza nelle attività di manutenzione delle linee ferroviarie [9], [10] supportando tecnologicamente l'agente avvisatore nella verifica della condizione sicura, mettendo a disposizione la posizione in tempo reale di tutti gli operai che lavorano presso il cantiere e di ciascun mezzo e/o attrezzatura da essi adoperati.

In tale modo non esistono sovrapposizioni di funzioni: l'ATWS rileva l'arrivo dei treni tramite dispositivi elettromeccanici installati lungo la linea, allarma l'agente di copertura per l'attivazione degli allarmi acustici e luminosi ai lavoratori e consente di comandare il sistema di segnalamento per arrestare il treno in caso di condizioni non sicure, SEMOR è quindi complementare infatti supporta l'agente di copertura per consentire o meno il passaggio del treno, attenuando il rischio residuo di errore umano, grazie alla localizzazione di precisione in tempo reale di lavoratori, attrezzature e veicoli.

in working site continue to occur sporadically. On one hand, the process that allows train to access to the adjacent track utilizes SIL3 or SIL4 equipment (ATWS) for managing sighting and warning. However, when it comes to ensuring the return of workers to the safe area and verifying their safety status, these actions rely entirely on human factors.

Unfortunately, fatalities do occur, albeit rarely, with an average of one incident every two or three years [8], and they are often due to overzealousness combined with an excess of self-confidence (the worker continues working despite the alarm), as well as other factors such as miscommunication or distractions. The simplest way to minimize the impact of human factors is to ensure technological support for other stages of the process as well, not only for sighting and warning (supported provided through ATWS), but also to secure workers and machines.

With this objective in mind, Si Consulting, together with Rete Ferroviaria Italiana, LEVEL System and Gter, proposed a research and development project to ESA (European Space Agency) to further reduce risk in the protection of railway work sites.

It can therefore be said that the SEMOR (Safety Enhancement of Maintenance Operators in Railway worksite) solution integrates the current safety systems in railway track maintenance activities [9][10] technologically supporting the covering agent in verifying the safe condition by providing the real-time position of all the workers and of each working machine and/or equipment in use.

In such a way there are no functional overlaps: ATWS detects the arrival of trains by electromechanical devices along the line, warns the covering agent to activate the acoustic and light alarms to the workers, and enables to command the signalling system to stop the train in the case of unsafe conditions, SEMOR is consequently complementary, in fact supports the covering agent to allow or not the passage of the train, mitigating the residual risk of human error, thanks to the real-time precision localization of workers, equipment and vehicles.

Thus, it can be stated that SEMOR fits within the current regulatory framework without requiring modification and is complementary, not alternative, to ATWS. All the roles foreseen by the railway norm remain unchanged; the covering agent responsibilities is the same but is lightened thanks to two technological support system: ATWS and SEMOR.

As will be seen later, SEMOR does not introduce any specific additional actions during the process. Rather, it allows the covering agent to avoid scanning the entire working site within a few second to verify the safety of the workers, instead allowing him to view their positions on the screen. Additionally, the two interfaces can be physically associated during field installation, thereby minimizing the management impact of the HMI, as show in Fig. 1.

Si può quindi affermare che SEMOR si inserisce nell'attuale quadro normativo senza richiederne modifiche e risulta complementare e non alternativo all'ATWS.

Tutti i ruoli previsti dalla normativa rimangono immutati; la responsabilità dell'agente avvisatore rimane la stessa, ma viene alleggerita grazie a due sistemi tecnologici di supporto: ATWS e SEMOR.

Come si vedrà nel seguito, SEMOR non introduce particolari azioni supplementari durante il processo. Consente anzi all'avvisatore di non dover percorrere con lo sguardo in pochi secondi l'intero cantiere per accertarsi della messa in sicurezza dei lavoratori, consentendogli al contrario di visualizzarne la posizione sullo schermo. Le due interfacce possono inoltre essere associate fisicamente nell'installazione in campo minimizzando anche l'impatto gestionale dell'HMI come visibile in Fig. 1.

3. Analisi preliminare

SEMOR è stato sviluppato facendo riferimento alle norme [11][12][13][14][15].

Per quanto riguarda le fasi del ciclo di vita del software [14], sono state coperte tutte le fasi definite dalla norma fino alla realizzazione del prototipo: requisiti software, architettura e design, progettazione dei componenti, implementazione e test dei componenti, integrazione e validazione finale. Le fasi di distribuzione e manutenzione del software, invece, non hanno ancora avuto luogo, essendo il sistema, ad oggi, realizzato a livello prototipale.

In particolare, i requisiti software sono stati individuati attraverso un processo condiviso con RFI e il software è stato sviluppato in modo da soddisfare il livello di sicurezza SIL2 secondo i criteri definiti dalla norma CENELEC 50128.

Al momento, il prototipo utilizza un hardware COTS (*Off-the-Shelf component*), ovvero fa uso di prodotti in serie disponibili in commercio. Le fasi di trasformazione del prototipo in un prodotto industriale, e quindi la sua certificazione in sicurezza con il coinvolgimento di un *Independent Safety Assessor*, prevedono la sostituzione delle componenti hardware con sottosistemi certificati, almeno per quanto riguarda le funzioni di sicurezza; ciò è fattibile essendo oramai diverse le ditte in grado di realizzare lo sviluppo di prodotti generici hardware certificati pronti per l'integrazione.

Il SIL2 consentirà peraltro di raggiungere il target opportuno per ottenere un livello di integrità tale da garantire la sicurezza: nell'ambito di un'attività realizzata all'inizio del secondo decennio del secolo per RFI (2012), riguardante un'analisi per i possibili scenari di rischio nei cantieri ferroviari, è emerso che il SIL2 risulta essere sufficiente se anche la progettazione del cantiere (ovvero della posa dei sistemi per la rilevazione dei treni in approccio) viene effettuata secondo criteri di verifica indipendente [16]. Ad ogni modo, l'obiettivo finale di SEMOR è



Figura 1 – Possibile integrazione del CCS di SEMOR nell'ATWS.

Figure 1 – Possible integration of SEMOR's CCS into the ATWS.

3. Preliminary analysis

SEMOR was developed with reference to standards [11][12][13][14][15].

With regards the phases of the software life cycle [14], all the phases defined by the standard were covered up to the realization of the prototype: software requirements, architecture and design, component design, component implementation and testing, integration and validation. The software deployment and maintenance phases, on the other hand, have not yet taken place, since the system, to date, has been implemented on a prototype level.

In particular, the software requirements were identified through a process shared with RFI and the software was developed in order to meet the SIL2 safety level according to the criteria defined by the CENELEC 50128 standard.

quello di ottenere un prodotto definitivo SIL4. La sfida, non è tanto la realizzazione del software che richiede un *effort* aggiuntivo minimo quanto l'attuale ingombro di una scheda SIL4 relativamente alla sua indossabilità da parte dei lavoratori.

Al fine di progettare il sistema SEMOR, è stato necessario individuare gli scenari operativi, attraverso i quali sono stati indagati e definiti in dettaglio tutti i passaggi delle diverse situazioni in cui è stato introdotto l'utilizzo del software.

Le fasi di analisi sono le medesime previste dalla normativa ferroviaria. Queste servono a gestire in modo sicuro il comportamento dei lavoratori lungo la linea, quando un treno deve transitare sul binario adiacente:

- inizio dei lavori;
- avvicinamento di un treno e gestione della sicurezza dei lavoratori per consentire il transito del treno;
- ripresa dei lavori.

Inoltre sono stati considerati gli scenari di degrado, quali:

- guasto dei sistemi di comunicazione;
- errore nel controllo di sicurezza dei lavoratori.

Infine, tenendo in considerazione le normative sulla privacy, è stata gestita la funzione di *Juridical Recorder*, ovvero la memorizzazione di tutti gli eventi riguardanti la sicurezza, esclusi i movimenti al di fuori dell'area di lavoro delimitata, i *timestamp* e gli eventi quando non è attivo alcun allarme per il treno in avvicinamento.

Analizzando i passaggi sequenziali degli scenari, sono emersi requisiti di dettaglio che sono stati assegnati ai diversi dispositivi del sistema.

I requisiti di sistema sono classificati sia dall'allocazione al componente (dispositivo portatile individuale PID per localizzare i lavoratori e dispositivo CSS portatile del gestore di cantiere) sia dall'aspetto tecnico (hardware e software).

Rispetto ai requisiti definiti dalla proposta tecnica, grazie al brainstorming orientato ad un approccio più sicuro, sono stati identificati tutti i requisiti di sicurezza; ad esempio, per la condizione nominale che il segnale a protezione del cantiere deve assumere è stata identificata quella di "via impedita"; in tale modo, in caso di avaria dei sistemi di comunicazione, il sistema rimane nella condizione di sicurezza più restrittiva e il treno in avvicinamento viene fermato sino al completo ripristino delle funzionalità.

Un ulteriore elemento di estrema importanza per la riuscita del progetto è stato individuare la metodologia migliore per rilevare in tempo reale la posizione dei lavoratori, la quale deve soddisfare la precisione necessaria e, allo stesso tempo, l'adeguata robustezza. È importante sottolineare come non sia necessaria una precisione centimetrica, con errore istantaneo non noto, bensì occorra

At the moment, the prototype uses COTS (Off-the-Shelf component) hardware, i.e. it makes use of commercially available serial products. The steps for transformation the prototype into an industrial product, and thus its safety certification with the involvement of an Independent Safety Assessor, provide for the replacement of the hardware components with certified subsystems, at least as regards the safety functions; this is feasible as several companies are now able to develop certified generic hardware products ready for integration.

Furthermore, SIL2 will make it possible to reach the appropriate target for obtaining an integrity level such as to guarantee safety: in the context of an activity carried out at the beginning of the second decade of the century for RFI (2012), concerning an analysis of the possible risk scenarios in railway yards, it emerged that the SIL2 is sufficient if also the design of the yard (i.e. the installation of systems for detecting trains in approach) is carried out according to independent verification criteria [16]. In any case, SEMOR's ultimate goal is to achieve a definitive SIL4 product. The challenge is not so much the implementation of the software, which requires minimal additional effort, but the actual footprint of a SIL4 board relative to its wearability by workers.

In order to design the SEMOR system, it was necessary to identify the operational scenarios, through which all the steps of the different situations, in which the use of the software was introduced, were investigated and defined in detail.

The analysis phases are the same as those required by the railway legislation. These are used to safely manage the behavior of workers along the line when a train has to pass on the adjacent track:

- *start of work;*
- *approach of a train and management of the workers safety to allow the transit of the train;*
- *resumption of work.*

In addition, degradation scenarios were considered, such as:

- *failure of communication systems;*
- *workers' safety control failure.*

Finally, taking into consideration the privacy regulations, the Juridical Recorder function was managed, i.e. the storage of all safety-related events, excluding movements outside the delimited work area, timestamps and events when no alarm is active for the approaching train.

By analyzing the sequential steps of the scenarios, detailed requirements emerged that were allocated to the different devices in the system.

The system requirements are categorized both by the component aspect (portable individual PID device for locating workers or portable CSS device of the site manager) and by the technical aspect (hardware or software).

garantire, dato l'errore di misura, la possibilità di "allontanare" dinamicamente, quando necessario, il confine dell'area sicura dal binario attiguo.

La strategia sviluppata, rappresentata in Fig. 2, si basa su un ricevitore GNSS multi-costellazione e un dispositivo INS. Questi tipi di dispositivi generano dataset che consentono di calcolare posizioni indipendenti utilizzando flussi di elaborazione paralleli. Il primo flusso elabora i dati GPS in RTK (*Real Time Kinematic*), il secondo i dati GALILEO in modalità PPP (*Precise Point Positioning*), il terzo utilizza un dispositivo IMU (*Inertial Measurement Unit*).

La sostanziale differenza riguarda il fatto che mentre il posizionamento RTK utilizza un servizio esterno locale (sia esso una singola base o una rete di stazioni permanenti) i cui dati vengono utilizzati per fare delle correzioni che vengono poi inviate al ricevitore sul campo, il PPP indica, invece, una tecnica di rilievo in cui si effettua un posizionamento di precisione senza appoggiarsi a infrastrutture esterne.

Invece la IMU è basata su sensori inerziali, come accelerometri e giroscopi, che permettono un monitoraggio della dinamica di un mezzo al fine di distinguere un soggetto stazionario da uno in movimento.

Le soluzioni indipendenti calcolate a partire dai due sistemi satellitari, con l'ausilio della soluzione proveniente dalla IMU, vengono poi confrontate e se concordano (entro un errore accettabile ben definito) vengono mediate per ottenere il posizionamento finale preciso e robusto. Qualora, invece, i due segnali satellitari discordassero tra di loro per un tempo sufficientemente lungo, o la staticità/il movimento dalla IMU risultasse in contrasto con le rilevazioni satellitari, per evitare eventuali rischi, verrebbe impedito all'agente avvisatore di autorizzare il passaggio del treno, inibendo la possibilità di cambiare la condizione del segnale luminoso a protezione del cantiere, impostata di default a "via impedita".

Al momento, non esiste interfacciamento diretto fra SEMOR e comando del segnale di protezione, che è demandato invece all'agente avvisatore, per cui nulla impedisce all'agente di non rispettare l'indicazione di SEMOR. Il progetto definitivo prevede, tuttavia, l'interfacciamento diretto con il segnalamento e quindi anche tale limitazione del prototipo verrà superata.

4. Implementazione

Tenendo in considerazione quanto individuato durante l'analisi preliminare, il sistema è stato implementato sviluppando quattro sottosistemi (Fig. 3):

- Stazione di Riferimento Principale (MRS), un micro-computer utilizzato per l'esecuzione di un software che invia correzioni differenziali a tutti i dispositivi nell'area di lavoro al fine di ottenere una precisa localizzazione; dotato di un ricevitore GNSS a doppia frequenza con antenna a livello geodetico GNSS.

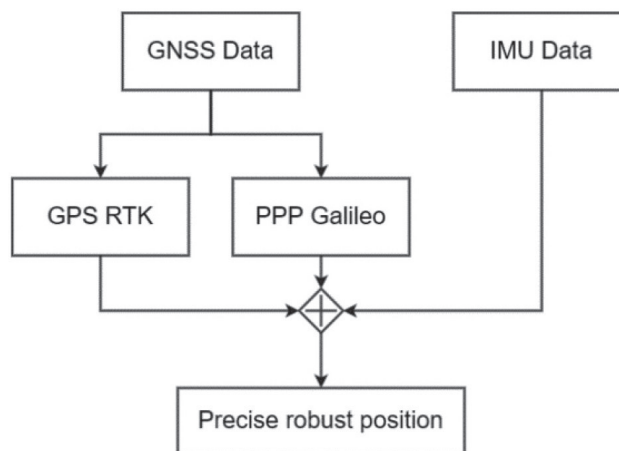


Figura 2 – Diagramma di flusso del processo di localizzazione preciso.

Figure 2 – Flowchart of the precise localization process.

With respect to the requirements defined by the technical proposal, thanks to brainstorming oriented towards a safer approach, all the safety requirements were identified; for example, for the nominal condition that the signal protecting the working site must assume, the 'via impeded' condition was identified; in this way, in the event of a failure of the communication systems, the system remains in the most restrictive safety condition and the approaching train is stopped until functionality is fully restored.

A further element of utmost importance for the success of the project was to identify the best methodology to detect the actual position of the workers in real time, which must meet the necessary precision and, at the same time, the appropriate robustness. It is important to emphasize that centimetre accuracy, with an unknown instantaneous error, is not required, but rather the possibility of dynamically "moving" the boundary of the safe area away from the adjacent track when necessary, given the measurement error.

The developed strategy, depicted in Fig. 2, is based on a multi-constellation GNSS receiver and an INS device. These types of devices generate datasets that allow independent position calculations using parallel processing streams. The first stream processes GPS data in RTK (Real Time Kinematic), the second processes GALILEO data in PPP (Precise Point Positioning) mode, the third uses an IMU (Inertial Measurement Unit) device.

The main difference is that while the RTK positioning uses a local external service (be it a single base or a network of permanent stations) whose data are used to make corrections that are then sent to the receiver in the field, the PPP, on the other hand, indicates a survey technique in which precision positioning is carried out without relying on external infrastructures.

In contrast, the IMU is based on inertial sensors, such as accelerometers and gyroscopes, which allow a monitor-

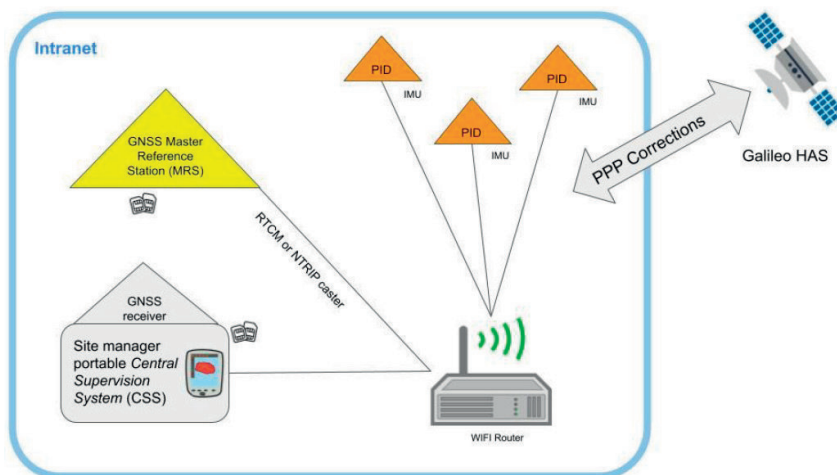


Figura 3 – Raffigurazione dell'architettura del sistema.
Figure 3 – Layout of the system architecture.

- Router WIFI:
 - LTE (Long-Term Evolution), per eseguire il posizionamento RTK/PPP, calcolare, in breve tempo, le coordinate precise dell'MRS (necessarie per computare le correzioni differenziali) e comunicare con l'ATWS o altri sistemi di segnalamento;
 - "a corto raggio", per supportare la comunicazione tra MRS, CSS e PID.
- Dispositivo Portatile di localizzazione e allarme Individuale (PID), per localizzare la posizione di ciascun lavoratore e di ciascun attrezzo e mezzo, inviata poi al CSS, e per allertare gli stessi qualora debbano liberare il cantiere e spostarsi in un'area sicura.
- Sistema di Supervisione Centrale (CSS) portatile, un'applicazione mobile GIS/web-GIS (Geographic Information System), utilizzata dall'agente avvisatore, per disegnare l'area del cantiere, opportunamente georeferenziata, e per mostrare, rispetto a quell'area, le posizioni degli interessati, stimate dai PID, in tempo reale.

I componenti principali sono i dispositivi portatili CSS e i PID, poiché entrambi gestiscono dati vitali e diagnostici. Le sezioni seguenti descrivono quindi i due sottosistemi, includendo le loro caratteristiche.

5. PID

Il Dispositivo Portatile di localizzazione e allarme Individuale (PID) e il Sistema di Supervisione Centrale (CSS) comunicano continuamente al fine di scambiare opportune informazioni, tra cui: la posizione, lo stato di batteria, i segnali di attivazione di allarmi e led, eventuali errori.

In particolare, i dati di localizzazione inviati da ogni PID al CSS, servono all'agente avvisatore per decidere se autorizzare o meno il passaggio del treno.

ing of the dynamics of a vehicle in order to distinguish a stationary subject from one in motion.

The independent solutions calculated from the two satellite systems, with the help of the solution from the IMU, are then compared and if they agree (within a well-defined accepted error) are averaged to obtain the final precise and robust positioning.

If, on the contrary, the two satellite signals disagree with each other for a sufficiently long time, or the static/movement from the IMU is at odds with the satellite readings, in order to avoid any risks, the covering agent would be prevented from authorizing the passage of the train, inhibiting the possibility of changing the condition of the light signal protecting

the yard, which is set to "prevented way" by default.

At the moment, there is no direct interface between SEMOR, and the control of the protection signal, which is instead delegated to the covering agent, so there is nothing to prevent the agent from not respecting the indication of SEMOR. The final design, however, provides for direct interfacing with the signaling agent, and therefore this limitation of the prototype will also be overcome.

4. Implementation

Taking into consideration what was identified during the preliminary analysis, the system was implemented by developing four subsystems (Fig. 3):

- Master Reference Station (MRS), a microcomputer used to run a software that sends differential corrections to all devices in the work area in order to obtain a precise localization; equipped with a dual frequency GNSS receiver with GNSS geodetic level antenna.
- WIFI Router:
 - LTE (Long-Term Evolution), to perform RTK/PPP positioning, calculate, in a short time, the precise MRS coordinates (necessary to compute the differential corrections) and communicate with the ATWS or other signaling systems;
 - "short range", to support communication between MRS, CSS and PID.
- Portable Individual localization and alerting Device (PID), to locate the position of each worker, and each piece of equipment and vehicle, which is then sent to the CSS, and to alert them if they need to vacate the site and move to a safe area.
- Portable Central Supervision System (CSS): a GIS/web-GIS (Geographic Information System) mobile application used by the site manager to draw the site area, ap-

Per l'attuale fase prototipale, durante la fase di allarme che segnala l'imminente approccio di un treno, i PID inviano i dati al CSS ogni secondo. Tale frequenza è stata ritenuta sufficiente a garantire la mappatura in sicurezza della localizzazione e per permettere una buona durata della batteria. Se, da ulteriori analisi, tale frequenza dovesse risultare insufficiente, esistono comunque margini per infittire la trasmissione.

Il prototipo del PID è così costituito, vedi Fig. 4:

- un Raspberry PI;
- 4led colorati (rosso, verde, giallo e arancione) e un pulsante di conferma;
- un buzzer piezoelettrico;
- un'unità di misura inerziale (IMU).

Inizialmente il PID era dotato unicamente di un allarme sonoro, che veniva attivato in fase di emergenza e veniva interrotto quando il lavoratore andava a posizionarsi in un'area sicura portando con sé tutti i mezzi e comandando le parti mobili dei mezzi di lavorazione. Successivamente, dopo l'esecuzione di una Hazard Analysis, è stato individuato il rischio che l'operaio venisse a trovarsi casualmente nell'area sicura e non si accorgesse dell'allarme a causa dell'utilizzo di strumenti di lavoro rumorosi quali una sega-rotale o delle cuffie antirumore. Pertanto l'autorizzazione del passaggio del treno da parte dell'agente avvisatore, avendo ricevuto la posizione sicura, avrebbe potuto indurre un rischio di incidente nel caso in cui il lavo-

propriately georeferenced, and to show, with respect to that area, the positions of those involved, estimated by the PIDs, in real time.

The main components are the portable CSS and PID devices, as both handle vital and diagnostic data. The following sections therefore describe the two subsystems, including their characteristics.

5. PID

The Portable Individual Location and Alarm Device (PID) and the Central Supervision System (CSS) communicate continuously in order to exchange appropriate information, including; location, battery status, alarm and LED activation signals, and any errors.

In particular, the location data sent by each PID to the CSS is used by the covering agent to decide whether or not to authorize the passage of the train.

For the current prototype phase, during the alarm phase, which signals the imminent approach of a train, the PIDs send data to the CSS every second. This frequency was deemed sufficient to ensure safe location mapping and allow for good battery life. If, on further analysis, this frequency proves insufficient, there is, however, scope to thicken the transmission.

The PID prototype is made up as follows, see Fig. 4:

- a Raspberry PI;

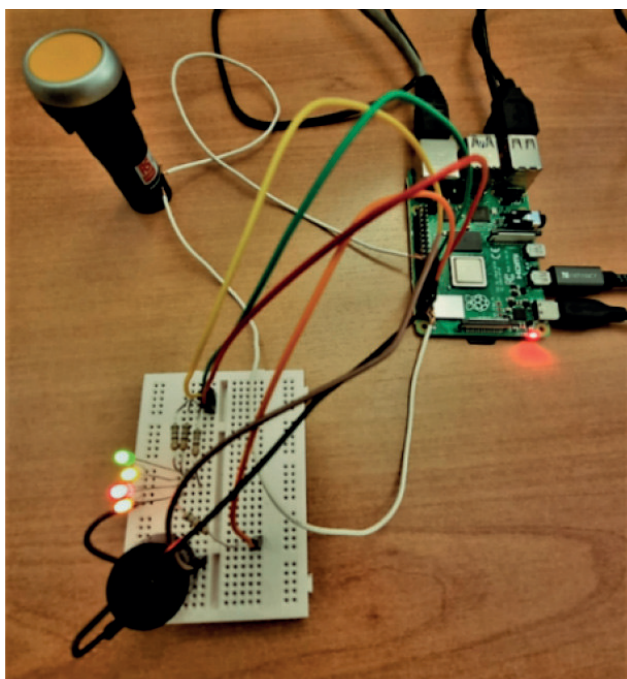


Figura 4 – (a) Prototipo PID iniziale; (b) Prototipo PID finale.
Figure 4 – (a) Initial PID prototype; (b) Final PID prototype.

ratore, non essendosi accorto dell'allarme, avesse invaso casualmente l'area pericolosa, per esempio per aggirare un mezzo di lavoro od oggetti ingombranti posizionati sulle rotaie del binario in interruzione.

Ragione per cui, è stato deciso di aggiungere led luminosi, tramite i quali comunicare al lavoratore il suo stato e un pulsante di conferma, che si attiva solo all'interno della zona sicura, con il seguente funzionamento (vedi rappresentazione grafica Fig. 5):

1. la luce rossa avvisa il lavoratore che deve spostarsi presso una zona sicura portando con sé gli eventuali attrezzi/mezzi;
2. la luce gialla indica che il lavoratore si trova in un'area sicura e che quindi deve premere il pulsante di conferma sia del suo PID che di quello posizionato sul mezzo da lui utilizzato, al fine di garantire la consapevolezza del lavoratore relativamente alla situazione in atto;
3. la luce arancione dimostra che il lavoratore ha premuto i pulsanti;
4. la luce verde, infine, segnala al lavoratore che il treno è transitato e la situazione di pericolo è terminata.

Riguardo le condizioni di allarme, ricordiamo che comunque, al momento, non è previsto l'utilizzo di SEMOR disgiunto dall'ATWS e che, di conseguenza, sono comunque attivi nel cantiere, i sistemi di allarme visivo e sonoro dell'ATWS stesso.

Il CSS mostra all'agente avvisatore lo stato di abilitazione all'autorizzazione del passaggio del treno soltanto se, tutti gli indicatori di posizione dei PID, visualizzati sulla mappa del sito di lavoro, diventano "arancioni", ovvero se tutti i lavoratori hanno raggiunto l'area sicura e hanno premuto il pulsante di conferma sia del proprio PID che del PID degli attrezzi e mezzi di cui sono responsabili.

Infine, al termine della situazione di pericolo, viene inviato un messaggio dal CSS ai PID i quali riportano lo stato dei led in condizione normale riaccendendo il led verde.

Alternativamente, ai fini della sperimentazione, abbiamo testato una soluzione che prevede l'utilizzo di un pic-

- 4 colored LEDs (red, green, yellow and orange) and a confirmation button;
- a piezoelectric buzzer;
- an inertial measurement unit (IMU).

Initially, the PID was only equipped with an audible alarm, which was activated during an emergency phase and was interrupted when the worker went to position himself in a safe area carrying all the tools and controlling the moving parts of the work machines. Subsequently, after the execution of a Hazard Analysis, it was identified that there was a risk that the worker might accidentally find himself in the safe area and not notice the alarm due to the use of noisy working tools such as a rail-saw or noise-cancelling headphones. Therefore, the authorization of the passage of the train by the site manager, having received the safe position, could have induced a risk of accident in the event that the worker, not realizing the alarm, had casually invade the dangerous area, for example to get around a work vehicle or bulky objects placed on the rails of the interrupted track.

Reason for which, it was decided to add luminous LEDs, through which to inform the worker of his status and a confirmation button, which is only activated within the safe area, with the following operation (see graphic representation Fig. 5):

1. the red light warns the worker that he must move to a safe area carrying any tools/vehicles;
2. the yellow light denotes that the worker is in a safe area and must therefore press the confirmation button on both his PID and the button on the vehicle he is using, in order to ensure that the worker is aware of the situation;
3. the orange light shows that the worker has pressed the buttons;
4. finally, the green light signals to the worker that the train has passed and the dangerous situation has ended.

Regarding the alarm conditions, we would like to point out that, at the moment, there are no plans to use SEMOR separate from the ATWS and that, consequently, the visual

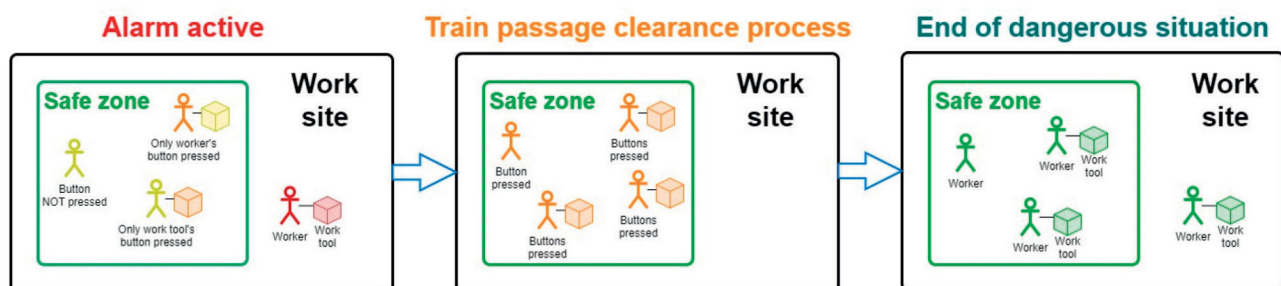


Figura 5 – Schema rappresentativo colori LED del PID. Nella figura l'omino rappresenta il PID associato all'operaio mentre il cubo raffigura il PID posizionato sull'attrezzo/mezzo di lavoro.

Figure 5 – Representative LED color scheme of the PID. In the figure, the little man represents the PID associated with the worker, while the cube represents the PID located on the tool/vehicle.

colo schermo touchscreen, Fig. 6, con il medesimo funzionamento dei led, per quanto riguarda lo stato dei colori.

Questo strumento consente una maggiore elasticità grazie alla possibilità di implementare schermate di servizio che avvisano l'operatore incaricato con brevi messaggi informativi.

Per esempio, la Fig. 7 (a), mostra una schermata viola che avvisa il lavoratore che è in corso la creazione di un'area sicura, mentre la Fig. 7 (b), viene visualizzata nel momento in cui si attiva l'allarme per l'imminente approccio di un treno.

Le due soluzioni proposte sono intercambiabili e parallele: mentre i LED si dimostrano più robusti per un funzionamento in campo e più adatti ad essere posizionati sui mezzi di lavoro, con il display, invece, si ha la possibilità di fornire più informazioni, in quanto ogni schermata colorata ha anche un titolo e una didascalia che spiegano lo stato attuale.

Infine, tra le altre caratteristiche, il PID utilizza una batteria, ricaricabile tramite cavo USB, tale da far sì che la carica duri circa 12 ore, tenendo in considerazione il fatto che il consumo avviene principalmente durante l'allarme per il passaggio del treno, mentre in condizioni normali si trova in stato di attesa e invia solo un segnale di vitalità: l'*heartbeat*.

Questi messaggi di vitalità vengono inviati periodicamente per verificare che la connessione sia ancora funzionante. Il periodo predefinito è impostato, per la attuale fase prototipale, su 10 minuti ma è modificabile.

Il dispositivo CSS riceve il segnale di vitalità da ogni dispositivo connesso e verifica che tutti siano correttamente in funzione; nel caso in cui un dispositivo attivato non venisse più rilevato ne verrebbe data segnalazione tramite CCS all'agente avvisatore che avrebbe il tempo di gestire la sostituzione del dispositivo. Nel caso in cui il guasto dovesse presentarsi all'attivazione di una condizione di allarme per treno in approccio, non verrebbe garantita l'autorizzazione al passaggio del treno fino al ripristino delle condizioni sicure. Se da una sperimentazione in campo dovesse risultare che 10 minuti di frequenza per il segnale di vitalità non fossero sufficienti, sarà possibile rimodularlo.

I dispositivi sono dotati di sistema inerziale che rileva i più piccoli movimenti: nei casi in cui lo stato di "immobilità" perdurasse per un tempo superiore a 5 secondi (intervallo di tempo impostabile in fase di configurazione), verrebbe inviato un allarme a CCS. Questo per evidenziare eventuali malesseri del personale e l'allontanamento del lavoratore dal dispositivo.

6. CSS

Il visualizzatore, adoperato dall'agente avvisatore, è una applicazione ElectronJS che gira su ambiente Chromium.



Figura 6 – Prototipo PID con touchscreen.
Figure 6 – PID prototype with touchscreen.

and acoustic alarm systems of the ATWS itself are still active on the site.

The CSS only shows the covering agent the authorized status of the train passage if all the PIDs' position indicators, displayed on the work site map, turn "orange", i.e. if all the workers have reached the safe area and have pressed the button confirmation of both their own PID and the PID of the equipment and vehicles for which they are responsible.

Finally, at the end of the dangerous situation, a message is sent from the CSS to the PIDs which return the status of the LEDs to normal condition by turning on the green LED again.

Alternatively, for experimentation purposes, we tested a solution that involves the use of a small touchscreen, Fig. 6, with the same operation as the LEDs, as regards the status of the colors.

This tool allows greater flexibility thanks to the possibility of implementing service screens that alert the operator in charge with short information messages.

For example, the Fig. 7 (a), depicts a purple screen that shows to the worker that the creation of a safe area is in progress, while the Fig. 7 (b), is displayed when the alarm goes on for the imminent approach of a train.

The two solutions proposed are interchangeable and parallel: while the LEDs prove to be more robust for field operation and more suitable for placement on work vehicles, with the display, on the other hand, there is the possibility of providing more information, as each coloured screen also has a title and caption explaining the current status.

Finally, among other features, the PID uses a battery, rechargeable via USB cable, such as to ensure that the charge lasts about 12 hours, taking into consideration the fact that consumption occurs mainly during the alarm for the passage of the train, while under normal conditions it is in a waiting state and only sends a signal of vitality: the *heartbeat*.

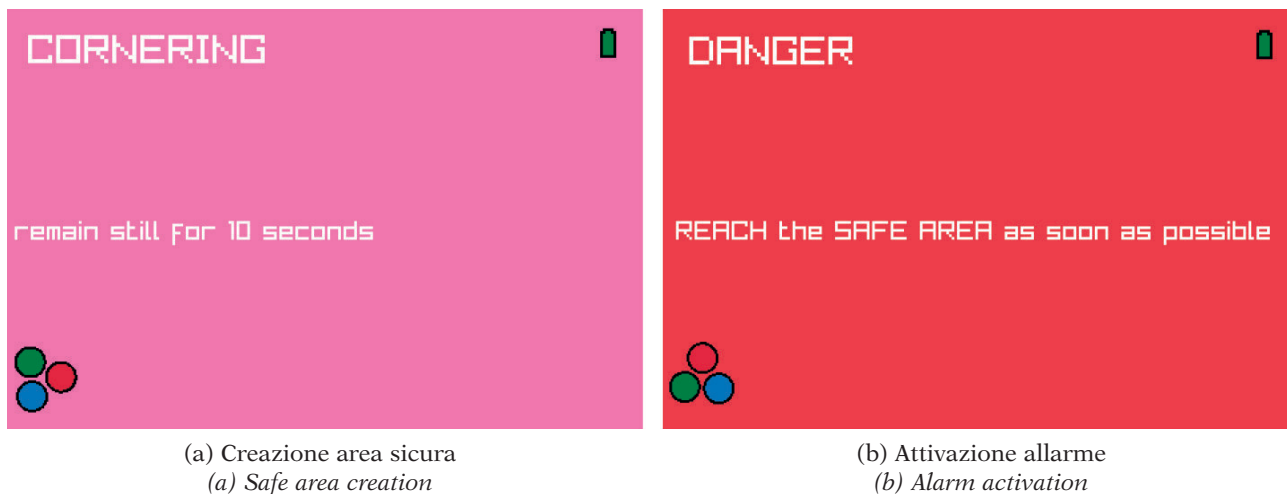


Figura 7 – Schermate sul PID.
Figure 7 – Screen on the PID.

È stata sviluppata utilizzando il linguaggio di programmazione JavaScript e HTML e fa uso di OpenStreetMap tramite l'API Openlayers e GeoJSON. Inoltre è un eseguibile stand-alone, il che significa che non è necessario alcun altro software per poter essere eseguito.

L'applicazione, vedi Fig. 8, comunica con un database per recuperare tutte le informazioni di cui ha bisogno e per interagire con i PID.

Il DBMS (DataBase Management System), basato su PostgreSQL 13 è un sistema di database open source relazionale a oggetti, sviluppato sul linguaggio di programmazione SQL:2016 (Structured Query Language).

Il protocollo di comunicazione si basa sul protocollo TCP/IP e sui principi del PVS [9], il Protocollo Vitale Standard di RFI. Dispone di una protezione crittografica ottenuta mediante le specifiche AES (Advanced Encryption Standard) e AES-CMAC (Advanced Encryption Standard-Cipher-based Message Authentication Code) [17].

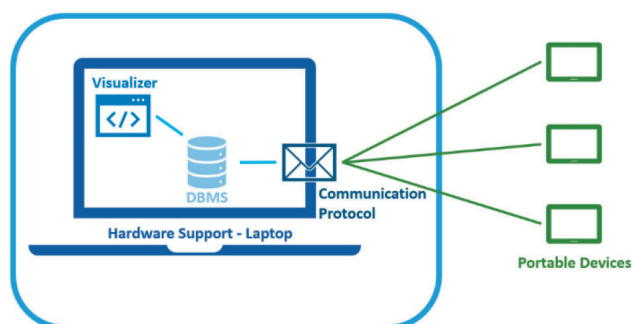


Figura 8 – Schema relativo alla comunicazione tra CSS, PID e database.

Figure 8 – Scheme relating to the communication between CSS, PID and database.

These vitality messages are sent periodically to verify that the connection is still functional. The default period is set to 10 minutes but is editable.

The CSS device receives the signal from each connected device and verifies that all are functioning correctly; in the event that an activated device was no longer detected, it would be reported via CCS to the alerting agent who would have time to manage the replacement of the device. In the event that the fault was to occur on activation of an alarm condition for a train on approach, there would be no guarantee that the train would be allowed to pass until safe conditions were restored. If field experimentation were to show that 10 minutes of frequency for the vitality signal was not sufficient, it would be possible to reschedule it.

The devices are equipped with an inertial system that detects the smallest movements: in cases where the state of "stillness" lasts for more than 5 seconds (time interval that can be set during configuration), an alarm would be sent to CCS. This is to highlight any staff discomfort and removal of the worker from the device.

6. CSS

The visualiser, used by the site manager, is an ElectronJS application running on a Chromium environment.

It was written using the JavaScript and HTML programming language and makes use of OpenStreetMap via the Openlayers API and GeoJSON.

Furthermore, it is a stand-alone executable, which means that no other software is required to run it.

The application, see Fig. 8, communicates with a database to retrieve all the information it needs and to interact with the PIDs.

The DBMS (DataBase Management System) based on PostgreSQL 13, is an object-relational, open source data-

La GUI (Graphical User Interface) del CSS, mostrata in Fig. 9, è caratterizzata dalla presenza di tre cerchi rotanti, uno blu, uno rosso e uno verde, disposti nell'angolo in basso a sinistra.

Questi cerchi servono come misura di sicurezza, affinché l'agente avvisatore sia sicuro che lo schermo non sia bloccato, che tutto funzioni correttamente e che i colori relativi allo stato dei PID siano congruenti col messaggio che devono proporre.

Sul visualizzatore vengono mostrati:

- la mappa dell'area di lavoro;
- l'elenco e lo stato dei dispositivi collegati;
- l'area sicura;
- le posizioni trasmesse dai PID, rappresentate da un pallino di diversi colori a seconda della situazione in cui si trovano.

L'agente avvisatore, attraverso l'applicazione, può: disegnare le aree sicure, attivare lo stato di allarme e autorizzare automaticamente il passaggio del treno se collegato ai sistemi di segnalamento oppure autorizzarlo manualmente in caso di assenza di interfaccia diretta.

Fino a quando esiste un lavoratore o un attrezzo in posizione non sicura o se almeno un operatore non ha confermato la "consapevolezza" premendo il bottone di tutti i PID di cui è responsabile, l'interfaccia grafica non solo evidenzia i suddetti lavoratori e/o mezzi, ma mostra automaticamente una segnalazione di allarme per richiamare l'attenzione dell'agente avvisatore.

Inoltre, è sufficiente che un solo PID segnali uno stato di "pericolo" (led rosso o giallo sul PID e indicatore rosso o giallo sul CSS), che l'allarme a video venga immediatamente e automaticamente attivato.

Da sottolineare che l'allarme acustico e luminoso emesso dall'ATWS rimane comunque attivo fino al termine del transito del treno a prescindere dalla posizione sicura o meno dei lavoratori, per cui lo stato di pericolo viene continuamente segnalato.

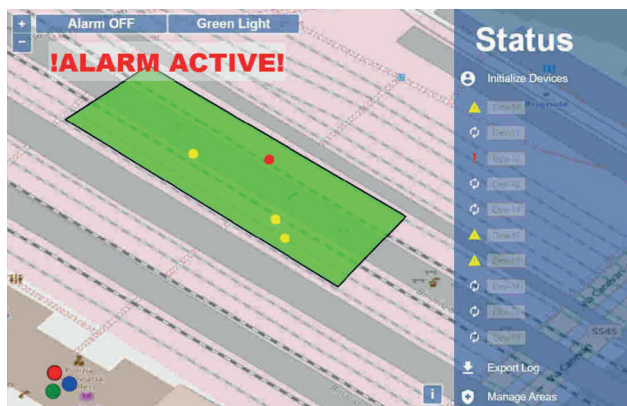


Figura 9 – L'interfaccia grafica.
Figure 9 – The GUI.

base system, developed on the SQL:2016 (Structured Query Language) programming language.

The communication protocol is based on the TCP/IP protocol and on the principles of the PVS [9], the RFI's Standard Vital Protocol.

It has cryptographic protection using the AES (Advanced Encryption Standard) and AES-CMAC (Advanced Encryption Standard-Cipher-based Message Authentication Code) specifications [17].

The CSS GUI (Graphical User Interface), shown in Fig. 9, is characterized by the presence of three rotating circles, one blue, one red and one green, arranged in the lower left corner.

These circles serve as a safety measure, so that the site manager can be sure that the screen is not locked, that everything is working properly and that the colors relating to the status of the PIDs are congruent with the message they are supposed to propose.

The display shows:

- the map of the working area;
- the list and status of the connected devices;
- the safe area;
- the positions transmitted by the PIDs, represented by a dot of different colours according to the situation they are in.

The site manager, through the application, can: draw the safe areas, activate the alarm status and automatically authorize the passage of the train if connected to the signaling systems or authorize it manually if there is no direct interface.

As long as there is a worker or equipment in an unsafe position, or if at least one of them has not confirmed "awareness" by pressing the button of all PIDs for which he/she is responsible, the graphical interface not only highlights the aforementioned workers and/or equipment, but automatically displays an alarm signal to draw the attention of the covering agent.

Furthermore, it is sufficient for a single PID to signal a 'danger' state (red or yellow LED on the PID and red or yellow indicator on the CSS), that the on-screen alarm is immediately and automatically activated.

It should be emphasized that the acoustic and luminous alarm emitted by the ATWS remains active until the end of the train's transit regardless of whether the workers are in a safe or unsafe position, so that the state of danger is continuously signaled.

In detail, Fig. 9 depicts a situation in which the alarm is active and shows workers and/or vehicles (represented with yellow dots) which, for privacy reasons are associated with an identifier, are all within the safe area but have not yet pressed the button.

In addition, a PID can be seen depicted instead with a red dot and marked with an exclamation mark in the

Nel dettaglio, la Fig. 9, descrive una situazione in cui l'allarme è attivo e mostra lavoratori e/o mezzi (rappresentati con dei pallini gialli) che, per questioni di privacy sono associati a un identificativo, i quali si trovano tutti all'interno dell'area sicura ma non hanno ancora premuto il pulsante.

Per di più, si può notare un PID raffigurato, invece, con il pallino rosso e segnalato con un punto esclamativo nello "Status" (la barra laterale). Tale circostanza si verifica quando, per un qualsiasi motivo, il PID genera un errore.

La successiva Fig. 10 mostra tutti i passi del processo visualizzati sullo schermo del CCS.

Al termine della giornata lavorativa, alla chiusura del software, l'agente avvisatore può decidere se salvare tutti i log, provvisti di un *timestamp*, generati dai PID.

Il sistema è sviluppato in modo tale che il file dei logs sia protetto da accessi, modifiche o cancellazioni non au-

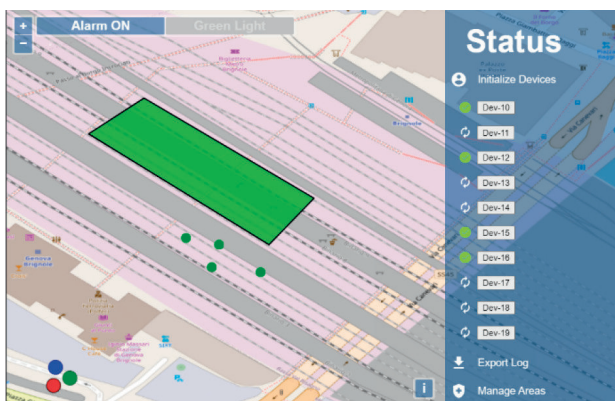
"Status" (the sidebar). This occurs when, for whatever reason, the PID generates an error.

The Fig. 10 below show all the process steps displayed on the CSS screen.

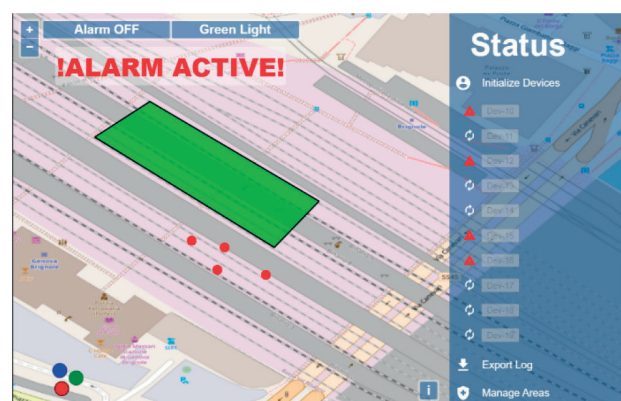
At the end of the working day, when closing the software, the covering agent can decide whether to save all logs, with a timestamp, generated by the PIDs.

The system is developed in such a way that the logs file is protected against unauthorized access, modification or deletion. The information can only be read by authorized persons.

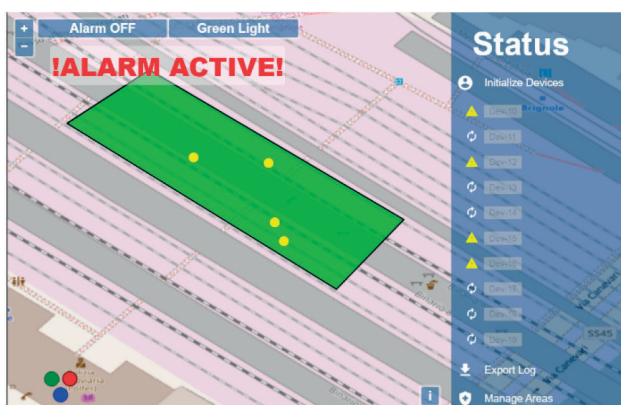
The association between the PID and the identity of the associated operator, is stored, but, for privacy purposes, is not accessible to the employer: it can only be provided to the bodies in charge of investigating incidents and is automatically removed from the system if, at the end of the work session, its storage is not requested with adequate justification.



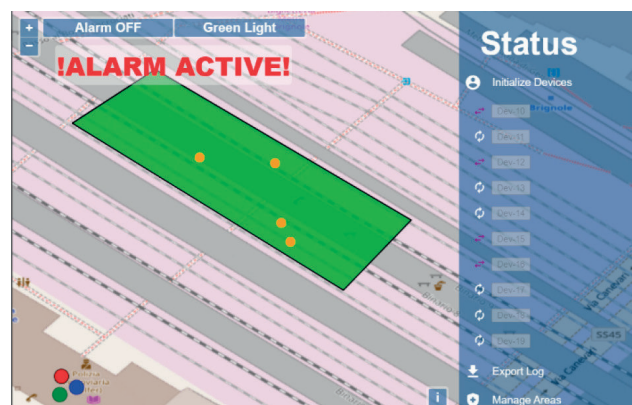
a) operatori in assenza di treni in arrivo
a) operators in the absence of arriving trains



b) attivazione dell'allarme "treno in arrivo"
b) activation of the "arriving train" alarm



c) gli operatori non hanno ancora effettuato il riconoscimento premendo i pulsanti
c) operators have not yet acknowledged by pressing the buttons



d) operatori hanno effettuato il riconoscimento
d) operators have acknowledged but the train has not yet passed so the alarm remains active

Figura 10 – Passaggi completi del processo visualizzati sullo schermo del CCS.

Figure 10 – Process steps displayed on the CSS screen.

torizzate. Le informazioni, infatti, possono essere lette solo da chi è autorizzato.

L'associazione fra Identificativo del PID e identità dell'operatore associato, viene memorizzata, ma, ai fini della privacy, non è accessibile al datore di lavoro: può essere fornita solo agli enti preposti alle indagini in caso di incidente e viene automaticamente rimossa dal sistema se, alla chiusura della sessione lavorativa non viene richiesta la sua conservazione con adeguata giustificazione.

7. Test

Il prototipo software è stato validato attraverso alcuni test funzionali preliminari, che hanno ampiamente ricoperto i requisiti specificati in fase di progetto e di *Hazard Analysis*.

Lo scopo dei test è stato quello di verificare il corretto funzionamento del CSS, dei PID e del database, e di valutare la qualità della sicurezza del posizionamento.

Per esaminare il funzionamento delle differenti parti del sistema, sono stati svolti test sia di laboratorio che sul campo.

I primi hanno analizzato il software utilizzando 10 differenti PID configurati e connessi al Sistema di Supervisione Centrale (CSS) tramite la stessa rete.

Le principali funzionalità verificate sono:

- la corretta inizializzazione e la piena capacità computazionale richiesta del dispositivo CSS;
- le prestazioni del sistema (tempo di prima attivazione e connessione con la Stazione di Riferimento, tempi di scambio delle informazioni fra CSS e PID);
- il mantenimento della vitalità da parte del CSS e dei PID durante tutto il ciclo operativo;
- il corretto comportamento della procedura di creazione della zona sicura;
- la procedura di messa in sicurezza dei lavoratori in caso di avvicinamento del treno, tramite l'attivazione manuale della "Modalità Allarme";
- il corretto comportamento in sicurezza del sistema nel caso in cui un dispositivo PID smetta di funzionare.

I test sul campo, invece, hanno impiegato 3 PID reali e hanno avuto luogo presso il sito sperimentale di RFI, ovvero il Circuito San Donato a Bologna, vedi Fig. 11.

Tutti i test eseguiti hanno dato esito positivo. Per quanto riguarda i test relativi all'attivazione automatica dell'allarme e alla procedura per attivare, tramite CSS, l'autorizzazione del passaggio di un treno in avvicinamento (o il mantenimento dello stato di via impedita) non sono stati effettuati in quanto non è stato possibile, al momento, realizzare un'interfaccia diretta con il sistema ATWS o con un sistema di segnalamento. SEMOR è comunque predisposto per scambio informativo tramite protocollo sicuro PVS: la visualizzazione dell'indicazio-

7. Test

The software prototype was validated through some preliminary functional tests, which largely covered the requirements specified in the design and Hazard Analysis phase.

The purpose of the tests was to verify the correct functioning of the CSS, the PIDs and the database, and to assess the quality of positioning security.

To examine the functioning of the different parts of the system, both laboratory and field tests were carried out.

The former analyzed the software using 10 different PIDs configured and connected to the Central Supervisory System (CSS) via the same network.

The main functionalities tested are:

- *the correct initialization and full required computational capacity of the CSS device;*
- *system performance (time of first activation and connection with the Reference Station, time of information exchange between CSS and PID);*
- *the maintenance of vitality by the CSS and the PIDs throughout the operating cycle;*
- *the correct behavior of the safe zone creation procedure;*
- *the procedure for securing workers in case of approaching the train, through the manual activation of the "Alarm Mode";*
- *the correct safety behavior of the system in case a PID device stops working.*

The field tests, on the other hand, used 3 real PIDs and took place at RFI's experimental site, the San Donato Circuit in Bologna, see Fig. 11.

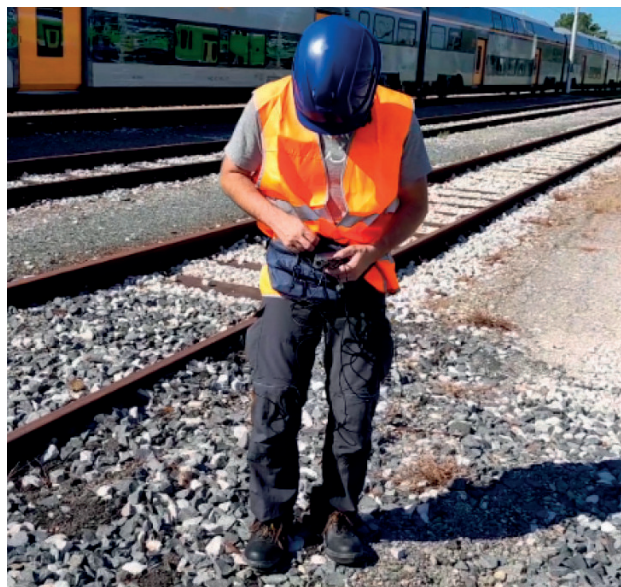


Figura 11 – Test localizzazione PID.
Figure 11 – PID localization test.

ne per l'autorizzazione del passaggio del treno (operazione che al momento, in assenza di interfaccia diretta, può essere effettuata solo manualmente) avviene correttamente.

Inoltre, sono stati effettuati i test sul posizionamento GNSS confrontando le due soluzioni GPS RTK e Galileo PPP, utilizzate dal software.

I test hanno avuto luogo in ambiente reale presso la stazione di Genova Brignole, durante una giornata soleggiata, approfittando della presenza di un cantiere su un marciapiede.

Il sito di test risulta di particolare interesse in quanto presenta sia ostacoli e interferenze aeree, quali palificazioni, tralicci e funi di contatto dell'alimentazione, Fig. 12, sia aree con buona visibilità.

Oltre a ciò, spostandosi verso il centro della banchina vi è una copertura, che può essere utilizzata come ostacolo architettonico alla visibilità satellitare al fine di simulare la riduzione dei satelliti disponibili.

Tale sito di test ha permesso quindi di avere, inizialmente, buone condizioni di ricezione del segnale da parte dei PID e successivamente uno scenario più difficile.

Il test, di tipo cinematico, ha previsto la registrazione dei dati grezzi ed il calcolo delle due soluzioni parallele.

La soluzione GPS-RTK è risultata piuttosto stabile e completa nel tempo.

Il *time to first fix*, ovvero il tempo di attivazione del sistema, preliminare all'avvio delle operazioni nel cantiere e necessario a fissare le ambiguità e ad ottenere quindi un posizionamento con precisione inferiore ai 10 cm è, in generale, entro i 40 secondi.

Da questo valore, che può variare tra pochi secondi e diversi minuti, dipende la velocità di messa in opera del dispositivo PID che non influenza in alcun modo la normale operatività di SEMOR ai fini dell'individuazione delle posizioni una volta che il ricevitore è entrato a regime.

All tests performed were positive. Tests relating to the automatic activation of the alarm and the procedure for activating, via CSS, the authorization of the passage of an approaching train (or the maintenance of the impeded status) were not carried out as it was not possible, at the moment, to implement a direct interface with the ATWS system or with a signaling system. However, SEMOR is set up for information exchange via a secure PVS protocol: the display of the indication for authorizing train passage (an operation that at the moment, in the absence of a direct interface, can only be carried out manually) occurs correctly.

In addition, GNSS positioning tests we carried out by comparing the two GPS RTK and Galileo PPP solutions used by the software.

The tests took place in a real environment at the Genova Brignole station, during a sunny day, taking advantage of the presence of a working site on a sidewalk.

The test site is of particular interest as it presents both obstacles and aerial interference, such as piling, pylons and power supply contact cables, Fig. 12, and areas with good visibility.

Furthermore, moving towards the center of the quay there is a cover, which can be used as an architectural obstacle to satellite visibility in order to simulate the reduction of available satellites.

This test site therefore made it possible to initially have good signal reception conditions by the PIDs and subsequently a more difficult scenario.

The kinematic test involved the recording of the raw data and the calculation of the two parallel solutions.

The GPS-RTK solution was found to be quite stable and complete over time.

The time to first fix, i.e. the system activation time, prior to the start of operations at the site and necessary to fix ambiguities and thus achieve positioning with an accuracy of less than 10 cm, is generally within 40 seconds.

From this value, which can vary between a few seconds and several minutes, depends the speed at which the PID device is set up, which in no way influences the normal operation of SEMOR for the purpose of locating positions once the receiver has become fully operational.

In the most complicated sections, the solution switches to FLOAT, still showing deviations of the order of 10 cm from the actual position.

The difference between the FIX and FLOAT solution from an algorithmic point of view, consists in the fact that the unknown representing the number of wavelengths between the satellite and the receiver, is set to an integer value or a decimal value. In the former



Figura 12 – Zona critica per la visibilità satellitare nell'area di prova.
Figure 12 – Critical zone for satellite visibility in the test area.

Nei tratti più complicati la soluzione passa a FLOAT, evidenziando comunque scostamenti dell'ordine di 10 cm rispetto alla posizione reale.

La differenza tra soluzione FIX e FLOAT da un punto di vista algoritmico, consiste nel fatto che l'incognita rappresentante il numero di lunghezze d'onda tra satellite e ricevitore, venga fissata ad un valore intero o ad un valore decimale. Nel primo caso l'incertezza sulla misura dell'istanza satellite-ricevitore è molto bassa e la precisione del posizionamento raggiunge i pochi centimetri, mentre nel secondo aumenta.

La soluzione PPP evidenzia, invece, un periodo di inizializzazione decisamente più alto, in ogni caso accettabile per un'attivazione di cantiere, in quanto si rimane sempre entro i 3 minuti.

Bisogna precisare, infatti, che durante l'attivazione dei sistemi di localizzazione, viene effettuata l'attivazione e l'associazione dei PID ai lavoratori e ai mezzi adoperati, operazione che richiede tempi sicuramente più elevati, dei 3 minuti evidenziati sopra.

Riguardo la completezza dei risultati è necessario segnalare che nei tratti di maggiore complessità, dove sono presenti strutture aeree in acciaio, il posizionamento presenta dei "buchi" in cui non è possibile calcolare la posizione.

In alcune aree, infatti, le distanze delle soluzioni rispetto alla traiettoria reale sono più ampie, ed in particolare la distanza della soluzione PPP è maggiore di 50 cm.

L'errore relativo fra i due sistemi satellitari risulta comunque entro la fascia prefissata di accettabilità prevista dai requisiti SEMOR [18], con un errore medio fra i due sistemi nell'ordine di 10 cm e quindi inferiore al tetto globale stabilito per l'errore. Nel caso in cui tale errore fosse superiore ai 50 cm, SEMOR è in grado di avviare fornendone avviso all'agente avvisatore e ridefinendo in modo più restrittivo il confine dell'area sicura. In tale modo il livello di sicurezza del sistema rimane comunque immutato a discapito dell'ampiezza dell'area sicura.

Osservando le due figure la Fig. 13 (a) e Fig 13 (b), che riportano una porzione di dati raccolti dal ricevitore, risulta evidente come, nel medesimo arco temporale, i dati grezzi della soluzione Galileo PPP, vedi Fig. 13 (b), si dilatano maggiormente nello spazio rendendo la soluzione meno precisa.

Per risalire alle cause dell'aumento dell'errore di localizzazione è stata effettuata un'analisi delle condizioni al contorno che hanno generato tale anomalia analizzando i dati grezzi ovvero quei dati dai quali non sono ancora state ricavate le coordinate finali.

Il rapporto segnale rumore (SNR) evidenzia un calo di precisione dei valori in corrispondenza dei tratti in cui il posizionamento PPP e RTK hanno maggiori difficoltà.

In particolare, dallo studio dei grafici di ogni singolo satellite, è stato possibile dedurre che il suddetto calo è piuttosto generalizzato e ciò indica una forte relazione tra

case, the uncertainty of the satellite-receiver instance is very low and the positioning accuracy reaches a few centimetres, while in the latter it increases.

The PPP solution, on the other hand, shows a much higher initialization period, which is in any case acceptable for a site activation, as it always remains within 3 minutes.

It must be pointed out, in fact, that during the activation of the localization systems, the activation and association of the PIDs to the workers and the vehicles used is carried out, an operation that certainly takes longer than the 3 minutes highlighted above.

With regard to the completeness of the results, it is necessary to point out that in the most complex sections, where there are overhead steel structures, the positioning has 'holes' where it is not possible to calculate the position.

In some areas, in fact, the distances of the solutions with respect to the real trajectory are larger, and in particular the distance of the PPP solution is greater than 50 cm.

The relative error between the two satellite systems is nevertheless within the set band of acceptability envisaged by SEMOR requirements [18], with an average error between the two systems in the order of 10 cm and therefore below the global ceiling established for error. In the event that this error is greater than 50 cm, SEMOR is able to remedy this by providing notice to the covering agent and redefining the boundary of the safe area more restrictively. In this way, the safety level of the system remains unchanged at the expense of the width of the safe area.

Observing the two figures Fig. 13 (a) and Fig 13 (b) which show a portion of the data collected by the receiver, it is evident how, in the same time frame, the raw data of the Galileo PPP solution, see Fig. 13 (b), expands more spatially, making the solution less accurate.

In order to trace the causes of the increase in localization error, an analysis of the boundary conditions that generated this anomaly was carried out by analyzing the raw data, i.e. those data from which the final coordinates have not yet been derived.

The signal-to-noise ratio (SNR) shows a drop in the accuracy of the values at the locations where PPP and RTK positioning have the most difficulty.

In particular, from studying the graphs of each satellite, it was possible to deduce that the aforementioned drop is rather generalized, indicating a strong relationship between the presence of local infrastructures, such as poles and portals, and the degradation of the signal itself.

In support of this, a clear increase in multipath effects can be seen at the same intervals, Fig. 14. Multipath is a lengthening of the signal path from the satellite to the receiver due to reflection phenomena on surfaces close to the receiver itself.

In any case, considering that, near the problem areas, the number of satellites, both GPS and Galileo, increases, as evident from Fig. 15, given the very low value of Position DoP (Dilution of Precision), it can be inferred that the

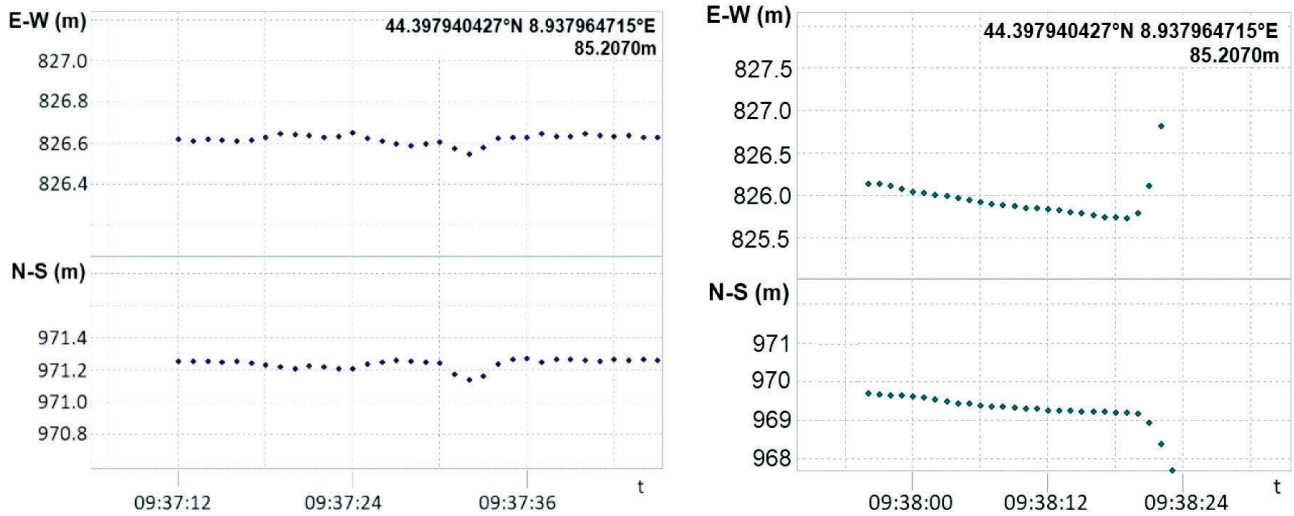


Figura 13 – a) Soluzione GPS RTK - b) Soluzione Galileo PPP.
Figure 13 – a) GPS RTK solution - b) Galileo PPP solution.

la presenza di infrastrutture locali, quali pali e portali, e il degrado del segnale stesso.

A sostegno di ciò, in corrispondenza dei medesimi intervalli, si può notare un evidente aumento degli effetti di *multipath*, Fig. 14. Il *multipath* è un allungamento del percorso del segnale proveniente dal satellite al ricevitore per effetto di fenomeni di riflessione su superfici prossime al ricevitore stesso.

Ad ogni modo, considerato che, in prossimità delle aree problematiche, il numero di satelliti, sia GPS che Galileo, aumenta, come evidente da Fig. 15, dato il valore

number of satellites is not the cause of the problem. The DoP is the index of satellite geometric robustness, as it defines the number of satellites relative to the more or less uniform distribution in the sky above the receiver.

For more detail, a further analysis was performed on the presence of cycle slips (cycle jumps on the electromagnetic signal, generally induced by obstruction or electromagnetic disturbance effects), which have a direct impact on the SNR (signal-to-noise ratio) value.

Fig. 16, depicts, through different colors, the signal strength for each satellite (green optimum quality, purple

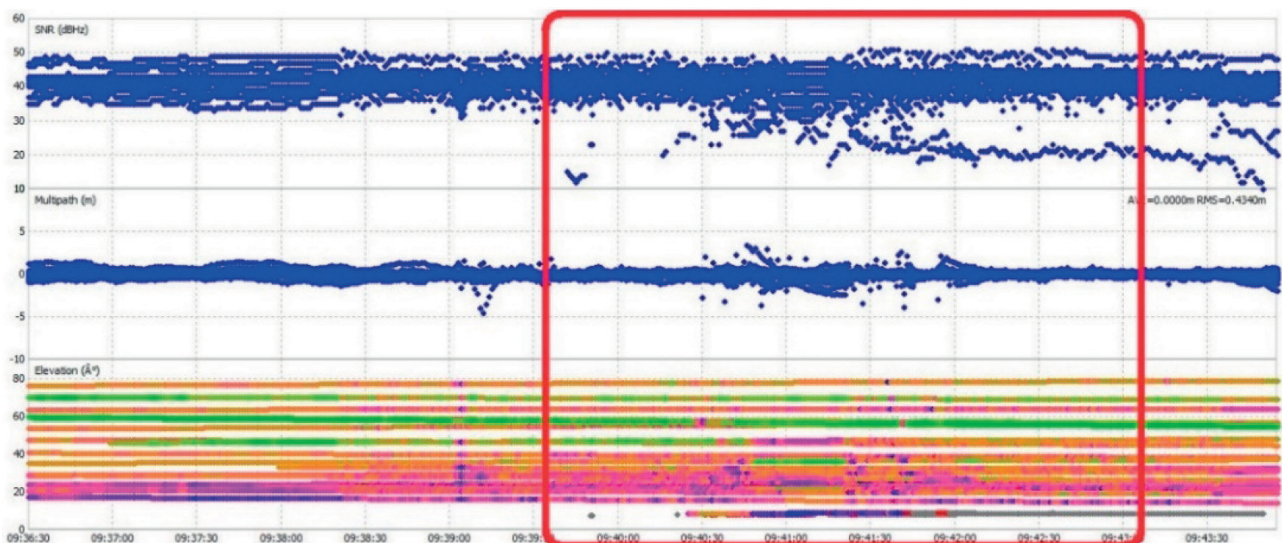


Figura 14 – Effetti di multipath.
Figure 14 – Effects of multipath.

molto basso del Position DoP (*Dilution of Precision*), si può evincere che il numero degli stessi non è la causa del problema. Il DoP è l'indice di robustezza geometrica satellitare e definisce il numero di satelliti relativamente alla distribuzione più o meno uniformemente nel cielo, al di sopra del ricevitore.

Per maggiori dettagli, è stata eseguita un'ulteriore analisi relativa alla presenza di *cycleslips* (salti di ciclo sul segnale elettromagnetico, generalmente indotti da ostruzione o effetti di disturbo elettromagnetico), che hanno un impatto diretto sul valore di SNR (rapporto segnale rumore).

La Fig. 16, rappresenta, attraverso differenti colori, l'intensità di segnale per ciascun satellite (verde qualità ottima, viola qualità scarsa). Nell'intervallo di tempo corrispondente alla zona ove sono presenti elementi di disturbo, è possibile notare, come la frequenza dei *cycleslips* (indicati da linee rosse verticali) aumenta in maniera considerevole. Questo significa che per brevi periodi di tempo il segnale viene meno e anche se il ricevitore riesce a ricucirlo, si crea rumore e il relativo errore.

Individuata la causa, è stato quindi possibile intervenire sul software al fine di migliorare la qualità delle soluzioni: l'algoritmo utilizza infatti l'MDP (*Multipath Detection Parameter*), un parametro capace di rilevare e mitigare le osservabili interessate da *multipath*. In caso di *multipath* in entrata la variabile MDP dovrebbe evidenziare valori anomali e grazie ad un diverso peso attribuito all'MDP, l'algoritmo sviluppato consente di ridurre il peso delle osservabili affette da disturbo durante il calcolo delle coordinate. Per fare ciò viene utilizzato un valore di soglia, implementato dinamicamente, che si adatta automaticamente alle osservabili stesse e alle condizioni dell'ambiente circostante.

poor quality). In the time interval corresponding to the area where noise elements are present, it can be seen that the frequency of cycle slips (indicated by vertical red lines) increases considerably. This means that for short periods of time, the signal is lost and even if the receiver manages to patch it up, noise and the associated error are created.

Having identified the cause, it was then possible to intervene on the software in order to improve the quality of the solutions: the algorithm in fact uses the MDP (*Multipath Detection Parameter*) a parameter capable of detecting and mitigating the observables affected by multipath. In the case of incoming multipath, the MDP variable should show abnormal values, and thanks to a different weight given to the MDP, the algorithm developed makes it possible to reduce the weight of the observables affected by multipath during the calculation of the coordinates. To do this, a dynamically implemented threshold value is used, which automatically adapts to the observables themselves and the conditions of the surrounding environment.

Finally, the results of the experimentation were used to assess the quality of the behavior of the IMU, for which, already in the design phase, it had been decided not to use it as a third location method, but only for the purpose of verifying the static or motion condition of the PID, as difficulties had emerged in its operation.

The tests of the IMU, used in the prototype, have in fact revealed a number of problems, proving the correctness of the choices made during the design phase.

The first concerns a strong instability of the timestamp. The difference between the two successive instants at which the measurement is taken does not guarantee a constant value. This justifies the generation of synchronization difficulties between the IMU and the GNSS.

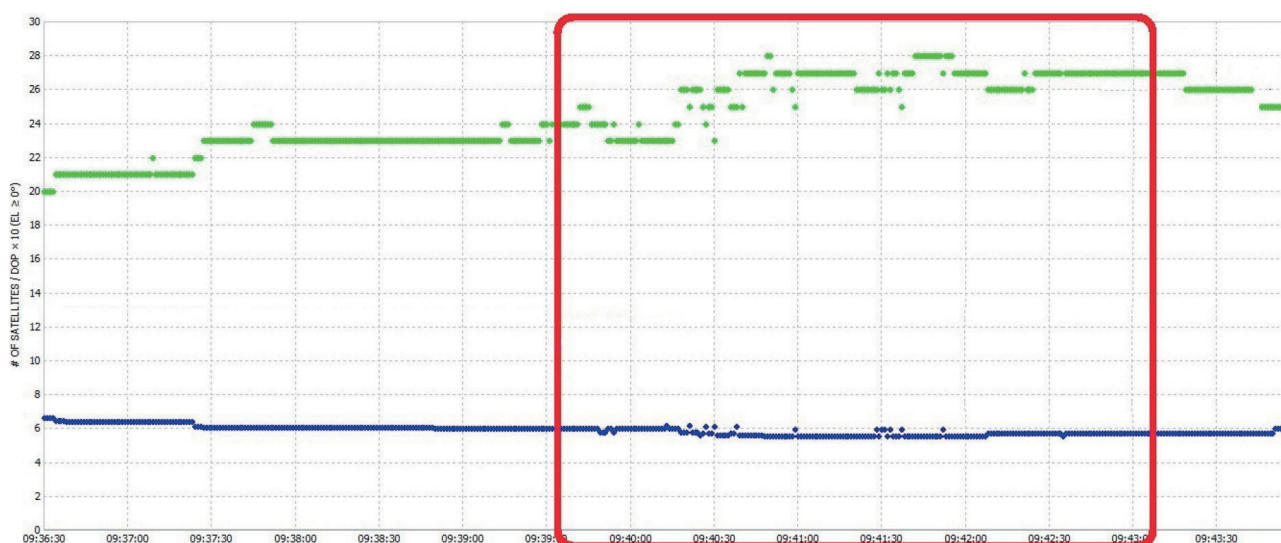


Figura 15 – Numero di satelliti in vista (in verde) e andamento del Position DOP (in blu).
Figure 15 – Number of satellites in sight (green) and Position DOP trend (blue).

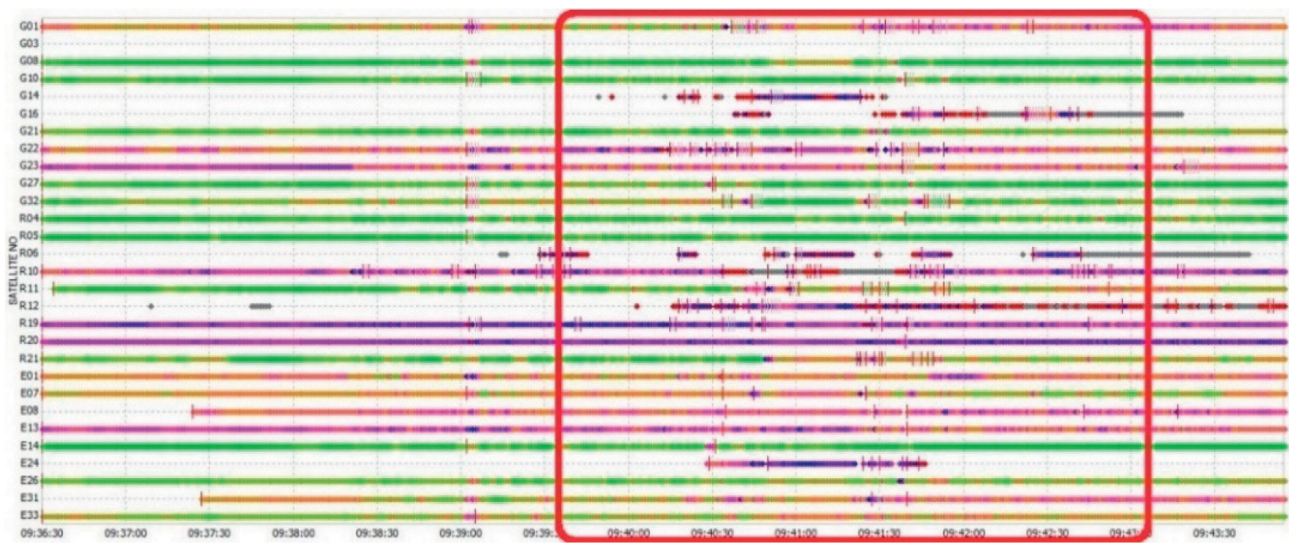


Figura 16 – Rappresentazione dei cycleslips per ogni satellite.
Figure 16 – Representation of the cycleslips for each satellite.

I risultati della sperimentazione sono infine stati utilizzati per valutare la qualità del comportamento della IMU, per la quale, già in fase di progettazione, si era optato per un utilizzo non come terzo metodo di localizzazione, ma solo ai fini della verifica della condizione statica o di moto del PID essendo emerse difficoltà nel suo funzionamento.

I test della IMU, impiegata nel prototipo, hanno infatti evidenziato alcuni problemi a riprova della correttezza delle scelte effettuate in fase di progetto.

Il primo riguarda una forte instabilità del *timestamp*. La differenza tra i due istanti successivi in cui è effettuata la misura non garantisce un valore costante. Ciò giustifica la generazione di difficoltà nella sincronizzazione tra la IMU e il GNSS.

Il secondo problema, invece, è causato dal fatto che il dispositivo è soggetto a una deriva molto precoce. Con deriva s'intende l'errore di misura dell'IMU ottenuto come somma incrementale degli errori che si accumulano nel tempo causati dalla procedura di calcolo utilizzata dal dispositivo. Queste imprecisioni, se non corrette, si sommano a errori significativi che tendono a far divergere l'errore totale e quindi le stime di localizzazione molto rapidamente.

Pertanto, per garantire l'accuratezza delle letture del sensore diventa necessario aggiornare periodicamente la posizione generata dalla stessa, utilizzando i dati provenienti dal RTK e dal PPP. Tuttavia, come mostrato in Fig. 17, nelle situazioni più problematiche, dove anche questi sistemi hanno difficoltà a produrre risultati (assenza delle linee arancione per il GPS e blu per il Galileo) diventa impossibile re-inizializzare la IMU (tratto verde), la cui deriva diverge in modo irrecuperabile.

The second problem is caused by the fact that the device is subject to very early drift. Drift refers to the IMU measurement error obtained as the incremental sum of errors that accumulate over time caused by the calculation procedure used by the device. These inaccuracies, if not corrected, add up to significant errors that tend to make the total error and thus the location estimates diverge very quickly.

Therefore, to ensure the accuracy of the sensor readings, it becomes necessary to periodically update the position generated by the sensor using data from the RTK and PPP. However, as shown in Fig. 17, in the most problematic situations, where even these systems have difficulty producing results (absence of the orange lines for GPS and blue lines for Galileo), it becomes impossible to reinitialize the IMU (green line), the drift of which diverges irretrievably.

8. Conclusion

SEMOR addresses and improves safety-critical aspects of railway working sites.

The use of SEMOR integrates into the procedures defined by the Instruction for Working site Protection 1986 edition reprinted in 2014, with particular regard to what is indicated in article 12 thanks to integration with current ATWS systems.

In particular, it fills the main gap in the functional scenario for the protection of working sites by ATWS where all steps are now performed by high integrity technologies, from the stopping and restarting of trains on approach to the activation of acoustic and luminous alarms, but it is currently not possible to ensure the same level of integrity for the decision of the covering agent who must guarantee the safe status of each worker and vehicle under his or her individual responsibility.

8. Conclusione

SEMOR affronta e consente di migliorare aspetti critici per la sicurezza dei cantieri ferroviari.

L'uso di SEMOR si integra nelle procedure definite dall'Istruzione per la Protezione Cantieri edizione 1986 ristampa 2014, con particolare riguardo a quanto indicato nell'articolo 12 grazie all'integrazione con gli attuali sistemi ATWS.

Viene, in particolare, colmata la lacuna principale dello scenario funzionale per la protezione dei cantieri tramite ATWS dove tutti gli step sono ad oggi eseguiti tramite tecnologie ad elevato livello di integrità, dall'arresto e ripartenza dei treni in approccio alle attivazioni degli allarmi acustici e luminosi, ma non è al momento possibile assicurare lo stesso livello di integrità per la decisione dell'agente avvisatore che deve garantire sotto sua responsabilità individuale lo stato sicuro di ciascun lavoratore e mezzo di lavoro.

SEMOR, tramite il CSS, permette all'agente avvisatore di visualizzare in tempo reale la posizione precisa dei lavoratori e dei mezzi e di riconoscere lo stato di ciascuno di essi. In questo modo diventa possibile automatizzare il fonogramma/modulo M100 con cui l'agente avvisatore concede il nulla osta al transito del treno superando eventuali errori di valutazione dovuti al fattore umano e permettendogli di gestire in sicurezza l'attività sul campo senza l'impatto sulla circolazione dei treni.

Il sistema è applicabile sia su linee a doppio binario con il cantiere sul binario interrotto, sia su cantieri fuori dal binario quando esiste il rischio di interferire con la sagoma del treno (Art.10.1. b [2]).

La realizzazione di un interfacciamento con i sistemi di segnalamento consentirebbe di utilizzare SEMOR anche per la reintroduzione dell'Art. 16 dalla IPC [2], ad oggi soppresso.

L'ex Art. 16, nel caso di attività da realizzare in tempi molto rapidi, consentiva la protezione del cantiere con solo avvistatore; ipotizzando tempo nullo per la liberazione del cantiere che veniva gestito senza la necessità di installare barriere fisiche o tantomeno utilizzare segnali per fermare il treno.

Queste deroghe non sono più accettabili dall'attuale IPC che non contempla l'avvistamento tramite operatore umano e rende obbligatori per tale tipologia di attività l'utilizzo di un occupatore sicuro (pedale) e l'uso di barriere fisiche o di segnali.

Ad oggi per poter tornare ai vantaggi dell'ex Art.16 serve:

1. ricevere dall'impianto l'informazione di treno in avvicinamento senza installare occupatori;
2. gestire la liberazione in sicurezza dell'area cantiere con modulo M100 in modo automatico;
3. concedere il via libera al treno abilitando le attuali logiche del segnalamento.

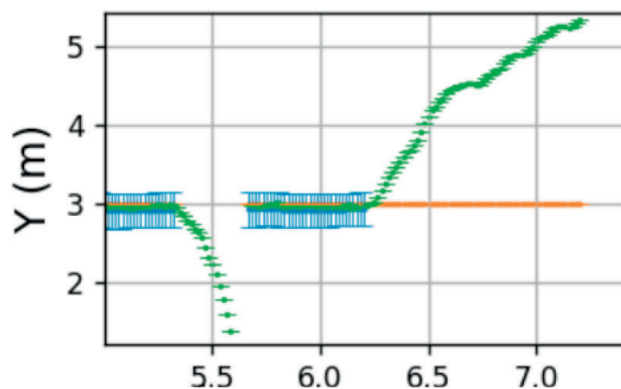


Figura 17 – Deriva degli errori di misura dell'IMU rispetto alle localizzazioni satellitari: GPS (tratto arancione), PPP (tratto blu) e IMU (tratto verde).

Figure 17 – Derivation of IMU measurement errors from satellite localizations: GPS (orange), PPP (blue) and IMU (green).

SEMOR, through the CSS, allows the alerting agent to view in real time the precise location of the workers and vehicles and to recognize the status of each of them. In this way, it becomes possible to automate the phonogram/M100 form with which the alerting agent grants clearance for the transit of the train, overcoming possible errors of judgement due to the human factor and allowing him to safely manage the activity in the field without the impact on the circulation of trains.

The system is applicable both on double-track lines with the yard on the interrupted track, and on off-track yards when there is a risk of interfering with the train gauge (Art.10.1. b [2]).

The implementation of an interface with the signaling systems would also allow SEMOR to be used for the reintroduction of Art. 16 from the IPC [2], which has now been abolished.

The former Art. 16, in the case of activities to be carried out in a very short time, allowed the protection of the yard with only a spotter; assuming zero time for the release of the yard, which was managed without the need to install physical barriers or even use signals to stop the train.

These exceptions are no longer acceptable under the current IPC, which does not contemplate human operator sighting and makes the use of a safe occupant (pedal) and the use of physical barriers or signals compulsory for this type of activity.

To date, in order to return to the benefits of the former Art. 16, it is necessary to:

1. *receive from the system the information of an approaching train without installing occupants;*
2. *manage the safe release of the yard area with the M100 module in automatic mode;*

L'implementazione di SEMOR, permetterebbe quindi di ripristinare i vantaggi dell'ex Art.16. A tale scopo sarebbe sufficiente un'applicazione semplificata di SEMOR: un tablet in grado di integrare le funzionalità del CCS, collegato ai PID dei suoi collaboratori in linea. SEMOR riceverebbe gli allarmi per il treno in approccio, genererebbe automaticamente un'area di ricovero sicuro limitrofa alla posizione degli operatori e l'avvisatore potrebbe visualizzare la propria posizione e quella dei collaboratori che raggiungono e si posizionano nell'area sicura. La possibilità di arrestare il treno in caso di pericolo al momento non è attivabile (in assenza di ATWS collegato a segnali di protezione), ma lo diventerà quando verrà introdotta un'interfaccia diretta con il segnalamento (ACC delle stazioni limitrofe).

In merito all'implementazione di SEMOR, i test effettuati nel sito sperimentale di San Donato e presso la stazione ferroviaria di Genova Brignole dimostrano l'efficacia di quanto realizzato evidenziando però alcuni problemi riguardanti la precisione della geolocalizzazione, ma non la quantificazione dell'errore e quindi la sicurezza della gestione dell'area sicura. Tali problemi sono causati principalmente da fenomeni di riflessione prodotti da strutture metalliche, specie pali e portali, che provocano alcuni difetti alle serie temporali generate da PPP ma superati globalmente grazie al peso della precisione garantita dall'RTK.

Per tale motivo, anche se i rilievi del Galileo PPP hanno dato risultati meno precisi nei tratti più complessi, ai fini dell'integrità della soluzione, la posizione finale può considerarsi comunque precisa e robusta e compatibile con il livello di integrità per la sicurezza del sistema (attualmente SEMOR è sviluppato applicando i requisiti CENELEC per il SIL2, ma l'obiettivo è di arrivare a realizzare un prodotto SIL4), visto che complessivamente l'errore è risultato essere minore di 10 cm anche in condizioni disturbate.

Riguardo gli sviluppi futuri, è previsto che venga adottato, appena sarà reso disponibile, il nuovo servizio Galileo HAS (*High Accuracy Service*). Con HAS sarà possibile migliorare la soluzione prodotta dai satelliti Galileo ottenendo un errore di posizionamento inferiore a due decimetri grazie alla trasmissione gratuita di correzioni PPP attraverso il segnale Galileo E6-B.

Concludiamo ricordando che l'obiettivo del progetto SEMOR, è quello di assicurare la robustezza della localizzazione in area di cantiere anche nelle zone con scarsa visibilità delle costellazioni satellitari (zone di montagna) o prive (gallerie).

Per ovviare a tali carenze è già avviato un nuovo progetto ESA NAVISP che introduce nel sistema l'utilizzo di tecniche di mappatura 3D integrate con altri metodi di localizzazione per supportare la localizzazione satellitare anche in aree critiche.

9. Partner

Il presente articolo descrive l'attività sviluppata nell'ambito del programma NAVISP di ESA (Agenzia Spazia-

3. *to give the go-ahead to the train by enabling the current signaling logic.*

The implementation of SEMOR would therefore make it possible to restore the benefits of the former Art. 16. For this purpose, a simplified application of SEMOR would be sufficient: a tablet capable of integrating the functionalities of the CCS, connected to the PIDs of its employees on the line. SEMOR would receive the alarms for the approaching train, would automatically generate a safe shelter area adjacent to the position of the operators, and the dispatcher would be able to display his own position and that of the co-workers reaching and positioning themselves in the safe area. The ability to stop the train in the event of danger is currently not possible (in the absence of ATWS connected to protective signals), but will become so when a direct interface with signaling (ACC of neighboring stations) is introduced.

With regard to the implementation of SEMOR, the tests carried out at the San Donato experimental site and at the Genoa Brignole railway station demonstrate the effectiveness of what has been achieved, highlighting, however, some problems concerning the precision of geolocation, but not the quantification of the error and therefore the safety of safe area management. These problems are mainly caused by reflection phenomena produced by metal structures, especially poles and portals, which cause some faults in the time series generated by PPP, but which are globally overcome thanks to the weight of precision guaranteed by RTK.

For this reason, although the Galileo PPP measurements gave less precise results in the more complex sections, for the integrity of the solution, the final position can still be considered precise and robust and compatible with the system's SIL level of integrity for system safety (currently SEMOR is developed applying CENELEC requirements for SIL2, but the goal is to achieve a SIL4 product), since overall the error was less than 10 cm even in disturbed conditions.

With regard to future developments, it is planned that the new Galileo HAS (High Accuracy Service) will be adopted as soon as it is made available. With HAS, it will be possible to improve the solution produced by the Galileo satellites by achieving a positioning error of less than two decimeters thanks to the free transmission of PPP corrections via the Galileo E6-B signal.

Let us conclude by recalling that the objective of the SEMOR project is to ensure the robustness of site localization even in areas with poor visibility of satellite constellations (mountainous areas) or without (tunnels).

To overcome these shortcomings, a new ESA NAVISP project is already underway that introduces the use of 3D mapping techniques integrated with other localization methods into the system to support satellite localization even in critical areas.

9. Partners

This article describes the activity developed within the ESA (European Space Agency) NAVISP programme [19] by

le Europea) [19] da Si Consulting e dai suoi partner nel progetto rappresentati dagli autori dell'articolo stesso.

Nell'ambito del progetto di ricerca, Si Consulting [20], società di consulenza operante nel settore tecnologico degli impianti ferroviari e urbani, è stata Prime Contractor mentre RFI - Rete Ferroviaria Italiana [21], LEVEL Systems [22], azienda ceca che opera nella localizzazione GPS e Gter [23], che opera nella gestione dei dati geografici e spaziali, sono stati subcontraenti.

Le opinioni presentate nel documento rappresentano esclusivamente l'opinione degli autori e non necessariamente il punto di vista dell'ESA.

Si Consulting and its partners in the project represented by the authors of the article.

Within the framework of the research project, Si Consulting [20], a consultancy company operating in the technological sector of railway and urban facilities, was Prime Contractor while RFI - Rete Ferroviaria Italiana [21], LEVEL Systems [22], a Czech company operating in GPS localization and Gter [23], operating in geographical and spatial data management, were subcontractors.

The opinions presented in the paper represent solely the views of the authors and not necessarily the views of ESA.

BIBLIOGRAFIA - REFERENCES

- [1] Agenzia Nazionale per la Sicurezza Ferroviaria (ANSF), *"Riordino delle norme di esercizio che regolamentano i regimi di esecuzione dei lavori all'infrastruttura ferroviaria e delle attività di vigilanza e di controllo della stessa"*. Edizione del 12/2010. Decreto n. 16/2010.
- [2] Rete Ferroviaria Italiana - Gruppo Ferrovie dello Stato Italiane (1986), *"Istruzione per la Protezione dei Cantieri operanti sull'infrastruttura ferroviaria italiana"*.
- [3] Rete Ferroviaria Italiana - Gruppo Ferrovie dello Stato Italiane (2004), *"Linee Guida per la Protezione Cantieri"*. RFI DMALG IFS 001 A.
- [4] Rete Ferroviaria Italiana - Gruppo Ferrovie dello Stato Italiane (2008), *"Linee guida per la protezione cantieri con l'utilizzo dei sistemi ATWS e delle barriere mobili"*. RFI DMA SIGSLG ATWS 02 0.
- [5] European Committee for Standardization (2017), *"Railway applications - Track - Safety protection on the track during work - Part 2-1: Common solutions and technologies - Technical requirements for Track Warning Systems (TWS)"*. CENELEC, EN 16704-2-1:2017 edition, 2017.
- [6] International Electrotechnical Commission (IEC) (2010), *"Functional Safety of electrical, electronic and programmable electronic (E/E/PE)safety-related systems"*. IEC 61508 Edition 2.
- [7] International Electrotechnical Commission (IEC) (2017), *"Safety instrumented systems for the process industry"*. IEC 61511 Edition 2.
- [8] P. SALMON, N.A. STANTON, G. WALKER (2003), *"Human Factors Design Methods Review"*. HFIDTC/WP1.3.2/1.
- [9] European Committee for Electrotechnical Standardization (2018), *"Railway applications - Communication, signalling and processing systems - Safety related electronic systems for signalling"*. CENELEC, EN 50129:2018.
- [10] European Committee for Standardization (2016), *"Railway applications - Track - Safety protection on the track during work"*. CENELEC, EN 16704:2016.
- [11] UNI EN ISO9001 - Criteria for quality assurance in design development, installation and assistance.
- [12] UNI EN ISO 9000-3 - Guide for quality assurance in design development, installation and assistance for SW.
- [13] EN 50126 - Railway Applications - The Specification and Demonstration of Dependability, Reliability, Availability, Maintainability and Safety (RAMS).
- [14] EN 50128 - Railway Applications: Software for Railway Control and Protection Systems.
- [15] EN 50129 - Railway Applications: Safety-related Electronic Railway Control and Protection Systems.
- [16] Si Consulting - Analisi del Rischio. Protezione Cantieri.
- [17] Relazione Tecnica "Protocollo Vitale Standard" RFI DTCDNSSS RT IS 05 021 E del 20\02\2012.
- [18] Si Consulting. WP400 - D4 - REQUIREMENTS SPECIFICATION.
- [19] European Space Agency. <https://www.esa.int/>.
- [20] Si Consulting. <https://www.siconsulting.biz/>.
- [21] RFI - Rete Ferroviaria Italiana. <https://www.rfi.it/>.
- [22] LEVEL Systems. <https://www.level.systems/>.
- [23] Gter. <https://www.gter.it/>.