

Principali tecnologie per la sicurezza della circolazione

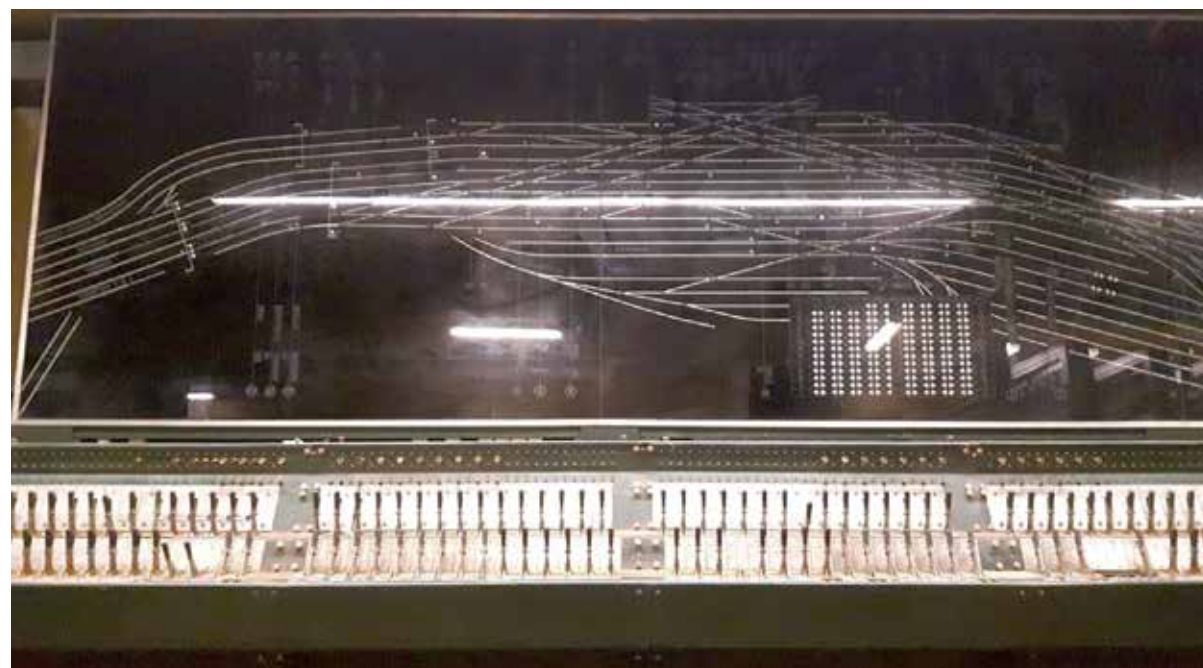
Sono qui illustrate alcune delle peculiarità specifiche del sistema ferroviario, con particolare riferimento alle soluzioni tecnologiche ad esso applicate

Il sistema ferroviario potrebbe sembrare caratterizzato da un consistente grado di semplicità intrinseca, potrebbe pertanto stupire il fatto che, contrariamente alle apparenze, il sistema ferroviario abbia da un lato adottato, in ciascuna epoca (il primo viaggio in treno risale al 1825), alcune tra le tecnologie più avanzate che il periodo storico ha messo a disposizione. Il presente articolo illustra alcune delle peculiarità specifiche del sistema ferroviario, con particolare riferimento alle soluzioni tecnologiche ad esso applicate.

Il binario: origini, vantaggi e conseguenze

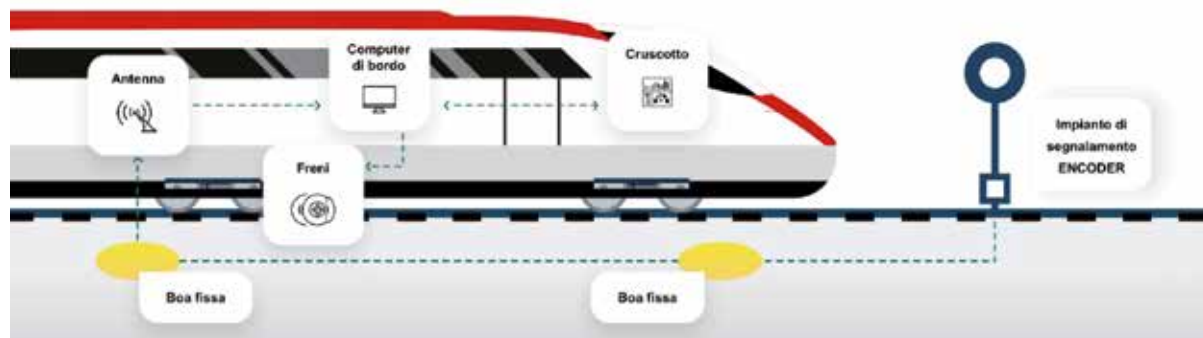
La principale motivazione alla base dell'introduzione della strada ferrata è riconducibile al fatto che, inventate le macchine a vapore come prime e inizialmente uniche sorgenti di energia meccanica e volendole utilizzare per trainare veicoli, fu necessario ricorrere ad una "strada" composta da due rotaie come unico modo per sopportare il notevole peso

per asse di tali enormi caldaie. C'è però un'ulteriore motivazione che ha condotto all'utilizzo del binario e che rende ancor'oggi attuale, dopo quasi 200 anni dalla sua nascita, il trasporto ferroviario: la notevolissima riduzione degli sforzi di trazione permessa dalla bassa aderenza delle rotaie in ferro, che ammontano di fatto solamente ad un decimo di quelli caratteristici del trasporto automobilistico. Ciò comporta una consistente efficienza energetica del trasporto su ferro, che è di dieci volte superiore a quella del trasporto aereo e automobilistico ed è battuta solo dall'efficienza delle navi portacontainer, di circa venti volte superiore, e ancor più da quella delle superpetroliere. Le rotaie in ferro, all'origine dell'elevata efficienza energetica del trasporto ferroviario, hanno però un rovescio della medaglia: così come infatti esse permettono di trainare veicoli con ridotti consumi energetici grazie alla bassa aderenza offerta, per il medesimo motivo impediscono di ottenere sforzi e distanze di frenatura paragonabili a quelli del trasporto su strada.



**Banco a leve del vecchio
ACELI di Roma Termini
(fonte Gruppo FS).**

**Architettura dell'SCMT
(fonte RFI).**



Ciò comporta che, mentre un veicolo stradale può generalmente frenare nello spazio di visuale libera, questo risulta impossibile per un treno, caratterizzato da spazi di frenatura decisamente superiori. Divenne così necessario provvedere, in origine con agenti e successivamente con dispositivi tecnologici via via più evoluti, a segnalare ai macchinisti, con adeguato anticipo (anche di diversi chilometri a seconda della velocità e delle caratteristiche di frenatura del treno nonché della geometria della linea), la necessità di attivare il sistema di frenatura del treno per ridurre la velocità o arrestarsi. Ciò condusse alla necessità di attrezzare l'infrastruttura ferroviaria con impianti di sicurezza e segnalamento di cui ci occuperemo nei prossimi paragrafi.

Gli impianti di segnalamento e sicurezza

Come accennato sopra, a causa dei consistenti spazi di frenatura generalmente molto superiori alla distanza di visibilità libera, nelle ordinarie condizioni di esercizio i treni non circolano con marcia a vista come le automobili, ma lo fanno basandosi sulle indicazioni fornite ai macchinisti dai segnali luminosi disposti in linea e nelle stazioni oppure riportate in cabina di guida su opportuni monitor facenti parte della cosiddetta Driver-Machine Interface o DMI. Tali indicazioni concedono al macchinista la cosiddetta Autorizzazione al Movimento ossia gli comunicano se il tratto di linea davanti possiede le condizioni di sicurezza necessarie per poter essere impegnato oppure se, mancando tali condizioni, il treno deve essere arrestato.

Le indicazioni di arresto del treno o di riduzione di velocità sono inoltre precedute da indicazioni di avviso adeguatamente anticipate, che comunicano al macchinista la necessità di iniziare ad attivare il sistema di frenatura del treno in vista di un successivo arresto o rallentamento.

I sistemi tecnologici che svolgono tali funzioni sono detti Impianti di Segnalamento e Sicurezza (detti anche Impianti IS) ed erano inizialmente basati su tecnologie di tipo essenzialmente meccanico nei cosiddetti Apparat Centrali Elettrici a Leve Individuali (ACELI) che però non erano di semplice utilizzo e richiedevano negli impianti più complessi un eleva-

to numero di agenti operanti su banchi con centinaia di leve. Ad esempio, l'apparato ACELI di Roma Termini utilizzava un banco con circa 300 leve (vedi figura 1).

Si passò quindi a logiche basate su catene di relè elettromeccanici, nei cosiddetti Apparat Centrali Elettrici a Pulsanti di Itinerario (ACEI), che potevano essere manovrati da un unico operatore che impartiva i comandi di itinerario agendo su un numero ridotto di pulsanti.

Attualmente le logiche di sicurezza dei moderni apparati centrali sono realizzate con calcolatori elettronici, nei cosiddetti Apparat Centrali a Calcolatore, che consentono tra l'altro di implementare funzioni di diagnostica d'impianto molto evolute.

La progressiva applicazione, negli impianti di segnalamento e sicurezza, di tecnologie sempre più avanzate trova la sua intima motivazione, al di là del fisiologico adeguamento al progresso tecnico, nell'esigenza, attraverso l'automatizzazione delle funzioni di sicurezza, di neutralizzare l'errore umano. Gli errori del personale di prima linea con compiti di sicurezza della circolazione (regolatore della circolazione, agente di condotta, agente che manutene gli apparati di sicurezza) hanno infatti un impatto diretto e immediato sulla sicurezza dell'esercizio e rendono quindi necessari sistemi automatici che intervengano in tempo reale per neutralizzarli.

I sistemi automatici di protezione e controllo della marcia: SCMT ed ERTMS

Compito degli impianti di sicurezza e segnalamento è quello di comunicare ai macchinisti dei treni i vincoli di sicurezza da rispettare sulla base dello stato degli enti di binario. Rimarrebbe però ancora un problema di sicurezza: e se il macchinista, ad esempio per errore, decidesse comunque di superare il segnale disposto a via impedita e di accedere col treno ad una sezione già occupata da un altro convoglio provocando così una collisione fra i due?

Compito dei sistemi di protezione e controllo della marcia dei treni, che vedremo nel seguito, è proprio evitare che lo scenario sopra raffigurato si verifichi, provocando automaticamente a tal fine, in caso di mancato rispetto dei vincoli di sicurezza da parte del macchinista, l'intervento del sistema di frenatu-

ra del treno, per ridurre la sua velocità o per arrestarlo a seconda dei casi.

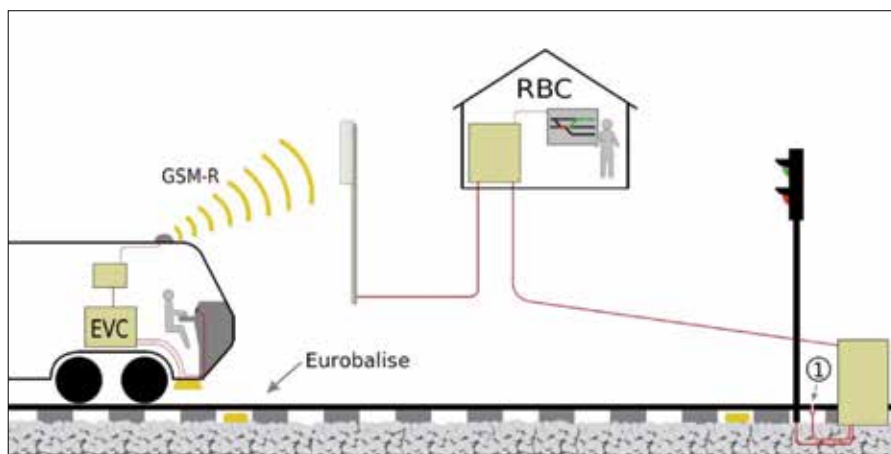
Il sistema SCMT (vedi figura 2), sviluppato in ambito nazionale e installato sulla rete RFI nel primo decennio degli anni 2000, è sostanzialmente composto da un sottosistema di terra formato da encoder, cavi e boe. Gli encoder sono sostanzialmente dei calcolatori che si interfacciano con gli impianti di sicurezza e segnalamento e ricevono in ingresso, da questi ultimi, l'aspetto dei segnali presenti lungo la linea. Sulla base degli aspetti dei segnali, gli encoder stabiliscono lo specifico "telegramma" (composto da una sequenza di bit) da inviare via cavo alle boe disposte sui binari tra le rotaie in corrispondenza dei vari segnali.

Le boe sono delle antenne che, a loro volta, quando il treno vi passa sopra, trasmettono il telegramma ricevuto dagli encoder al sottosistema di bordo. Quest'ultimo è un calcolatore che, sulla base dei telegrammi ricevuti dalle boe, calcola una "curva di frenatura" ed agisce automaticamente sul sistema di frenatura affinché tale curva sia comunque rispettata, anche in caso di errori del macchinista.

L'SCMT è un sistema di protezione della marcia di tipo nazionale adottato solo in Italia, così come negli altri Stati europei ne sono in uso altri ancora diversi. Tale proliferazione di sistemi nazionali determina un consistente pregiudizio per l'interoperabilità ferroviaria, sia da un punto di vista tecnico perché un treno che attraversasse più stati membri dovrebbe avere installati tutti i sottosistemi di bordo dei sistemi di protezione utilizzati in ciascun paese, sia da un punto di vista operativo, poiché il macchinista dovrebbe conoscere le specifiche indicazioni date dai sistemi di segnalamento di ciascuno stato membro. In ambito europeo si decise pertanto di specificare un sistema di controllo della marcia che consentisse di conseguire la piena interoperabilità sia tecnica, prevedendo di installare a bordo un solo sistema tecnologico, che è per l'appunto lo European Railway Traffic Management System (ERTMS), specificato in tre differenti "Livelli".

L'ERTMS Livello 1 ha una architettura sostanzialmente analoga a quella dell'SCMT e prevede che il sottosistema di bordo gestisca la marcia e monitori il rispetto dei relativi vincoli di sicurezza sulla base delle informazioni comunicate dalle boe disposte lungo la linea. L'ERTMS Livello 1, pur consentendo di conseguire una interoperabilità tecnica, non consente tuttavia di conseguire una completa interoperabilità operativa in quanto prevede che si continuino ad utilizzare i segnali laterali nazionali.

L'ERTMS Livello 2 è invece, a differenza del Livello 1, un sistema di tipo continuo essendo i vincoli di marcia comunicati al sottosistema di bordo non più tramite boe disposte sul binario ma via radio, attraverso la rete GSM-R. L'architettura del sistema (vedi figura 3) prevede la presenza di un Radio Block Cen-



tre che riceve in ingresso lo stato di libertà o occupazione delle sezioni di binario davanti al treno e, sulla base di tale stato, calcola e invia al sottosistema di bordo (detto European Vital Computer o EVC), tramite la rete radiomobile GSM-R, i vincoli di marcia da rispettare. L'ERTMS Livello 3, infine, ha una architettura sostanzialmente analoga a quella del Livello 2, con la differenza che, mentre nel Livello 2 la lunghezza del tratto di via libera davanti ad un treno viene calcolata sulla base dello stato di occupazione delle sezioni in cui è suddivisa la linea (composte dai cosiddetti circuiti di binario o CdB), nel Livello 3 tale lunghezza viene calcolata direttamente sulla base della posizione della coda del treno che precede.

L'ERTMS e la sfida della cybersecurity

La necessità di automatizzare sempre più le funzioni che gestiscono la sicurezza della circolazione ferroviaria, ha condotto nel corso degli anni all'introduzione in ferrovia di tecnologie via via più sofisticate, inizialmente basate su logiche di tipo meccanico per poi passare a circuiti a relè e infine ai calcolatori elettronici.

La progressiva diffusione di tecnologie basate su computer ha però un rovescio della medaglia, costituito dal fatto che con tale diffusione è aumentata parallelamente anche la superficie esposta ad attacchi informatici. Benché non sia possibile risalire ad un unico evento che abbia alzato il livello di allarme della comunità dei tecnici ferroviari riguardo ai possibili rischi derivanti dagli attacchi cyber, sicuramente un ruolo determinante in tal senso la ebbe una intervista rilasciata il 24 aprile 2015 dal professor David Stupples, esperto di sistemi di trasmissione elettronici della City University di Londra [1], ripresa anche da alcuni quotidiani nazionali [2].

Nell'intervista, il professor Stupples dichiarò che i nuovi sistemi ferroviari, ed in particolare l'ERTMS, avrebbero potuto essere ingannati da malware che avrebbero ad esempio potuto far credere al sistema di controllo che il treno stesse rallentando mentre in realtà stava accelerando.

Occorre però evidenziare che fortunatamente il si-

Architettura dell'ERTMS Livello 2 (fonte RFI).

Riferimenti internet

[1] <https://www.openaccessgovernment.org/new-rail-system-hacked/16384/>

[2] <https://www.ilgiornale.it/news/cronache/terrorismo-adesso-basta-computer-far-deragliare-treno-1122057.html>

Riferimenti bibliografici

- "Impianti di sicurezza" – Vittorio Finzi – Editore da Coedit

- "Impianti Ferroviari" Volumi I e II – Lucio Mayer – Editore dal Collegio Ingegneri Ferroviari Italiani

- "European Train Control System, Development and implementation in Italy" – Fabio Senesi, Enzo Marzilli – Editore dal Collegio Ingegneri Ferroviari Italiani

- "Dinamica del Veicolo Ferroviario" – Romano Panagin – Editore da Levrotto & Bella

- "Dizionario Ferroviario" – Pier Luigi Guida, Eugenio Milizia – Editore dal Collegio Ingegneri Ferroviari Italiani.

**Sensori di rotaia
in fibra ottica (fonte RFI).**

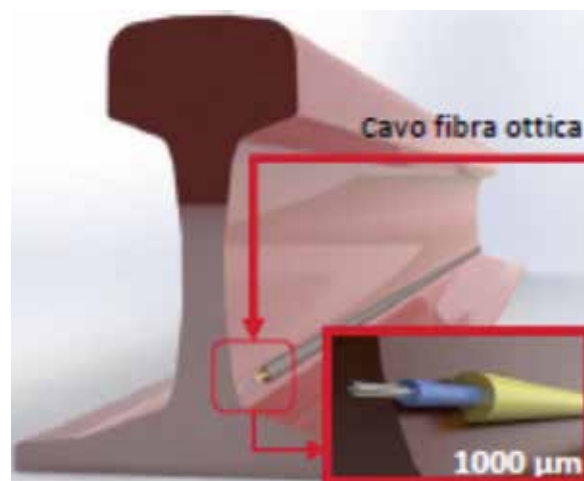
stema, per come specificato, prevede alcuni meccanismi di difesa dagli attacchi cyber, tra cui uno dei principali è l'utilizzo di chiavi crittografiche.

Scopo dell'utilizzo delle chiavi crittografiche nell'ambito dello scambio di informazioni tra due entità ERTMS, tipicamente l'EVC di bordo e l'RBC descritti nei paragrafi precedenti, è garantire che ciascuna delle due entità possa essere sicura che il messaggio che sta ricevendo, ed in base al quale deve attuare le funzioni di sicurezza a cui essa è preposta, provenga realmente dall'altra entità e non invece da un possibile soggetto terzo (il cosiddetto "man in the middle") che fraudolentemente si sia inserito nel canale di comunicazione tra le due entità allo scopo di inviare messaggi ingannevoli.

Per dare un'idea della robustezza dell'algoritmo di cifratura utilizzato nell'ERTMS, si riporta di seguito una tabella coi tempi medi di decrittazione da parte di un malintenzionato che adoperi una tecnica di decifrazione a "forza bruta"

Dalla suddetta tabella appare evidente l'adeguatezza dell'algoritmo di cifratura utilizzato nell'ERTMS, tenuto conto che il tempo di validità di una chiave di sessione ERTMS risulta essere dell'ordine di un'ora! Visto che, da quanto evidenziato sopra, almeno per quanto riguarda le problematiche connesse a eventuali minacce di tipo man in the middle nell'ambito dello scambio di messaggi fra EVC e RBC le preoccupazioni del professor Stupples possono essere ritenute ragionevolmente immotivate, il problema si sposta su un altro fronte: tutto il meccanismo descritto sopra si basa sul fatto che le chiavi segrete configurate negli EVC e RBC rimangano segrete. Il problema diventa quindi come fare a garantire la sicurezza del processo di distribuzione di tali chiavi.

A tal fine sono in corso studi per valutare l'applicazione, all'ERTMS, della cosiddetta "Distribuzione di chiavi quantistiche", o, in inglese, "Quantum key Distribution", ossia un protocollo teorizzato nel 1984 dagli informatici Charles H. Bennett e Gilles Brassard



con lo scopo di risolvere il problema della distribuzione di chiavi segrete tra due soggetti A e B su un canale non sicuro, ad esempio perché soggetto ad intercettazione.

Uno sguardo al futuro: la diagnostica automatica dell'infrastruttura

Le anomalie dell'infrastruttura ferroviaria possono compromettere gravemente la sicurezza della circolazione ferroviaria, sfociando a volte in incidenti tragici.

Attualmente l'integrità dell'infrastruttura viene monitorata soprattutto attraverso controlli periodici eseguiti dal personale (ad esempio visite linea), in alcuni casi anche mediante l'ausilio di treni diagnostici. Tali tipologie di controllo, dato il loro carattere di periodicità, non consentono di rilevare anomalie che si manifestino tra un controllo ed il successivo, con le relative conseguenze sulla sicurezza. Inoltre, ricorrendo sovente ad agenti per la loro effettuazione, tali controlli possono essere suscettibili all'errore umano.

Si stanno però progressivamente diffondendo moderne tecnologie che da un lato consentono di automatizzare il processo di monitoraggio, che viene così reso immune dall'impatto dell'errore umano, e dall'altro di conseguire un monitoraggio continuo dell'infrastruttura sia nel tempo sia nello spazio, che consenta di rilevare in tempo reale l'insorgere di anomalie con possibile impatto sulla sicurezza e di adottare tempestivamente le restrizioni di circolazione necessarie, eventualmente in modo automatico mediante idonee interfacce col sistema di segnalamento.

Negli ultimi due decenni è stato ad esempio sviluppato un numero significativo di tecnologie di rilevamento innovative basate su sensori in fibra ottica (Fiber Optic Sensors o FOS) per il monitoraggio dell'infrastruttura ferroviaria, grazie ai loro vantaggi distintivi intrinseci, come dimensioni ridotte, leggerezza, immunità alle interferenze elettromagnetiche e alla corrosione (vedi figura 4).

Architettura	Tempo medio decrittazione
Singolo microprocessore (Pentium 4)	$2,5 \times 10^{16}$ anni
HW dedicato (Deep Crack)	$1,6 \times 10^{13}$ anni
Network di PC su Internet (106 elementi)	$2,5 \times 10^{10}$ anni
Singolo microprocessore (nel 2010)	$2,8 \times 10^{15}$ anni
HW dedicato (nel 2010)	$1,8 \times 10^{12}$ anni
Network di PC su Internet (10^7 elementi, nel 2010)	$1,6 \times 10^8$ anni
Singolo microprocessore (nel 2020)	$2,8 \times 10^{13}$ anni
HW dedicato (nel 2020)	$1,8 \times 10^{10}$ anni
Network di PC su Internet (10^8 elementi, nel 2020)	$1,6 \times 10^5$ anni