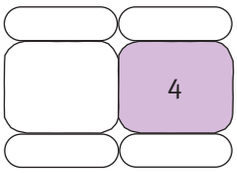
SISTEMI DI CONTROLLO PER L'ALTA VELOCITÀ FERROVIARIA

Francesco Flammini

Da alcuni anni siamo abituati a viaggiare a bordo dei treni cosiddetti ad Alta Velocità (AV), il cui movimento è gestito da un sistema di controllo che sintetizza i risultati di decenni di ricerche in ambito ICT. In particolare, si tratta del primo sistema ferroviario in Italia (e non solo) a sostituire i segnali luminosi con segnali "virtuali", ovvero realizzati tramite pacchetti dati trasmessi su reti wireless. In quest'articolo descriveremo il funzionamento del sistema AV, cogliendo l'occasione per illustrare i concetti fondamentali che accomunano i moderni sistemi di controllo ferroviario.



1. INTRODUZIONE

Le infrastrutture di trasporto su rotaia, incluse ferrovie, tranvie e metropolitane, sono percepite come uno dei segni tangibili del livello di civilizzazione di un territorio, riuscendo a spostare notevoli masse di individui attraverso zone rurali o urbane con un livello di capillarità elevato, una maggiore sicurezza rispetto al trasporto su gomma e un ridotto impatto ambientale, dovuto essenzialmente alla trazione elettrica (assenza di gas di scarico) e alla possibilità di installazione *underground*, con una conseguente riduzione del traffico stradale in superficie.
Allo scopo di rendere la sicurezza di tali sistemi meno dipendente dalla supervisione umana – per sua natura fallibile, come testimoniato dai tragici episodi di cronaca anche recente [1] – è in atto negli ultimi decenni una transizione dai tradizionali meccanismi di segnalazione luminosa (che vanno interpretati dai macchinisti) ai moderni sistemi di controllo computerizzati (*computer-based*) basati su segnali virtuali, interpretabili in modo autonomo dal sistema di controllo di bordo.

Bisogna dire che anche la gestione delle tradizionali logiche di segnalamento, finalizzate essenzialmente ad attivare i segnali luminosi e muovere i deviatoi (noti ai più come "scambi"), si sta spostando progressivamente da una realizzazione tramite relè (dispositivi elettromeccanici) a sistemi computerizzati cosiddetti di "gestione della via" (o *interlocking*). Affinché l'automazione sia completa, però, anche la trasmissione dei segnali da terra a bordo deve essere realizzata attraverso sistemi di elaborazione e comunicazione dati digitali. Questo è ciò che avviene nei sistemi di *Automatic Train Protection* (ATP), in cui è il sistema di bordo a ricevere i segnali virtuali e ad attivare automaticamente la frenatura in caso di pericolo. Tali segnali sono trasmessi attraverso opportuni pacchetti dati che contengono, tra le altre informazioni, la distanza che il treno è autorizzato a percorrere in modo sicuro e le limitazioni di velocità della tratta. Infine, nei sistemi di *Automatic Train Control* (ATC), abbastanza diffusi negli impianti metropolitani (si veda per esempio, la nuova Linea C di Roma [2]), la funzionalità

di ATP è complementata da quella di *Automatic Train Operation* (ATO), che è in grado di far muovere il treno senza l'intervento del macchinista, consentendo quindi di realizzare sistemi completamente *driverless* (senza conducente).
Il moderno standard ERTMS/ETCS (*European Railway Traffic Management System / European Train Control System*) [3] appartiene alla categoria dei sistemi ATP evoluti: pur non prevedendo una parte ATO, la velocità del treno è supervisionata dal sistema al punto tale che il macchinista deve soltanto seguire le indicazioni che compaiono sulla strumentazione di bordo, ovvero sul *cockpit* DMI (*Driver Machine Interface*; Figura 1). Tale standard, nato con lo scopo di migliorare prestazioni, sicurezza, affidabilità e interoperabilità delle linee ferroviarie transeuropee, è stato adottato in Italia su tutte le nuove linee AV, in cui sono completamente assenti i tradizionali segnali luminosi. Pertanto, la marcia a vista da parte del macchinista non è consentita se non in condizioni di degrado (esempio, malfunzionamento di alcuni apparati) e ad una velocità molto ridotta (poche decine di km/h). D'altronde, a velocità elevate (fino a 300 km/h) il macchinista non avrebbe alcuna possibilità di interpretare visivamente un segnale laterale reagendo per tempo ad eventuali situazioni di pericolo, dal momento che lo spazio medio di frenatura per l'arresto completo del treno è dell'ordine dei chilometri. Si tratta quindi di una classe di sistemi di controllo che appartengono alla categoria *real-time safety-critical* [4]: un eventuale malfunzionamento (che può essere anche un ritardo nella risposta del sistema) può avere conseguenze catastrofiche in termini di incolumità dei passeggeri oltre che di danni all'ambiente circostante. Attualmente esistono diverse linee ferroviarie basate sullo standard ERTMS/ETCS già in esercizio in Europa (con l'Italia tra i pionieri, con la tratta AV Roma-Napoli attivata nel Dicembre 2005 [5]) e numerosi progetti in corso nel resto del mondo, per un investimento totale che copre quasi 40.000 km, realizzati da consorzi che comprendono le aziende Ansaldo STS, Alcatel, Alstom, Bombardier, Invensys Rail e Siemens [3].

FIGURA 1

Un cockpit DMI ERTMS/ETCS (Fonte: <http://upload.wikimedia.org/wikipedia/commons/e/e9/F%C3%BChrerstand_ICE_1_ETCS.jpg)

2. DESCRIZIONE GENERALE

In questo e nei paragrafi che seguono verranno descritte nel dettaglio l'architettura e le funzionalità del sistema Alta Velocità, che, come anticipato, si basa sullo standard europeo ERTMS/ETCS. Come vedremo, la trattazione consentirà di approfondire molti aspetti che si applicano in generale ai moderni sistemi di controllo e segnalamento ferroviario [6].
Al fine di spiegare in modo chiaro i principi di funzionamento del sistema ATP è opportuno innanzitutto introdurre il concetto di "modello di frenatura". Si tratta di un modello matematico che si applica in linea teorica a qualsiasi veicolo terrestre a guida vincolata e consente di prevedere l'andamento della velocità in funzione dello spazio a partire dai seguenti dati:
- distanza obiettivo (per esempio, quella di un potenziale ostacolo lungo il percorso);
- velocità attuale del veicolo;
- caratteristiche fisiche del veicolo e del sistema di frenatura (esempio, massa, peso frenato ecc.).

A partire da tali dati è possibile costruire una curva come quella mostrata nella figura 2. Una volta noto il modello di frenatura è facile, ragionando a ritroso, determinare istante per istante qual è la velocità massima a cui può viaggiare il veicolo affinché possa arrestarsi in modo sicuro prima del punto pericoloso, che nel caso ferroviario può essere rappresentato da un segnale di arresto (o di "via im-

pedita"). Chiaramente, la velocità massima può essere limitata da altri fattori, quali caratteristiche fisiche della linea: presenza di curve più o meno strette, deviatoi, tratti con rallentamenti temporanei dovuti a squadre di lavoro in linea ecc.

Il modello di frenatura va rielaborato ogni qualvolta variano uno o più dei parametri coinvolti (esempio, la distanza obiettivo). Il sistema di bordo ha quindi lo scopo di elaborare la curva di protezione e verificare che la velocità attuale del treno sia sempre al di sotto di quella massima definita dal modello, come riportato schematicamente nella figura 3. Possono essere presenti più curve leggermente "sfasate" tra loro in modo da definire reazioni diverse (esempio, allerta audio-visiva sul *cockpit* del macchinista, frenatura elettrica, frenatura pneumatica o di emergenza). Inoltre, è possibile che alla distanza obiettivo la velocità cosiddetta "di rilascio" non debba essere necessariamente nulla, ma solo al di sotto di un certo limite (esempio, 15 km/h)[1].

Affinché il sistema di bordo possa elaborare la curva di protezione, esso deve ricevere dal sistema di segnalamento di terra almeno le seguenti informazioni:

- ❑ autorizzazione al movimento, ovvero lo spazio che il treno è autorizzato a percorrere in modo sicuro, da cui viene ricavata la distanza obiettivo del modello di frenatura;
- ❑ profili di velocità, ovvero le limitazioni di velocità statiche (dovute alle caratteristiche fisiche della linea) o dinamiche (dovute a rallentamenti temporanei per lavori in corso), da cui viene ricavato il tetto di velocità del modello di frenatura.

Per contro, affinché il sistema di terra (*trackside*) possa fornire le suddette informazioni al bordo (*on-board*), esso deve ricevere almeno le seguenti informazioni:

- ❑ posizione attuale del treno lungo la linea e verso di percorrenza:
- ❑ libertà del percorso o stato della linea a valle della posizione del treno.

L'architettura di riferimento del sistema ERTMS/ETCS cosiddetto di livello 2 utilizzato sulle linee ferroviarie ad Alta Velocità è riportata nella figura 4. Un siffatto sistema consente l'elaborazione e lo scambio di informazioni tra il sistema di bordo e quello di terra utilizzando diversi mezzi trasmissivi cablati o *wireless*. In particolare, lo stato della linea è ricevuto attraverso una rete geografica in fibra ottica (WAN, *Wide Area Network*) dal cosiddetto sistema di *interlocking* (IXL), che tra le altre cose riceve lo stato di libero/occupato dei circuiti di binario nell'area di propria competenza. Un circuito di binario (*track circuit*, in inglese) è una sorta di *loop*

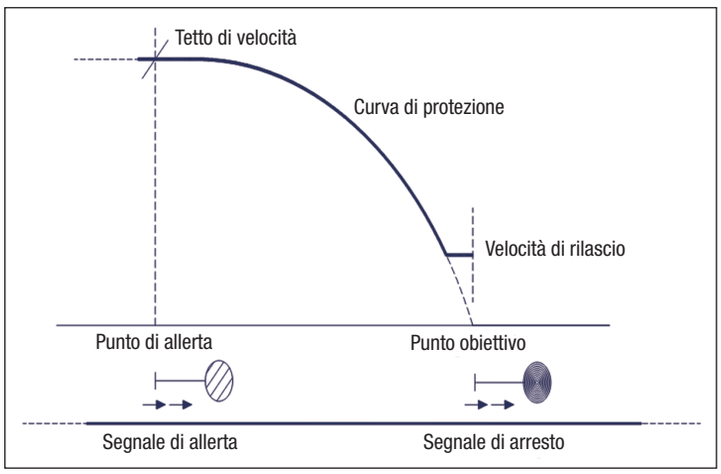


FIGURA 2
Rappresentazione schematica della curva di protezione elaborata dal sistema di bordo treno

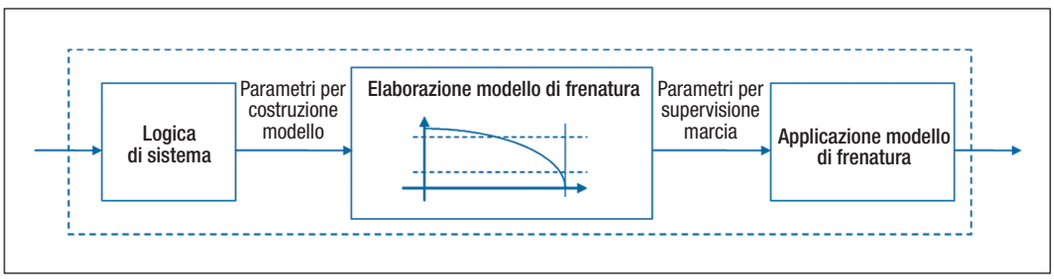


FIGURA 3
Compiti del sistema di controllo di bordo treno

[1] Un modello del genere è comune a praticamente tutti i sistemi evoluti di ATP, compreso quello denominato SCMT (*Sistema Controllo Marcia Treno*) impiegato in Italia sulle linea non ad Alta Velocità (riferimento [7]).

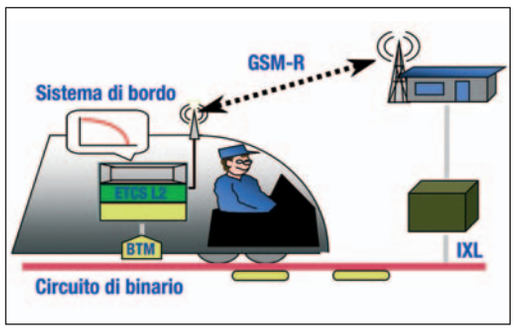


FIGURA 4

Schema semplificato del sistema ERTMS/ETCS di livello 2

elettrico (la cui lunghezza può superare un chilometro in piena linea), realizzato attraverso le rotaie, atto a rilevare la presenza di materiale rotabile (treni, locomotori, carrelli ecc.) che con i loro assi lo cortocircuitano. La posizione del treno è invece rilevata attraverso le cosiddette boe (o *balise*; Figura 5) statiche, ovvero dispositivi "passivi" installati fisicamente tra le rotaie in gruppi omogenei[2] e fissati alle traverse, che all'atto del passaggio del treno vengono energizzati per effetto induttivo e trasmettono in modalità *wireless* un telegramma fisso che contiene la chilometrica della linea (in altre parole, fungono da *milestones*). La posizione rilevata dal sistema di bordo, attraverso il cosiddetto captatore BTM (*Balise Transmission Module*), viene quindi trasmessa a terra attraverso un messaggio radio GSM-R, una versione dello standard GSM usata in ambito ferroviario anche per le comunicazioni vocali. A questo punto il sistema di terra attraverso il cosiddetto *Radio Block Center* (RBC) ha a disposizione tutte le informazioni per elaborare e trasmettere al treno, sempre tramite GSM-R, un messaggio contenente autorizzazione al movimento e profilo di velocità. Tutte queste elaborazioni devono soddisfare dei vincoli di ritardo massimo consentito, quantificati nel corso delle attività di *hazard analysis* [8].
Il riquadro 1 fornisce ulteriori elementi di approfondimento in relazione alle modalità di

[2] In AV tali gruppi, detti anche "punti informativi", sono costituiti tipicamente da due boe, il che assicura un certo livello di ridondanza e consente al sistema di bordo di rilevare il verso di marcia al passaggio sul singolo punto informativo.

FIGURA 5

Una balise ERTMS/ETCS (Fonte: <http://www.bahnindustrie.at/upload/bilder/-95/story/5096-96pk%28etcs-balise%29.jpg)

RIQUADRO 1 - Trasmissione dati terra-bordo in ambito ferroviario

Vale la pena citare che in altri livelli implementativi di ERTMS/ETCS e in differenti sistemi di segnalamento, la trasmissione di informazioni da terra a bordo può avvenire attraverso altri meccanismi, tra cui:

1. circuiti di binario o *loop* con codifica dei segnali, che vengono poi ricevuti dal bordo attraverso specifici captatori (è il caso per esempio del cosiddetto BACC, Blocco Automatico a Correnti Codificate);
2. boe attive (o "commutate") che replicano l'aspetto del segnale essendo connesse ad opportuni *encoder* lungo linea; esse trasmettono informazioni dinamiche sottoforma di telegrammi radio;
3. radio-segnalamento Wi-Fi, diffuso soprattutto nei sistemi CBTC (*Communication Based Train Control*) in ambito metropolitano;
4. satellite, in cui la posizione del treno è ricavata attraverso sistemi di georeferenziazione tipo GPS (*Global Positioning System*), come accade in alcuni sistemi americani di PTC (*Positive Train Control*).

Non tutte le suddette modalità trasmissive, variamente combinabili tra loro, consentono un aggiornamento continuo delle informazioni da terra a bordo. Per esempio, l'uso di boe commutate abilita una modalità di segnalamento **discontinuo**, dato che le informazioni aggiornate sullo stato della linea sono ricevute dal bordo unicamente all'atto della captazione del punto informativo. I *loop* permettono un tipo di segnalamento cosiddetto **semi-continuo**, dal momento che le informazioni sono aggiornate ovunque sia il treno, ma con un livello di granularità inferiore rispetto ad un sistema **continuo** di radio-segnalamento (esempio, GSM-R, Wi-Fi) dato che esse dovranno rimanere necessariamente le stesse per tutta la lunghezza del circuito. Un comportamento analogo (segnalamento semi-continuo) si ha con l'utilizzo del cosiddetto *radio infill*, tramite il quale si estende il raggio di azione di una boa commutata in modo da coprire una lunghezza maggiore. È intuitivamente evidente che la granularità superiore del radio-segnalamento continuo consente un migliore sfruttamento della capacità della linea, visto che non costringe a trasmettere informazioni in modo conservativo (secondo una logica *worst case*).
Vale la pena di osservare che lo standard ERTMS/ETCS prevede la coesistenza di eventuali sistemi di segnalamento pre-esistenti nel caso di transito sulle linee "storiche", per esempio in Italia ciò avviene quando il treno deve entrare nelle stazioni non AV, attrezzate con sistemi come SCMT. La coesistenza è possibile avendo previsto un'architettura a livelli sovrapposti, in cui quello "nazionale" coincide con il cosiddetto livello STM (*Specific Transmission Module*).

trasmissione delle informazioni di controllo in ambito ferroviario.

3. GESTIONE DEGLI ITINERARI

Se il treno avesse la sola possibilità di percorrere un unico binario tra un punto di origine e uno di destinazione, la logica precedentemente introdotta sarebbe grossomodo sufficiente al funzionamento del sistema. La realtà è che l'origine e la destinazione del movimento di un rotabile è tipicamente una stazione, e, come ben sanno i viaggiatori, diverse stazioni possono essere attraversate anche durante il percorso. Una stazione è fondamentalmente una parte del sistema ferroviario tipicamente più ampia (la cui area è detta in gergo "piazzale") costituita da un numero di binari paralleli (di "stazionamento", "corsa", "interconnessione", "manovra" ecc.) superiore a 2 e relativi deviatoi (*switch points* in inglese) che consentono di instradare i treni sui diversi binari. Il percorso di un treno dall'ingresso all'uscita - o allo stazionamento - in una stazione è detto "itinerario". Un itinerario copre un certo numero di circuiti di binario e di deviatoi. Il sistema di controllo che si occupa dell'instradamento dei treni sugli itinerari è detto in gergo di "gestione della via" o in inglese *interlocking* (IXL). In genere ogni sistema di stazione ha un numero predefinito di itinerari preconfigurati che devono essere formati di volta in volta per consentire il passaggio del treno. La formazione di un itinerario può essere automatica o comandata da un operatore (esempio, il capostazione, in caso di stazioni presenziate) ed è subordinata al superamento di tutta una serie di controlli, tra cui:

- ❑ stato di libero di tutti i circuiti di binario inclusi nell'itinerario;
- ❑ corretta operabilità dei deviatoi lungo l'itinerario;
- ❑ assenza di condizioni di fuori servizio.

Se le suddette condizioni sono soddisfatte, l'itinerario viene formato e al treno viene inviato un segnale (virtuale) di via libera per l'ingresso in stazione. Altrimenti, a seconda delle situazioni, il transito non può essere concesso o può essere concesso solo con opportune limitazioni di velocità e procedure manuali per consentire al macchinista il controllo visivo del percorso.

Nel caso delle stazioni AV, lo stato degli itinerari deve essere trasmesso anche al sistema RBC in modo tale che questo possa estendere l'autorizzazione al movimento in modo da coprire l'itinerario in stazione. La trasmissione di queste informazioni può avvenire in modo:

- ❑ sincrono: tutto lo stato viene trasmesso ogni tot millisecondi, indipendentemente dal fatto che vi siano state variazioni;
- ❑ asincrono: lo stato (o parte di esso) viene trasmesso solo quando si verifica una variazione.

Nel caso di trasmissione asincrona, deve essere assicurato un controllo di vitalità per evitare che una perdita di connessione possa rendere il sistema silente nei confronti di variazioni di stato senza che RBC possa avere la possibilità di accorgersene.

La figura 6 mostra lo schema di un possibile sistema di gestione degli itinerari (*routes*). A sinistra è mostrata una possibile visualizzazione sull'interfaccia operatore (MMI, *Man Machine Interface*), con lo stato di libero/occupato dei circuiti di binario e degli itinerari. A destra è mostrata la connessione WAN verso eventuali altri sistemi IXL (nel caso il sistema sia dedicato ad una sola stazione) e verso il sistema di automazione che si occupa a più alto livello della supervisione della marcia dei treni. Al

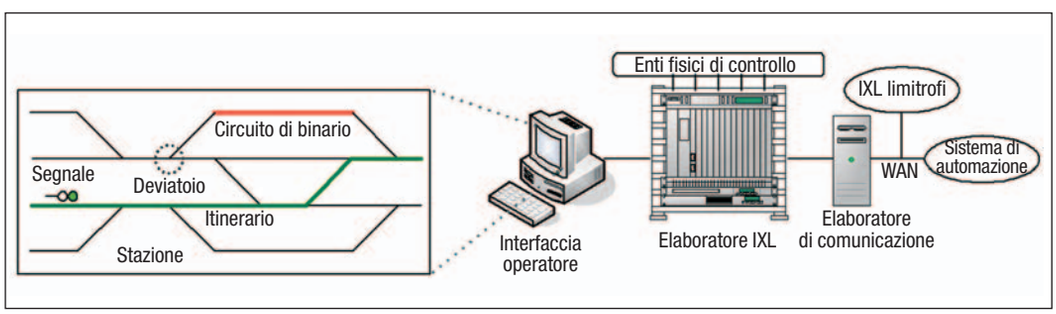


FIGURA 6

Schema di un possibile sistema di gestione degli itinerari

centro è mostrato il sistema di elaborazione vero e proprio, alloggiato in armadi (*rack*) posizionati a volte in posti periferici lungo la linea, che è connesso con le entità fisiche di controllo in campo (sensori e attuatori) attraverso protocolli di comunicazione proprietari (per esempio seriali).

4. DISTANZIAMENTO TRENI

Il sottosistema di AV responsabile di garantire un adeguato distanziamento tra un treno e l'altro, oltre che le altre informazioni necessarie ad assicurare la marcia sicura del treno, è il già citato *Radio Block Center* (RBC). Fondamentalmente, il RBC ha lo scopo di inviare periodicamente al sistema di bordo del treno dei messaggi radio contenenti le informazioni di cui esso ha bisogno per transitare in sicurezza. I più importanti tra questi sono i seguenti:

- *Movement Authority* (MA), ovvero autorizzazione al movimento, con specificata la distanza che il treno è autorizzato a percorrere ed i relativi profili di velocità statici (pacchetti SSP, *Static Speed Profile*) o dinamici (pacchetti TSR, *Temporary Speed Restrictions*).
- *Emergency Stop*, ovvero arresti d'emergenza, che possono essere condizionati (il treno deve arrestarsi solo se non ha superato un certo punto) o incondizionati (il treno deve arrestarsi immediatamente in qualsiasi condizione) e possono essere comandati manualmente dall'interfaccia operatore RBC presente al centro di controllo.

Al messaggio di MA possono essere aggiunte informazioni cosiddette di *linking*, che riportano ID e posizione dei punti informativi compresi nella MA (riquadro 2).

Un messaggio di tipo particolare è il cosiddetto *General Message*, che è il più semplice di tutti dal momento che ha l'unico scopo di segnalare periodicamente la "vitalità" del sistema RBC in assenza di altri messaggi da trasmettere (perché per esempio non vi sono state variazioni di stato significative rispetto alle ultime informazioni inviate). In assenza di messaggi di vitalità, infatti, il sistema di bordo non potrebbe accorgersi del fatto che non sta ricevendo informazioni perché nulla è cambiato (situazione sicura) o perché vi è stato un problema (perdita di connessione radio, guasto di RBC ecc.) ed esso non è più sotto la supervisione di RBC (situazione di pericolo). Come vedremo nel paragrafo successivo, esiste una specifica logica di bordo che consente di proteggersi nei confronti di quest'ultima eventualità.

Alcune tipologie di messaggi sono impiegati nella fase di *hand-shacking* tra il sistema di bordo

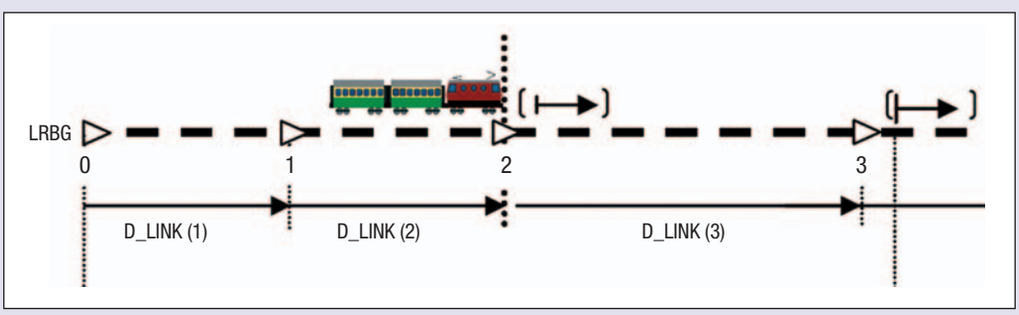
Riquadro 2 - Logica di appuntamento

Tra le informazioni inviabili al bordo rientrano le liste dei punti informativi in appuntamento (*linked balise groups*). Si tratta, in altre parole, dei gruppi di boe che il treno capterà durante il percorso e delle relative distanze (parametro D_LINK). Questa informazione serve per realizzare la cosiddetta "logica di appuntamento", ovvero un ulteriore controllo che garantisce:

- il corretto posizionamento dei punti informativi (può capitare che questi si stacchino o vengano rimossi in modo doloso), fattore critico per l'attendibilità dell'autorizzazione al movimento;
- la non esplosione dell'errore odometrico, qualora il treno "perdesse" uno o più punti informativi;
- il corretto instradamento lungo gli itinerari (se l'itinerario non è quello previsto, le boe captate saranno diverse).

La reazione del sistema di bordo ad un mancato appuntamento (considerata un'opportuna finestra di tolleranza) è configurabile e può anche coincidere con l'applicazione della frenatura.

Una rappresentazione schematica della logica di appuntamento è riportata nella figura.



Esempio di punti informativi in appuntamento (Fonte: rif. [24])

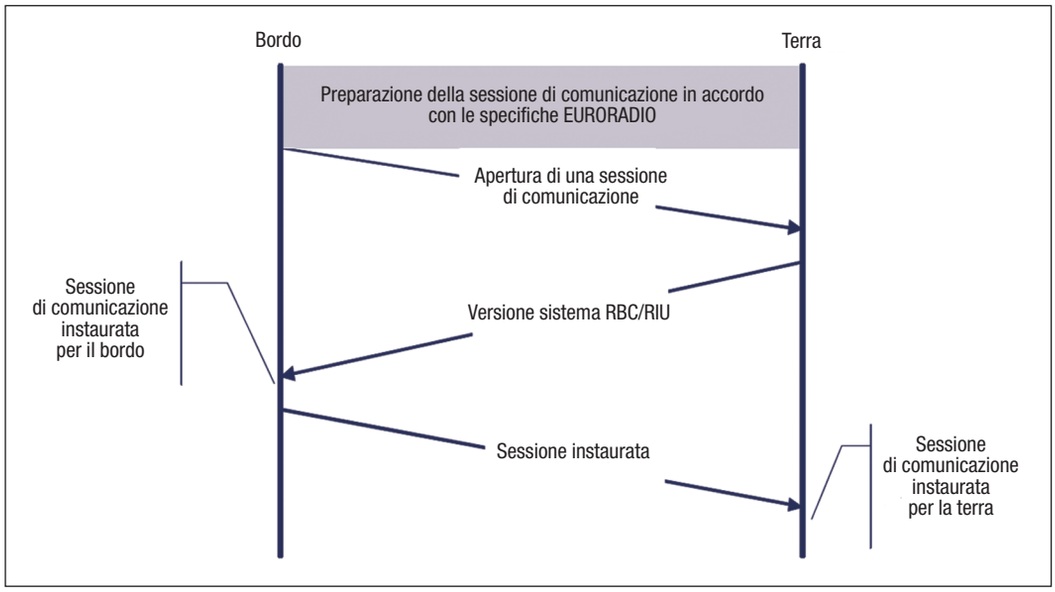


FIGURA 7
Instaurazione di una sessione di comunicazione tra bordo e terra (Fonte: rif. [24])

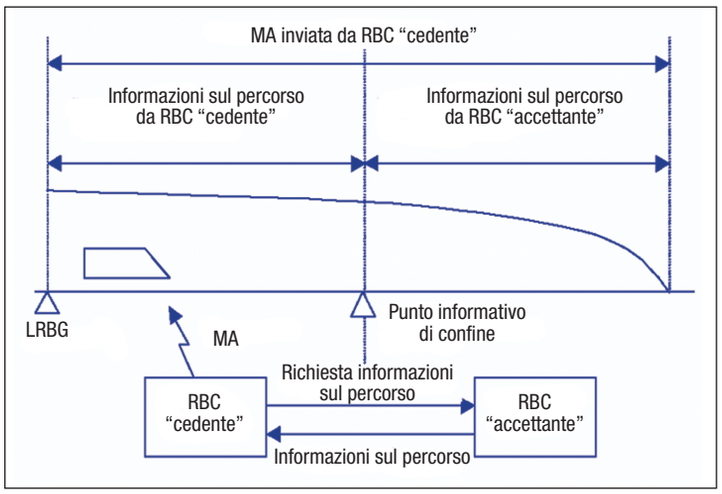


FIGURA 8
La procedura di RBC hand-over (Fonte: rif. [24])

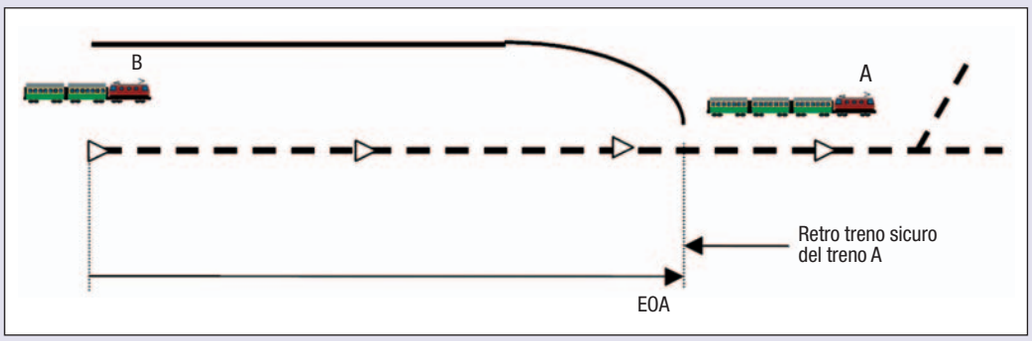
e quello di terra ad inizio missione (SOM, *Start Of Mission*), in cui tra le altre cose viene verificata la compatibilità delle versioni software di bordo e terra, e delle caratteristiche fisiche del treno con quelle della linea. La prima fase di questo colloquio è mostrata nella figura 7.
Altre tipologie di messaggi vengono adottate per gestire la procedura cosiddetta di RBC *Hand-Over* (HO) che si realizza quando un treno deve transitare dall'area di giurisdizione di un RBC a quella di un altro RBC (per esempio perché gli RBC controllano aree limitate per ragioni di prestazioni, o perché si sta attraversando un confine tra due stati). Tale procedura - di livello applicativo - non va confusa con quella di livello più basso che consiste nel passaggio del treno dall'area di copertura di una BTS (*Base Transceiver Station*) GSM-R a quella di un'altra. La procedura di HO, descritta schematicamente nella figura 8, ha lo scopo di evitare che il treno possa fermarsi o rallentare la sua corsa in corrispondenza del confine tra le aree di competenza di due RBC limitrofi. Per far sì che ciò non accada, quando il treno si avvicina al confine (condizione segnalata da opportune boe) il RBC cosiddetto "accettante" (*accepting*) deve trasmettere al RBC "cedente" (*handing-over*) le informazioni relative allo stato del percorso a valle del punto di confine (*border*), in modo che il cedente possa integrare la MA da trasmettere al treno con quella "concessa" dall'accettante. La logica di distanziamento di RBC al livello 2 di ERTMS/ETCS si basa sul principio del "blocco fisso" (per approfondimenti, riquadro 3 a p. 25).

5. CONTROLLO DELLA MARCIA

Come precedentemente descritto, il sistema di bordo ERTMS/ETCS ha lo scopo di elaborare il profilo di velocità dinamico del treno, cioè la curva di protezione, la cui distanza obiettivo coincide con la fine della MA (EoA, *End of Authority*) e il cui tetto è dato dal profilo di velocità più restrittivo (MRSP, *Most Restrictive Speed Profile*) tra quelli statici (SSP) e dinamici (TSR).
L'architettura di riferimento del sistema di bordo usato in AV è mostrata nella figura 9 **A**. Si

RIQUADRO 3 - Blocco fisso e blocco mobile

Nel livello 2 ERTMS/ETCS, la MA è costruita avvalendosi delle informazioni relative allo stato dei circuiti di binario e degli itinerari fornite dal sottosistema IXL (che non è standardizzato). Circuiti di binario ed itinerari costituiscono le cosiddette "*Sezioni di Blocco Radio*" (SBR). Una MA è costituita sempre e comunque da un numero intero di SBR. Vale la pena citare che questa logica si applica al caso di segnalamento cosiddetto a "blocco fisso", mentre esiste la possibilità che la MA venga costruita avvalendosi delle informazioni relative alla posizione dei treni, ovvero basandosi sulla distanza effettiva di un treno da quello successivo (si veda la Figura). In tal caso si parla di "blocco mobile", che può assicurare un maggiore sfruttamento della capacità della linea in quando si riduce la granularità del distanziamento. A fronte di tale vantaggio, però, non è assicurato il rilevamento di rotabili lungo il percorso non noti al sistema RBC, dal momento che la logica di distanziamento non si avvale dell'informazione di libertà della via comunicata da IXL. Pertanto, è fondamentale che sulla linea non possano accedere treni non ERTMS/ETCS (che non avrebbero nessuna possibilità di essere rilevati) e che sia assicurato un controllo di integrità dei treni per salvaguardarsi dall'eventualità di distacco dei vagoni. La modalità di distanziamento a blocco mobile è prevista dal livello 3 dello standard ERTMS/ETCS, che ha avuto sinora una diffusione di gran lunga inferiore rispetto al livello 2.



Autorizzazione al movimento in caso di blocco mobile (Fonte: rif. [24])

tratta di un sistema *real-time embedded* il cui nucleo vitale di elaborazione è denominato EVC (*European Vital Computer*) ed è connesso con diverse unità di I/O periferiche attraverso un apposito bus industriale. Tra le interfacce di I/O rientrano le seguenti:

- DMI (*Driver Machine Interface*), per l'interazione con il macchinista;
- BTM (*Balise Transmission Module*), per la captazione delle boe;
- TIU (*Train Interface Unit*), per l'interfacciamento con gli organi elettro-meccanici del rotabile (sistema di frenatura, odometria);
- RTM (*Radio Transmission Module*), per il collegamento con i terminali mobili GSM-R.

Oltre a questi componenti è prevista un'unità di JRU (*Juridical Recording Unit*), ovvero una sorta di "scatola nera" per la registrazione cronologica degli eventi (velocità e posizione del treno, interazioni del macchinista ecc.) e la possibile consultazione durante le indagini della magistratura a seguito di incidenti.

Attraverso la DMI il macchinista ha la possibilità di inserire o validare i dati del treno, che verranno poi inviati a RBC durante la procedura di inizio missione. La DMI è dotata di un tachimetro digitale che permette al macchinista di controllare, istante per istante, la ve-

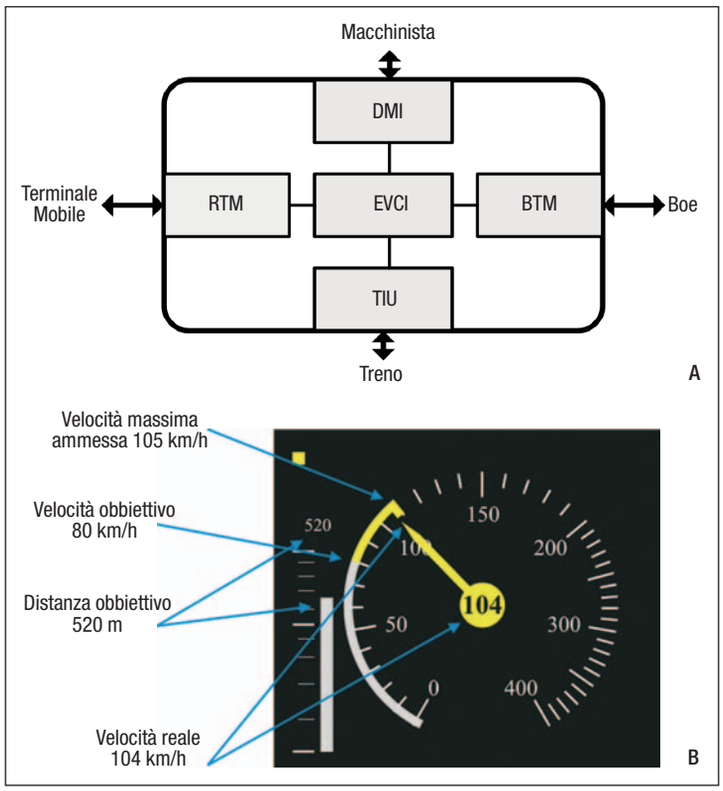


FIGURA 9

A - *Architettura di riferimento di bordo ERTMS/ETCS*

B - *Esempio di tachimetro digitale*

(*Fonte: http://upload.wikimedia.org/wikipedia/commons/b/b9/SegnaliFerroviari-AVAC-DMI.gif*)

locità massima consentita (Figura 9 **B**). Inoltre, essa consente di gestire modalità operative di degrado (con limiti di velocità di poche decine dikm/h), diverse dalla supervisione completa (FS, *Full Supervision*), tra cui:

- marcia a vista (*On-Sight*), che può essere concessa quando non vi è la certezza della libertà del percorso (ad esempio vi è un malfunzionamento di uno o più circuiti di binario);
- responsabilità del macchinista (*Staff Responsible*), che può essere concessa quando non vi è la certezza della corretta formazione dell'itinerario (per esempio vi è un malfunzionamento di uno o più deviatoi);
- manovra (*Shunting*), necessaria per proteggere il movimento dei treni durante le fasi di composizione/scomposizione di vagoni e locomotori.

I terminali mobili GSM-R presenti a bordo sono tipicamente due per garantire ridondanza e per semplificare la realizzazione della procedura di RBC *hand-over*, consentendo la connessione contemporanea a due RBC.

L'odometria è essenziale per misurare la distanza percorsa dall'ultimo punto informativo e riportare tali informazioni nel messaggio di rapporto di posizione (*Position Report*) che viene elaborato dal bordo (EVC) e inviato a terra (RBC) almeno ad ogni nuova captazione. In particolare, essendo sempre presente un errore di sovra/sotto-stima sulle misurazioni odometriche, la posizione del treno è sempre trattata tenendo conto delle seguenti informazioni:

- fronte treno massimo sicuro (*Max Safe Front End*), ovvero la posizione della testa del treno incrementata di una quantità pari alla distanza percorsa dall'ultimo punto informativo moltiplicata per la massima percentuale di errore odometrico;
- retro treno massimo sicuro (*Min Safe Rear End*), ovvero la posizione della coda del treno decrementata di una quantità pari alla distanza percorsa dall'ultimo punto informativo, a meno della lunghezza del treno, moltiplicata per la massima percentuale di errore odometrico.

Per esempio, con riferimento alla procedura di HO precedentemente descritta, per essere sicuri che il treno sia ancora completamente nell'area del RBC cedente bisogna far riferimento alla posizione del suo *Max Safe Front End*; viceversa, per essere sicuri che il treno sia transitato completamente nell'area del RBC accettante, bisogna far riferimento alla posizione del suo *Min Safe Rear End*.

Tra i parametri configurati sul sistema di bordo vi sono le velocità massime relative alle modalità di supervisione parziale e il cosiddetto T_NVCONTACT, ovvero il tempo massimo di omessa supervisione da parte di RBC prima di attivare un'opportuna reazione. In pratica, se la differenza tra il tempo corrente e la marcatura temporale dell'ultimo messaggio ricevuto (variabile T_TRAIN) è superiore al valore specificato dal parametro T_NVCONTACT, il sistema di bordo attiva una frenatura, eventualmente interrompibile (in gergo "riarmabile") alla ricezione di un nuovo messaggio "fresco". Il valore di T_NVCONTACT (tipicamente di pochi secondi) è un compromesso tra i requisiti di sicurezza, in base ai quali sarebbe opportuno che il treno percorresse il minor spazio possibile in assenza di supervisione, e quelli di prestazione, secondo i quali piccoli ritardi nel recapitare i messaggi radio (dovuti ad es. a ritrasmissioni in caso di corruzione dei dati contenuti nei pacchetti trasmessi) non dovrebbero compromettere le prestazioni di marcia.

6. GESTIONE DELLA CIRCOLAZIONE

Finora abbiamo discusso di sottosistemi critici per la sicurezza dei passeggeri. Benché non standardizzati in ERTMS/ETCS, per un funzionamento efficiente del sistema AV (così come di altri impianti ferroviari) è necessario prevedere un apparato non critico che si occupa specificamente della regolazione e supervisione centralizzata della circolazione dei treni. Un tale sistema deve fornire almeno le funzionalità di telecomando per il controllo remoto o automatico degli itinerari nei regimi di circolazione impresenziati, ovvero senza la presenza di un cosiddetto "dirigente locale del movimento" (volgarmente noto come "capostazione"), come accade su tutte le nuove linee AV. Il sistema è gestito da almeno un supervisore umano detto "dirigente centrale operativo" (o "dirigente centrale del traffico", in inglese *train dispatcher*).

Funzionalità aggiuntive rese disponibili nei cosiddetti posti centrali (cioè nelle sale di controllo, in inglese *central control rooms*) consistono nel monitoraggio diagnostico dello sta-

to del sistema (coadiuvato dalla videosorveglianza e da altra sensoristica), gestione delle informazioni al pubblico e raccolta dati statistici sulla circolazione, oltre che da altre peculiarità rese disponibili dall'interfacciamento con i sistemi SCADA (*Supervisory Control And Data Acquisition*).
Funzionalità avanzate dei sistemi cosiddetti di ATS (*Automatic Train Supervision*) possono essere la pianificazione automatica e l'ottimizzazione degli instradamenti per massimizzare la capacità della linea, in modo sia statico, cioè in funzione dei treni che vi devono circolare, che dinamico, cioè in funzione delle attuali condizioni del percorso.
Data la grande mole di informazioni da visualizzare, a volte condivisa tra più operatori, spesso le informazioni sono mostrate su schermi LCD o a retroproiezione (*overview screen o videowall*) pilotati da appositi client (Figura 10).

7. PROBLEMATICHE DI AFFIDABILITÀ E SICUREZZA

Trattandosi di sistemi critici per affidabilità e sicurezza, i sistemi di controllo ferroviario devono essere certificati secondo le direttive di rigorosi standard internazionali (esempio, CENELEC [10]). Tali norme regolano sia il processo di sviluppo che le caratteristiche del prodotto finale.
Come per tutti i sistemi *real-time embedded*, la schedulazione dei processi di controllo – scritti in linguaggi di logica proprietari e/o in *safe subset* di linguaggi *general purpose* (quale il *C*) – è realizzata attraverso sistemi operativi progettati e certificati per girare su *hardware* dedicato, per esempio è diffusa l'accoppiata *VxWorks* e piattaforma *PowerPC* [11].
Per i sottosistemi "vitali", il livello di certificazione richiesto è quello cosiddetto SIL4 (*Safety Integrity Level* 4), che tra le altre cose richiede un ciclo di sviluppo del tipo di quello mostrato nella figura 11 (cosiddetto "a V"), in cui la fase di verifica e validazione (*V&V*) rico-

FIGURA 10
Esempio di sala di controllo per la supervisione della circolazione ferroviaria (Fonte: http://neapolis.blog.rai.it/files/2008/01/fs-2.jpg)

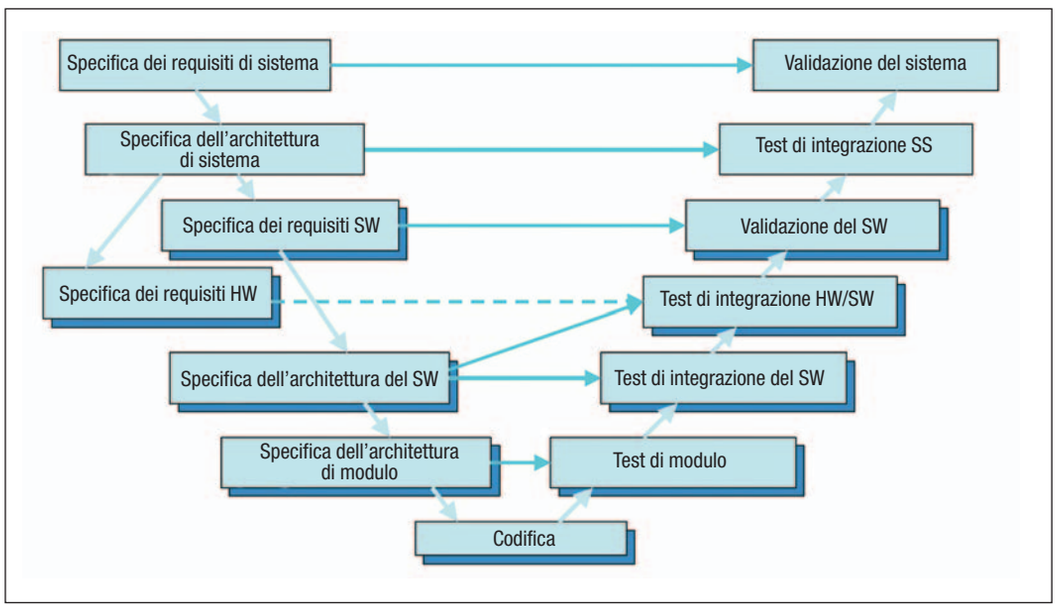


FIGURA 11
Ciclo di sviluppo a "V" (Fonte: http://www.intecs.it/pdf\BrochureVVRailwaylta13.pdf)

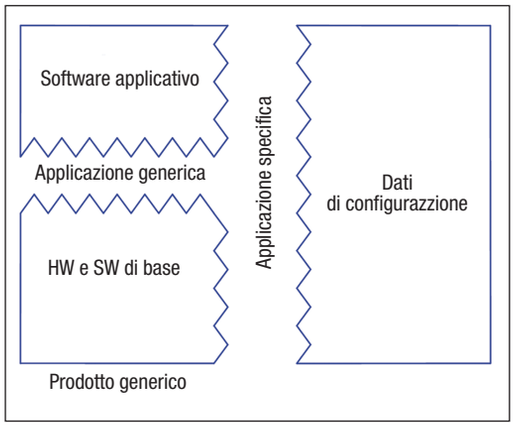


FIGURA 12
Processo di certificazione ferroviario

Parole chiave CENELEC EN 50159

Parola chiave	Significato
Ripetizione	Un messaggio viene ricevuto più di una volta
Cancellazione	Un messaggio viene rimosso dal flusso messaggi
Inserimento	Un nuovo messaggio viene inserito nel flusso messaggi
Riordinamento	Alcuni messaggi vengono ricevuti in una sequenza diversa da quella prevista
Corruzione	L'informazione contenuta in un messaggio viene mofidicata, casualmente o non
Ritardo	Alcuni messaggi vengono ricevuti in un tempo successivo rispetto a quello previsto
Mascheramento	Un messaggio non autentico viene pregettato in modo da apparire autentico (con "messaggio autentico" si intende un messaggio valido il cui contenuto è originato da una sorgente fidata)

TABELLA 1
Parole chiave definite dallo standard CENELEC EN50159

pre un ruolo predominante [12]. Dei risultati del processo di V&V viene data evidenza documentale in rapporti detti *safety case*, che possono riguardare il prodotto generico (ovvero l'hardware e il software di base), l'applicazione generica (esempio, logica del sistema di distanziamento treni) o l'applicazione specifica (esempio, distanziamento treni sulla linea Roma-Napoli), in cui sono presenti i dati di configurazione specifici dell'impianto (Figura 12) [13].
I requisiti di *safety* del sistema vengono ricavati dall'attività di analisi degli azzardi. Ad esempio, un risultato notevole di questa attività per il sistema AV è stato l'introduzione della funzionalità cosiddetta del circuito di binario (CdB) "ombra". Tale funzionalità serve a fronteggiare l'azzardo che può verificarsi a seguito dell'indebita occupazione del CdB successivo a quello occupato dal treno. Infatti, data la logica del distanziamento a blocco fisso, non sarebbe possibile discriminare in questo caso tra occupazione debita - il treno prosegue la sua marcia occupando il CdB successivo - o indebita - il CdB successivo viene occupato improvvisamente da un altro rotabile, ad esempio in ingresso da un deviatoio laterale. La funzionalità del CdB "ombra" consiste nell'invio al treno di un messaggio di emergenza condizionato con punto di arresto coincidente con il giunto che separa il CdB occupato dal treno dal successivo. Pertanto, se è il treno stesso ad aver occupato il CdB successivo, il sistema di bordo ignorerà semplicemente il messaggio, altrimenti attiverà la frenatura d'emergenza, detta in gergo *trip*.
Numerosi altri azzardi possono derivare dalle minacce, sintetizzate nella tabella 1, che caratterizzano un canale di comunicazione di tipo "aperto", quale è quello wireless GSM-R. Pertanto, il protocollo sicuro cosiddetto *Euroradio* è stato definito al fine di implementare i meccanismi atti a fronteggiare tali minacce (per approfondimenti, riquadro 4 a p. 29) [14, 15].
Venendo alle architetture hardware, quasi sempre vengono adottati sistemi di tipo NMR (*N-Modular Redundancy*) con votazione a maggioranza sull'output di sezioni di elaborazione indipendenti, diversamente sviluppate e galvanicamente isolate. Ciò consente di limitare al massimo l'incidenza di guasti di modo comune che potrebbero compromettere l'integrità del sistema (si vedano a tal proposito i riferimenti [16, 17]).
In particolare, nella specifica dei requisiti RAMS (*Reliability Availability Maintainability Safety*) del sistema ERTMS/ETCS [18], derivata dallo standard CENELEC 50129 [19], si richiede un tasso di guasti pericolosi (*Hazardous Failure Rate*, HFR[3]) inferiore a 10^{-9} per

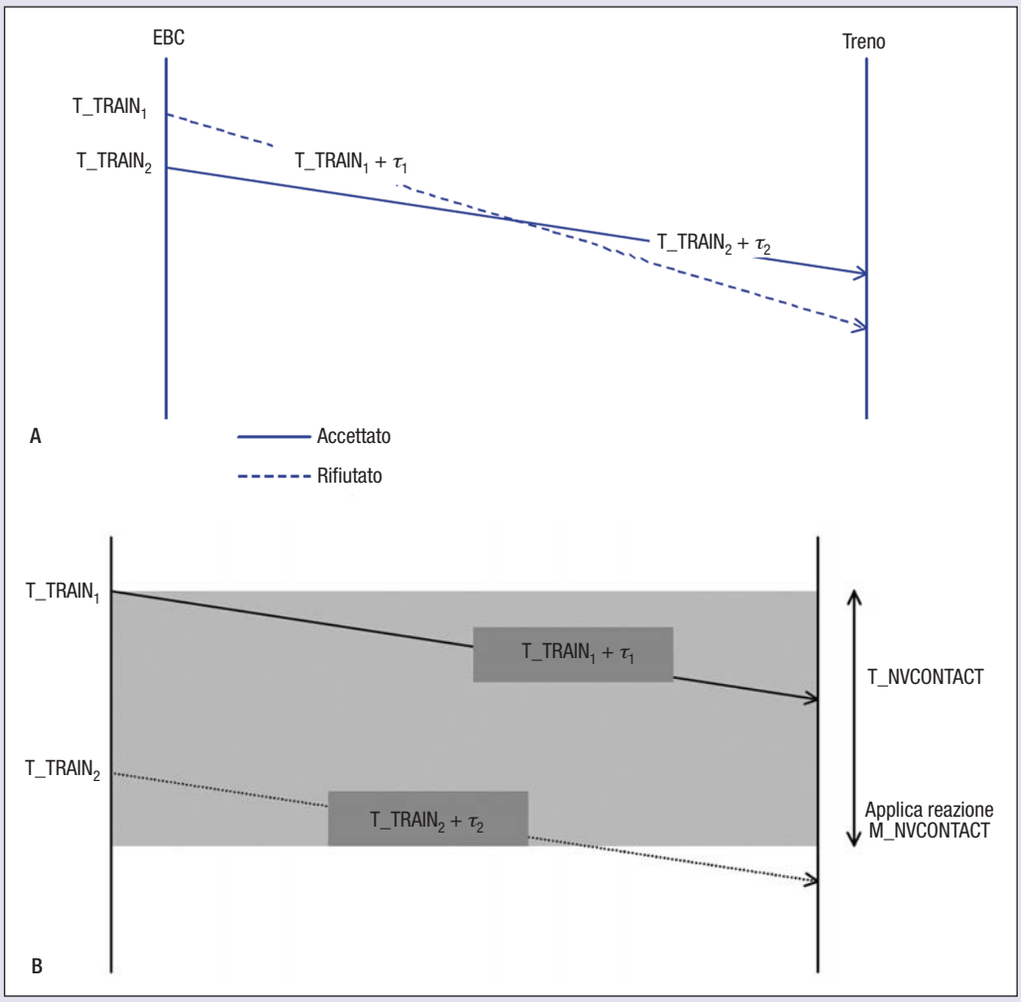
[3] L'HFR è l'inverso del tempo medio tra guasti pericolosi (*Mean Time Between Hazardous Events*, MTBHE).

Riquadro 4 - Il protocollo sicuro Euroradio

Al fine di fronteggiare le minacce che caratterizzano un canale di comunicazione aperto, definite nella tabella 1, il protocollo di comunicazione *Euroradio* applica le seguenti contromisure per elaborare il contenuto dei messaggi scambiati (si vedano a titolo di esempio le Figure **A** e **B**):

- ❏ numeri di sequenza (*sequence numbers*), per evitare cancellazioni, ripetizioni, inserimenti e perdita di sequenza nel flusso dei messaggi;
- ❏ marcature temporali (*time stamps*), per gestire i ritardi di comunicazione attraverso controlli di *freshness* e di vitalità;
- ❏ codici di controllo (*checksum*), per rilevare e correggere errori casuali nei dati trasmessi;
- ❏ cifratura (*cryptography*), per salvaguardare l'integrità e l'autenticità dei dati trasmessi nei confronti di attacchi informatici di tipo doloso (*hacking*).

In particolare, la specifica ERTMS/ETCS definisce un'entità cosiddetta KMC (*Key Management Center*) che ha il compito specifico di gestire le chiavi crittografiche usate per le comunicazioni via radio.



Protezione nei confronti di perdita di sequenza (**A**) *e ritardi* (**B**)*, (Fonte: rif. [24])*

ora (THR, *Tolerable Hazard Rate*), ovvero uno ogni almeno 100.000 anni.

Anche relativamente ai requisiti di disponibilità, la specifica è piuttosto precisa, definendo tra le altre cose i seguenti modi di guasto a livello di sistema [20]:

- ❏ guasto immobilizzante (*Immobilising Failure*), che si ha quando due o più treni sono costretti a marciare "a vista";
- ❏ guasto di servizio (*Service Failure*), che si verifica quando si ha un calo di prestazioni per uno o più treni e/o al più un treno è costretto a marciare "a vista";
- ❏ guasto minore (*Minor Failure*), che richiede

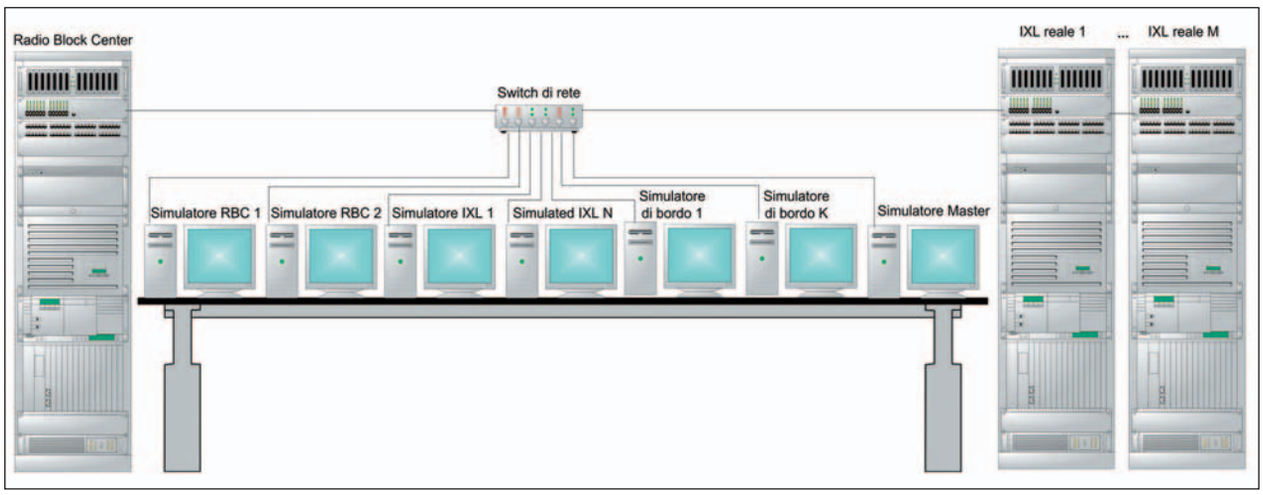


FIGURA 13

Esempio di ambiente di simulazione distribuito del tipo "hardware in the loop" per le prove di sistema ERTMS/ETCS

un intervento di manutenzione non pianificato ma non rientra nelle precedenti categorie.
Per esempio, secondo la specifica l'indisponibilità (MDT, *Mean Down Time*) del sistema rispetto ai guasti immobilizzanti di natura hardware non deve superare gli 8 minuti annui. Analogamente sono definiti i requisiti qualitativi e quantitativi di affidabilità (*Mean Time Between Failures*, MTBF) e manutenibilità (*Mean Time To Repair*, MTTR) suddivisi per modi di guasto e/o componenti.
A differenza della maggioranza dei prodotti software di tipo *consumer*, per i sistemi di controllo ferroviario non sono tollerati errori di progettazione o codifica, che, in quando sistematici, se attivati potrebbero avere conseguenze anche catastrofiche. Pertanto, requisiti quantitativi in termini di affidabilità del software lasciano spazio a criteri di sviluppo rigorosi e strumenti (esempio, compilatori, sistemi operativi) certificati per applicazioni critiche. Idealmente, tutto il software prodotto dovrebbe essere generato e/o verificato attraverso metodi formali. La complessità dei sistemi e la ridotta diffusione di approcci trasformazionali validati (esempio, generazione automatica del codice a partire da modelli di più alto livello, tipo UML) fa sì che all'atto pratico metodi puramente formali siano adottati solo in contesti limitati (esempio, verifica delle logiche di *interlocking* [21]). La maggior parte del software viene verificato attraverso tecniche di *testing*, coadiuvate da misure di copertura del codice e altre analisi statiche (quali per esempio quelle descritte in [22, 23]), in opportuni ambienti di simulazione [24]. Per esempio, la figura 13 mostra un possibile ambiente di simulazione per le verifiche di RBC del tipo *hardware-in-the-loop*, in cui alcuni componenti (esempio, i sistemi di bordo) girano su hardware commerciale, mentre altri (esempio, RBC) sulla piattaforma reale, in modo tale che per il sistema oggetto di test sia provata anche l'integrazione hardware-software.
Infine, approcci basati su modelli che consentano di migliorare efficacia ed efficienza del processo di verifica e validazione trovano applicazione in modo trasversale in tutte le fasi del ciclo di vita e a tutti i livelli di astrazione del sistema di controllo [25].

8. CONCLUSIONI

È opinione largamente condivisa che la capillarità e l'efficienza dei sistemi di trasporto su rotaia siano tra i segni più tangibili del livello di civilizzazione di un territorio. Ciò è dovuto a diversi fattori, tra cui: ridotta emissione di sostanze inquinanti per passeggero trasportato, riduzione del traffico sulle strade, maggiore sicurezza e comfort dei passeggeri. Alcuni di questi fattori si applicano in generale ai sistemi di trasporto pubblico, ma l'Alta Velocità ferroviaria aggiunge a questi tempi di percorrenza ridotti tra una città ad un'altra, in un ordine di distanza delle centinaia di kilometri (almeno). Negli ultimi

anni, non solo in Italia ma in tutto il mondo (Cina inclusa) stanno proliferando progetti basati sullo stesso standard europeo di interoperabilità su cui è basato AV. In particolare, in questo articolo abbiamo passato in rassegna del sistema AV gli aspetti relativi al controllo computerizzato che contribuiscono ad aumentarne prestazioni e sicurezza. L'ambito internazionale di ricerca in cui vengono studiati sistemi innovativi di trasporto a supervisione automatica è quello noto come *intelligent transportation systems*, a cui sono legati diversi convegni e pubblicazioni scientifiche in genere, che hanno sperimentato un forte impulso in tempi recenti. Per approfondimenti, esistono numerosi altri congressi che coprono almeno parzialmente le suddette tematiche, tra cui la serie *Computers in Railways* del *Wessex Institute of Technology*, o aspetti specifici, quali l'impiego di metodi formali nell'ingegneria ferroviaria (FORMS/FORMAT, *Symposium on Formal Methods for Automation and Safety in Railway and Automotive Systems*), o ancora lo stato dell'arte nello sviluppo e nell'implementazione dello standard ERTMS/ETCS a livello mondiale (*UIC World Congress*).

Bibliografia

[1] Pagina Wikipedia su incidenti ferroviari recenti, http://en.wikipedia.org/wiki/List_of_rail_accidents_(2010-2019)

[2] Descrizione ATC Roma Metro C, http://www.metrocspa.it/treni.asp

[3] Sito ufficiale ERTMS/ETCS, http://www.ertms.com

[4] Flammini F., Mazzocca N., Vittorini V.: Modelli per l'analisi di sistemi critici. *Mondo Digitale*, n. 3, settembre 2009, p. 11-21.

[5] Senesi F., Marzilli E.: *European Train Control System – Sviluppo e messa in esercizio in Italia*. CIFI, 2008.

[6] *Brochure sistema ERTMS*, http://www.rfi.it/-cms-file/allegati/rfi/ERTMStotale.pdf

[7] *Descrizione modello di frenatura SCMT*, http://www.rfi.it/cms-file/allegati/rfi/documenti/vol33ModellodiFrenaturaperSCMTVo3C.pdf

[8] Di Tommaso P., Esposito R., Marmo P., Orazzo A.: *Hazard Analysis of Complex Distributed Railway Systems*. In: 22-nd International Symposium on Reliable Distributed Systems (SRDS'03), 2003, p. 283-292.

[9] Unisig: *ERTMS/ETCS – Subset 026 System Requirements Specification (SRS)*. Issue 3.0.0, 2008.

[10] CENELEC 2000. EN 50126 Railways Applications – The specification and demonstration of Reliability, Maintainability and Safety (RAMS).

[11] VxWorks, http://www.windriver.com/products/-product-notes/PN_VE_61508_0109.pdf

[12] Sillitti A.: A caccia degli errori del software. *Mondo Digitale*, n. 4, dicembre 2005, p. 32-44.

[13] Flammini F., Mazzocca N., Orazzo A.: Automatic instantiation of abstract tests to specific configurations for large critical control systems. *Journal of Software Testing, Verification & Reliability* (STVR), Vol. 19, Issue 2, 2009, p. 91-110.

[14] Schulz O., Peleska J.: *Reliability Analysis of Safety-Related Communication Architectures*. Proc. SAFECOMP'2010, Springer LNCS, Vol. 6351/2011, p. 1-14.

[15] Smith J., Russell S., Looi M.: *Security as a safety issue in rail communications*. In Proc. 8-th Australian Workshop on Safety Critical Systems and Software, Vol. 33 (Canberra, Australia). Lindsay P., Cant T., Eds. Conferences in Research and Practice in Information Technology Series, Vol. 97. Australian Computer Society, Darlinghurst, Australia, 2003, p. 79-88.

[16] Coccoli A., Bondavalli A.: *Analysis of Safety Related Architectures*. In: 9-th IEEE International Workshop on Object-Oriented Real-Time Dependable Systems (WORDS'03), 2003.

[17] Amendola A.M., Impagliazzo L., Marmo P., Mongardi G., Sartore: *Architecture and Safety Requirements of the ACC Railway Interlocking System*. Proc. IEEE 2-nd Int. Computer Performance & Dependability Symposium (IPDS'96), Urbana Champaign, USA, 1996, p. 21-29.

[18] Unisig: *ERTMS/ETCS – Class 1 Safety Requirements*. Issue 2.2.11, Subset-091, 2005.

[19] CENELEC 2004. EN 50129 Railways Applications – Safety Related Electronic Systems for Signalling.

[20] Unisig: ERTMS/ETCS – RAMS Requirements Specifications Chapter 2 – RAM, http://www.era.europa.eu/Document-Register/Documents/B1-02s1266-.pdf

[21] Cimatti A., Giunchiglia F., Mongardi G., Romano D., Torielli F., Traverso P.: Model Checking Safety Critical Software with SPIN: an Application to a Railway Interlocking System. *Lecture Notes in Computer Science*, Vol. 1516/1998, 1998, p. 284-293.

[22] Caiazza A., Di Maio R., Fernando S., Poli F., Impagliazzo L., Amendola A.M.: *A New Methodology and Tool Set to Execute Software Tests on Real-Time Safety-Critical Systems*. Proc. 5-th European Dependable Computing Conference (EDCC 2005), p. 293-304.

[23] Abbaneo C., Flammini F., Lazzaro A., Marmo P., Sanseviero A.: *UML Based Reverse Engineering for the Verification of Railway Control Logics*. Proc. Dependability of Computer Systems (DepCoS'96), Szklarska Poreba, Poland, May 25-27, 2006, p. 3-10.

[24] Di Tommaso P., Flammini F., Lazzaro A., Pellecchia R., Sanseviero A.: *The Simulation of Anomalies in the Functional Testing of the ERTMS/ETCS Trackside System*. In: 9-th IEEE International Symposium on High-Assurance Systems Engineering (HASE'05), 2005, p.131-139.

[25] Flammini F., Impagliazzo L., Marmo P., Pragliola C.: Affidabilità e sicurezza dei sistemi innovativi di comando/controllo. Approcci basati su modelli e loro applicazioni industriali. *Ingegneria Ferroviaria*, n. 6, giugno 2010, p. 543-558.

Francesco Flammini, ha ottenuto la laurea con lode (2003) e il dottorato di ricerca (2006) in Ingegneria Informatica presso l'Università di Napoli "Federico II". Dal 2003 lavora in Ansaldo STS come progettista e ricercatore, occupandosi di verifica dei sistemi di controllo e protezione delle infrastrutture. Ha tenuto come professore a contratto corsi di informatica ed ingegneria del software. È autore di numerosi articoli scientifici pubblicati su riviste, libri e atti di congressi internazionali. Svolge attività editoriali per libri e riviste sul tema dei sistemi sicuri ed affidabili ed è nel comitato di programma di diversi convegni internazionali, tra cui SAFECOMP. È vicepresidente del capitolo italiano dell'IEEE Computer Society per il biennio 2010-2011.
E-mail: francesco.flammini@ieee.org