Railway Safety e Cyber Security

Garantire la circolazione sicura dei dati e dei treni

Firenze 21/5/2026

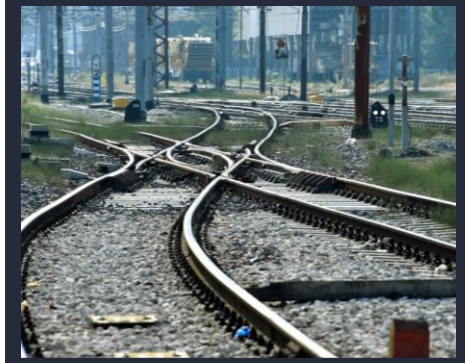
ANSFISA
AGENZIA NAZIONALE PER LA SICUREZZA DELLE FERROVIE
E DELLE INFRASTRUTTURE STRADALI E AUTOSTRADALI

Christian Lusi

Direzione Generale Sicurezza Ferroviaria
Responsabile ufficio «Sottosistema Controllo Comando e Segnalamento a terra»

Argomenti

- ANSFISA: principali attività
- Attacchi cyber al settore dei trasporti
- ANSFISA e Cyber Security
- Uno sguardo alle minacce future



18.000 km

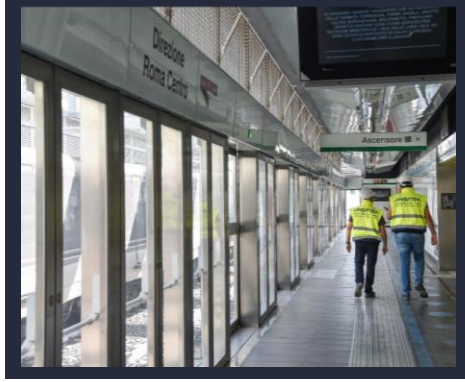
DI FERROVIE NAZIONALI REGIONALI, ISOLATE E TURISTICHE

con oltre **5.000 passaggi a livello** e **20.000 ponti, viadotti, gallerie** e **opere d'arte,** dove circolano **circa 9.000 treni al giorno**

840.000 km

DI STRADE E AUTOSTRADE

di cui **35.265 km** di **autostrade** e **strade statali (4%)** dove insistono **29.000** tra **gallerie, ponti e viadotti, cavalcavia**



IMPIANTI FISSI

metropolitane, tram, funivie, seggiovie, scale mobili, tapis roulant, ascensori pubblici

Promuove la sicurezza e assicura la vigilanza sulle condizioni di sicurezza del sistema ferroviario e delle infrastrutture stradali e autostradali e degli impianti fissi

ANSFISA

AGENZIA NAZIONALE PER LA SICUREZZA DELLE FERROVIE E DELLE INFRASTRUTTURE STRADALI E AUTOSTRADALI

Ferrovie e minacce informatiche

Open Access News | Transport

New rail system could be hacked

April 24, 2015

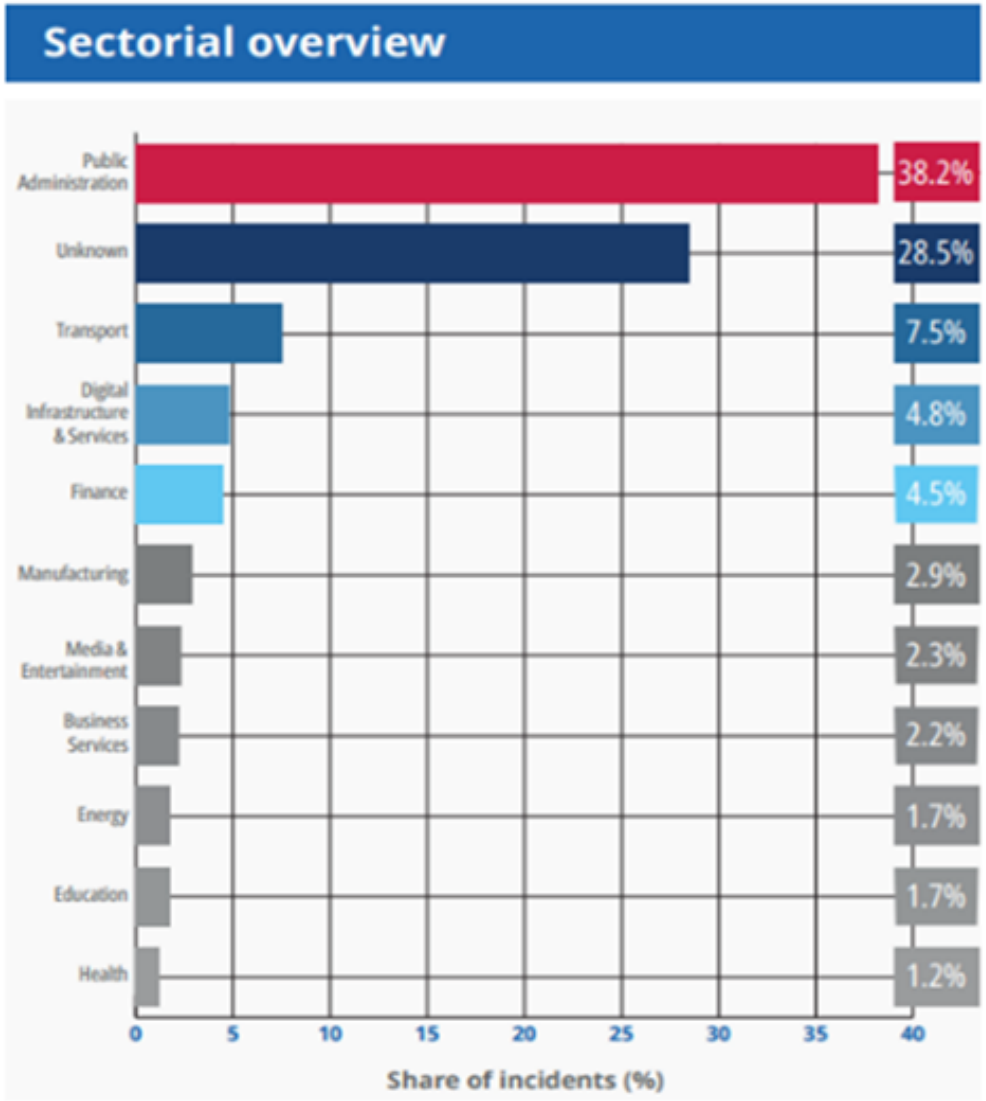
Expert and government adviser Professor David Stupples has warned that a new high-tech rail system could be hacked, leading to a serious crash...

- ***Professor David Stupples*** *at* ***City University London*** *said the new computers set to replaced ageing signal lights could be at risk of serious cyber attack*
- *The* ***European Rail Traffic Management System*** *(ERTMS) is currently being tested in the UK. Once it is launched computers will dictate critical safety information*
- *The system, which is already in use in other parts of the world, has never seen any reported cases of cyber attacks. However, Professor Stupples, who is an expert in networked electronic and radio systems, said hacking into the system could result in a "nasty accident" or "major disruption".*
- "It's the clever malware [malicious software] that actually alters the way the train will respond. "So, it will perhaps tell the system the train is slowing down, when it's speeding up"
- "The weakness is getting malware into the system by employees. Either because they are dissatisfied or being bribed or coerced"
- the main reason the system had not been hacked as frequently as financial institutions and media organisations was because much of the technology used was too old to be vulnerable

https://www.openaccessgovernment.org/new-rail-system-hacked/16384/

ANSFISA
AGENZIA NAZIONALE PER LA SICUREZZA DELLE FERROVIE E DELLE INFRASTRUTTURE STRADALI E AUTOSTRADALI

Quantità di attacchi nei trasporti



Threat Landscape 2025 ENISA
(https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025)

The transport sector came in second (7.5%), with most reported incidents pertaining to air and logistics, with a particular focus on targeting the maritime sector displayed by state-nexus intrusion sets.

ANSFISA
AGENZIA NAZIONALE PER LA SICUREZZA DELLE FERROVIE E DELLE INFRASTRUTTURE STRADALI E AUTOSTRADALI

Principali attacchi in Europa

- **2017**
  - Attacco ransomware *WannaCry* alla Deutsche Bahn in Germania: Il virus ha infettato circa 450 computer, bloccando i sistemi di informazione passeggeri nelle stazioni. La tipica schermata di riscatto del ransomware è apparsa sui tabelloni elettronici degli orari in diverse città tedesche. **Oltre ai tabelloni, sono stati compromessi i distributori automatici di biglietti e i sistemi CCTV**
  - Attacco *NotPetya* a ferrovie, banche, aeroporti e centrali energetiche in Ucraina con **criptazione dei sistemi e interruzione delle operazioni** (vulnerabilità Windows, Wiper mascherato da Cryptolocker, lanciato da GRU)
- **2022**
  - Interruzione servizio su rete ferroviaria danese dovuto ad un attacco ransomware al fornitore di servizi ICT Supeo che ha **impedito ai macchinisti di accedere a scheda treno e prescrizioni di movimento**
- **2023**
  - Attacco ferrovie nord-ovest Polonia. Con ricetrasmittenti da poche decine di euro **trasmesso un segnale che ha attivato automaticamente la frenata d'emergenza**. L'attacco ha bloccato circa 20 treni
  - Attacco ai sistemi di trasporto locale della città di Olsztyn (Polonia). Paralizzati i server che gestivano **i semafori intelligenti, i tabelloni elettronici alle fermate con i tempi di attesa e il sistema di vendita dei biglietti** online e alle emettitrici fisiche. Disagi durati varie settimane
- **2024**
  - Una violazione della sicurezza presso Transport for London (TfL): Hacker hanno avuto **accesso a database contenenti nomi, indirizzi e-mail, indirizzi di casa e, per circa 5.000 clienti, dati bancari** (numeri di conto e sort code) relativi ai rimborsi.
  - Nei giorni seguenti all'attacco fisico alle ferrovie Francesi in concomitanza della cerimonia di apertura delle Olimpiadi, **registrati attacchi DDOS e Ransomware**.
- **2025**
  - ondata di cyberattacchi ai sistemi di biglietteria della compagnia ferroviaria polacca PKP Intercity, causando **notevoli disagi nell'acquisto di biglietti tramite i canali elettronici**. Attacco DDOS (100 milioni di accessi al sistema in una singola).

Attacco Ransomware a Ferrovie dello Stato (Marzo 2022)

Il gruppo hacker Hive colpì le reti di Trenitalia e RFI utilizzando un virus di tipo *cryptolocker*

- Blocco totale dei sistemi di vendita nelle **biglietterie** fisiche e nei self-service in stazione.
- Impossibilità per il personale di accedere ai **servizi IT aziendali** (ad es. sistema di gestione documentale e protocollo)
- Per evitare la propagazione del virus, FS dovette isolare parte della rete IT.

Attacco Ransomware a Ferrovie del Gargano (2023)

I criminali informatici sono riusciti a infiltrarsi nei server aziendali, cifrando i dati e rendendoli inaccessibili, inclusi quelli di backup

l'incidente ha creato seri **disagi ai sistemi gestionali e amministrativi**:

- Il sistema di acquisto **biglietti** dal sito web e dall'app ha subito interruzioni prolungate.
- I canali ufficiali di **informazione all'utenza** sono rimasti parzialmente isolati per diversi giorni.
- Le attività amministrative interne sono state le più colpite, richiedendo il ripristino manuale di molti database dai backup (laddove integri).

Ondata di attacchi DDoS (Gennaio 2025)

Trenitalia, ATAC e AMT colpite da un'offensiva del gruppo hacker NoName057

- attacco DDoS (Distributed Denial of Service), mirato a rendere i siti web irraggiungibili inondandoli di traffico
- rallentamenti e malfunzionamenti temporanei ai **siti web e ai sistemi di informazione al pubblico**

Data Breach Almaviva (Novembre 2025)

Attacco indiretto a Ferrovie dello Stato attraverso una violazione dei sistemi di Almaviva, suo principale fornitore di servizi IT

- sottratti circa 2,3 TB di dati sensibili, tra cui contratti, buste paga, documenti contabili e configurazioni di rete aggiornati al terzo trimestre 2025
- tipo di attacco particolarmente pericoloso perché ha fornito agli hacker la "mappa" digitale delle infrastrutture, facilitando potenziali intrusioni future nei sistemi IT e OT

Attacco DDOS ad ATAC (Febbraio 2026)

attacco informatico facente parte di un’ondata di offensive cyber che ha coinvolto diverse infrastrutture critiche e istituzioni romane (come l'Università La Sapienza e Roma Tre) proprio all'inizio di quest'anno

- attacco di tipo DDoS volto a saturare i server per rendere inaccessibili i servizi online. Sono stati segnalati anche tentativi di intrusione più profondi volti a rallentare i sistemi gestionali interni.
- l'azione è stata attribuita al gruppo NoName057, che già in passato aveva preso di mira l'azienda capitolina

Impatto sulla safety?

- attacchi informatici finora condotti verso gli operatori **hanno avuto impatto sui sistemi IT**, causando rallentamenti e malfunzionamenti dei servizi on-line verso gli utenti e degli applicativi aziendali utilizzati dal personale

- **non risulta siano stati finora compromessi i sistemi OT preposti alla sicurezza della circolazione** (apparati centrali, sistemi di protezione della marcia, sistemi di blocco automatico) in modo tale da causare un impatto diretto sulla safety dell'esercizio

ANSFISA e Cyber Security in ambito ferroviario

Ai sensi del vigente quadro normativo, la cybersecurity esula dalle specifiche competenze di ANSFISA, che si occupa della sicurezza ferroviaria rispetto a rischi di natura accidentale (safety) e non rispetto ad atti intenzionali (security)

Compiti e ruoli di cui al D.Lgs. n. 138/2024

- **ACN**
  - ✓Autorità nazionale competente NIS
  - ✓Punto di contatto unico NIS, che assicuri il raccordo nazionale e transfrontaliero
  - ✓Gruppo di intervento nazionale per la sicurezza informatica in caso di incidente in ambito nazionale (CSIRT Italia)
  - ✓Gestione crisi informatiche su vasta scala (resilienza nazionale)
- **Ministero della difesa**
  - ✓Gestione crisi informatiche su vasta scala (difesa dello Stato)
- **Autorità di settore NIS**
  - ✓Collaborazione con ACN, supportandone le funzioni svolte quale Autorità nazionale competente NIS e Punto di contatto unico NIS
- **Soggetti essenziali**
  - ✓ Soggetti che operano in settori ad **alta criticità** (energia, **trasporti**, finanza, sanità, acqua potabile, Infrastrutture digitali , spazio, ecc.) o **critici** (servizi postali, gestione rifiuti, produzione alimenti, ecc) e che superano i massimali per le medie imprese
  - ✓ Fornitori di reti pubbliche di comunicazione elettronica e di servizi di comunicazione elettronica
  - ✓ Prestatori di servizi fiduciari qualificati (es. firma elettronica), gestori di registri dei nomi di dominio di primo livello, prestatori di servizi di sistema dei nomi di dominio
  - ✓ Pubbliche amministrazioni centrali (Organi costituzionali e di rilievo costituzionale, Presidenza del Consiglio dei ministri e i Ministeri, Agenzie fiscali, Autorità amministrative indipendenti)
- **Soggetti importanti**
  - ✓ Soggetti che operano in settori ad alta criticità o critici e che non superano i massimali per le medie imprese ma superano i massimali per piccole imprese
  - ✓ Amministrazioni regionali e locali
  - ✓ Altri soggetti pubblici (Enti di regolazione dell'attività economica [come **ANSFISA**], Enti e le Istituzioni di ricerca, ecc.)
- **Ulteriori tipologie di soggetti** (specificamente individuati da ACN)
  - ✓ **Soggetti che forniscono servizi di trasporto pubblico locale**
  - ✓ Istituti di istruzione che svolgono attività di ricerca.
  - ✓ Soggetti che svolgono attività di interesse culturale.
  - ✓ Società in house, società partecipate e società a controllo pubblico

Compiti e ruoli di cui al D.Lgs. n. 138/2024

Su quali fronti agire:

- Attribuzione di risorse (umane e strumentali) e competenze necessarie
- Coinvolgimento, da parte degli Organi istituzionali di governance, dei soggetti detentori del know-how specialistico
- Chiarire nel dettaglio, compiti, responsabilità e «procedure di interfaccia» tra tutti i soggetti

ANSFISA e Cyber Security in ambito ferroviario

Su richiesta di ERA e a supporto del MIT, ANSFISA parteciperà al **Gruppo di Coordinamento per la Sicurezza Informatica** in corso di istituzione da parte di ERA, che si occuperà di :

- Condividere informazioni sulle minacce, le sfide e le migliori pratiche in materia di sicurezza informatica rilevanti per il settore ferroviario
- Monitorare e scambiare opinioni su come ogni Stato membro sta recependo e attuando la Direttiva NIS2, con particolare attenzione alla sua applicazione alle entità ferroviarie
- Discutere le implicazioni, le interpretazioni e gli orientamenti settoriali derivanti dalla Direttiva NIS2 per le ferrovie
- Fungere da forum per l'allineamento e potenziali approcci comuni ove utile.

ANSFISA
AGENZIA NAZIONALE PER LA SICUREZZA DELLE FERROVIE E DELLE INFRASTRUTTURE STRADALI E AUTOSTRADALI

ANSFISA e Cyber Security in ambito ferroviario

Su richiesta di ERA, ANSFISA parteciperà anche al **Topical Working Group on Cybersecurity** in corso di istituzione da parte di ERA, che si occuperà di:

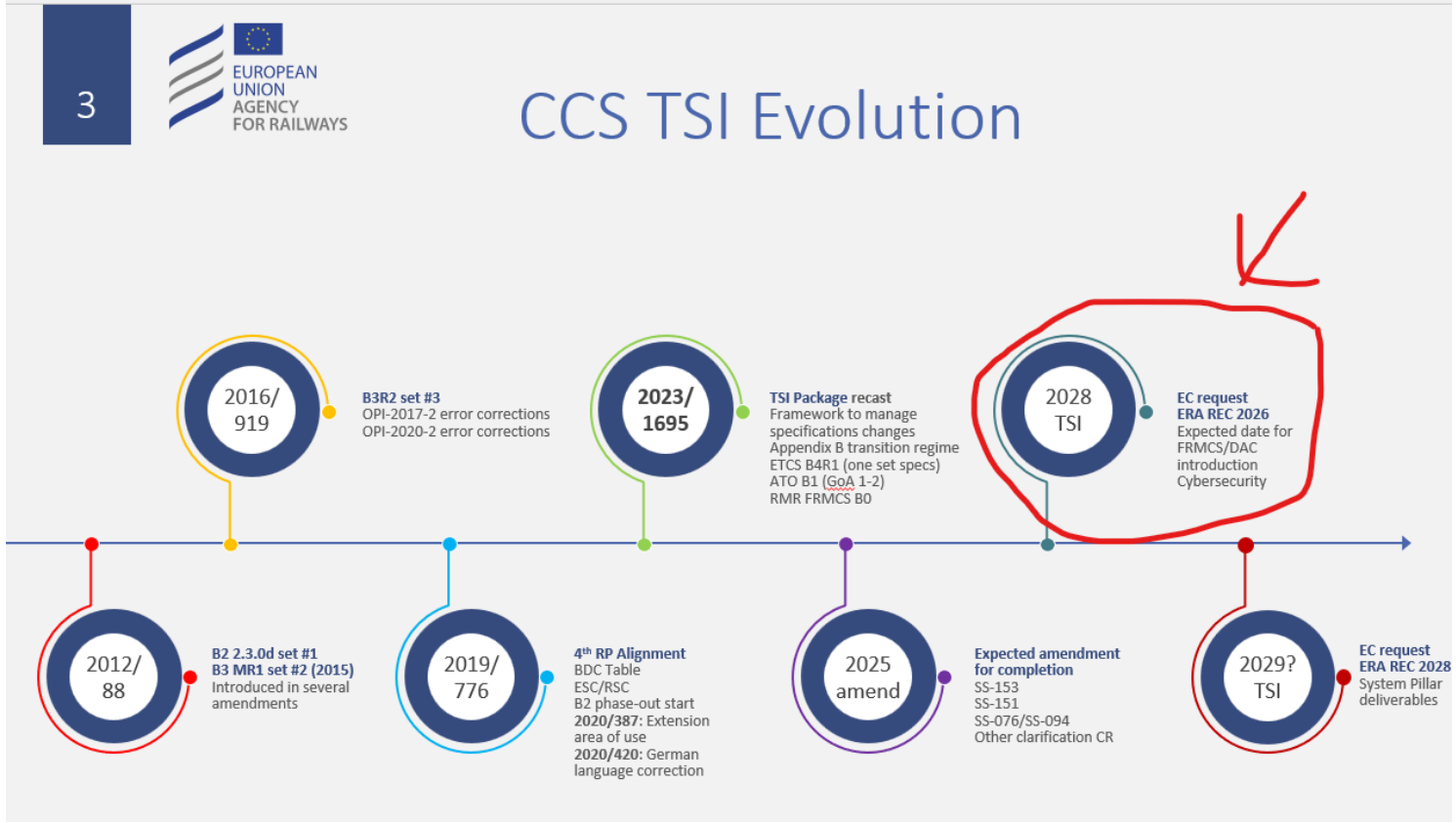
- Analizzare le due specifiche sviluppate da ERJU riguardo alla cybersecurity:
  - *SP-SEC_Secure Communication Specification_1.1_Released.pdf*
  - *SP-SEC_Shared Cybersecurity Services Specification_1.1_Released.pdf*

- Valutare la relativa adozione come ERA Technical Documents, anche ai fini della revisione delle STI

Le due specifiche sono disponibili sulla ERJU webpage (*https://rail-research.europa.eu/security-2/*) al link (*https://rail-research.europa.eu/wp-content/uploads/2026/04/CYBERSECURITY-SPECIFICATIONS-V1.1_EURAIL-SP.zip*)

ANSFISA e Cyber Security in ambito ferroviario

ANSFISA parteciperà ai **gruppi di lavoro ERA per la revisione delle STI** al fine in particolare di introdurre **specifici requisiti sulla cybersecurity** e sulla **relativa certificazione dei sottosistemi**:



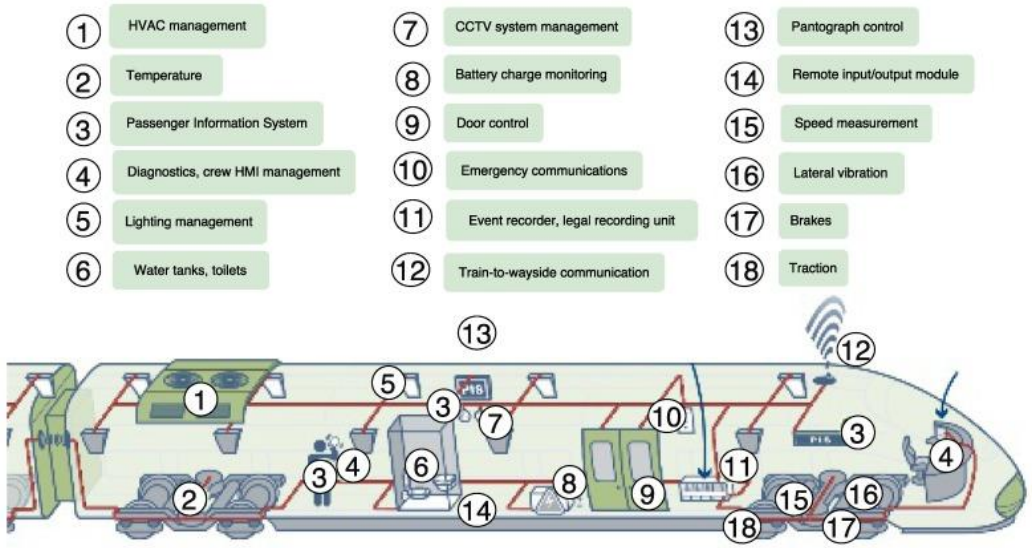
Attività da svolgere su cybersecurity

- Analisi delle **implicazioni del quadro giuridico dell'UE** in materia di sicurezza informatica (es. NIS 2 e CRA) sul sistema ferroviario europeo e sui requisiti delle STI
- Regolamentare **l'interoperabilità delle misure di sicurezza informatica** ed evitare che la sicurezza informatica influisca negativamente sulla interoperabilità o la safety
- Garantire che gli aspetti specifici del settore ferroviario della sicurezza informatica **ai fini della certificazione** siano considerati nelle STI per evitare processi paralleli e potenzialmente conflittuali

ANSFISA
AGENZIA NAZIONALE PER LA SICUREZZA DELLE FERROVIE E DELLE INFRASTRUTTURE STRADALI E AUTOSTRADALI

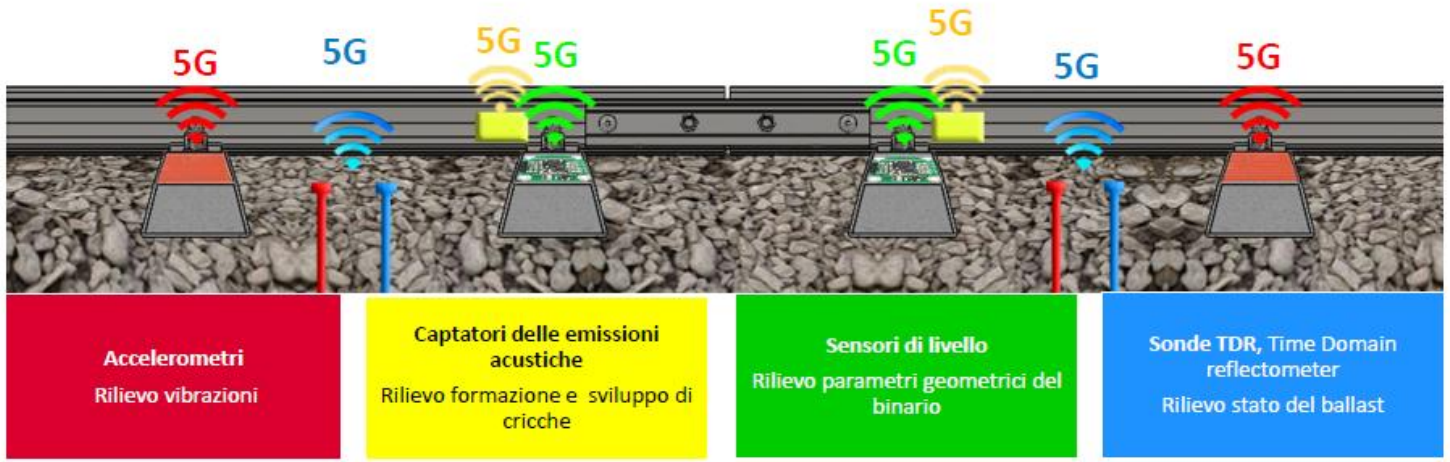
Uno sguardo alle possibili minacce future

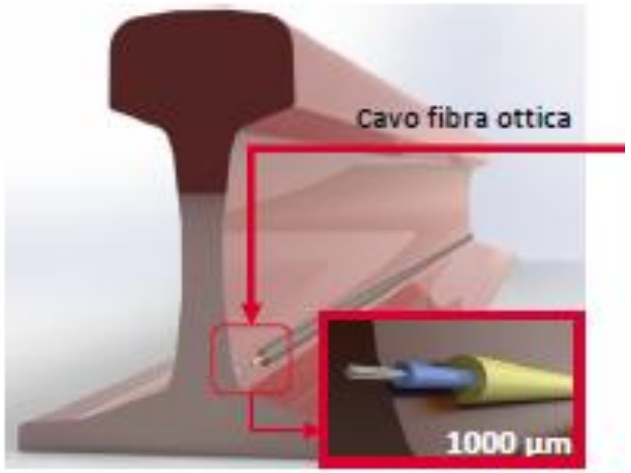
- Sensori **IoT** capillarmente diffusi su infrastruttura e veicoli
- Copertura radio **5G** per invio dati a centri di elaborazione



Supervisione della sede ferroviaria e del binario

- **Monitoraggio continuo** degli elementi base dell'infrastruttura attraverso nodi sensoriali
- **Analisi predittiva** dell'evoluzione nel tempo
- Sensori multipli intelligenti e auto-alimentati
- I dati raccolti vengono **trasmessi in tempo reale** ad un punto di raccolta per la formazione di un database con cui operare attività di diagnostica in remoto.





ANSFISA
AGENZIA NAZIONALE PER LA SICUREZZA DELLE FERROVIE E DELLE INFRASTRUTTURE STRADALI E AUTOSTRADALI

Grazie per l’attenzione!

ANSFISA

AGENZIA NAZIONALE PER LA SICUREZZA DELLE FERROVIE
E DELLE INFRASTRUTTURE STRADALI E AUTOSTRADALI