Mobilità ferroviaria: tecnologie digitali emergenti

La Cybersecurity per i dispositivi a bordo treno e la normativa CRA.

Roberto Bonomi
SELECTRON
Gruppo Knorr-Bremse
roberto.bonomi@selectron.ch

Riccardo Scalisi
SELECTRON
Gruppo Knorr-Bremse
riccardo.scalisi@selectron.ch

21 Maggio 2026

AICQ: Giornata di Studio e Dibattito
Settore AICQ-ETS Trasporto su Rotaia

Agenda

1. Gruppo Knorr-Bremse e Selectron
2. Aspetti Normativi
3. Cybersecurity

Gruppo Knorr-Bremse e Selectron

1

SELECTRON

Traguardi del Gruppo Knorr-Bremse

KNORR-BREMSE

MERAK | MICROELETTRICA

NEW YORK AIR BRAKE | IFE

ZELISKO | RAILSERVICES

SELECTRON | KB SIGNALING

DUAGON | EVAC

Traguardi di SELECTRON

1950 - 1970
Sviluppo di apparecchi acustici e relè temporizzati

1956
Fondazione a Lyss (Svizzera)

1970 - 1980
Produzione di controlli elettronici

1970
Prima votazione elettronica nel Consiglio nazionale svizzero

1985
Specializzazione in controlli elettronici

1974
Primo sistema di controllo (PLC) proprietario, liberamente programmabile

2015
Ingresso nel Gruppo Knorr-Bremse

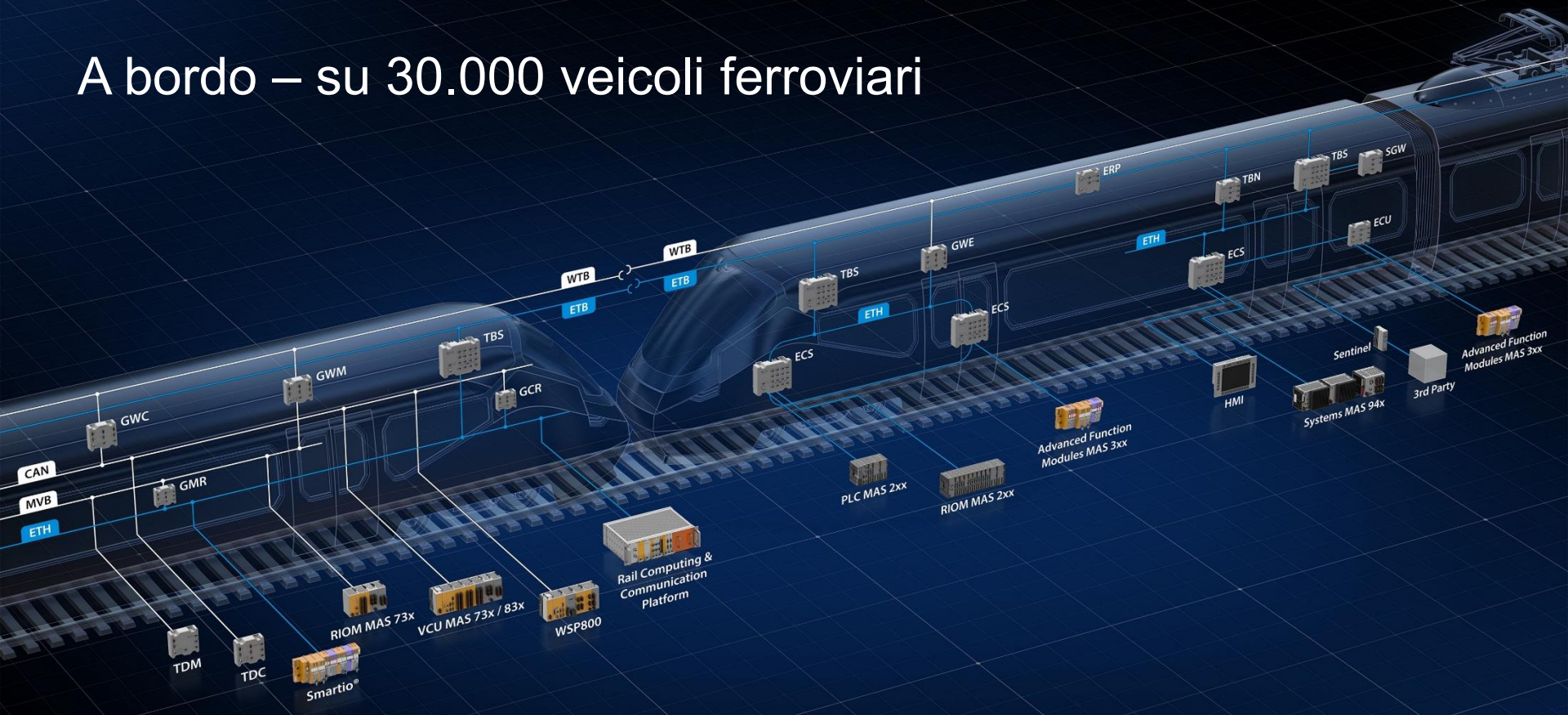
1996
Focus sull'industria ferroviaria

2018
Fondazione del Centro di competenza per la tecnologia di rete (Selectron, Italia)

2017
Fondazione del Centro di competenza per la cybersicurezza

2023
Business Unit Computing & Communication

A bordo – su 30.000 veicoli ferroviari



SELECTRON

Aspetti Normativi

2

Cybersecurity – proteggere un ecosistema ferroviario connesso

Prospettiva europea ...

(Legge sulla Resilienza Cibernetica (CRA)
Norme di prodotto➔ Marcatura CE

REGOLAMENTAZIONE DELLA SICUREZZA

INFORMATICA

EU CRA PRODOTTI	EU NIS2 OPERATORI
Proteggere il mercato europeo da prodotti a basso costo e pericolosi **Norme**: - IEC 62443 - CLC/TS 50701 - IEC 63452 (bozza)	Protezione essenziale / Operatori dei sistemi importanti nell'UE **Norme**: - IEC 62443 - ISO 2700x - Direttive e standard del BSI

➔ La conformità CRA dovrebbe rappresentare la barriera all'ingresso nel mercato europeo in futuro

SELECTRON

Confronto tra il testo giuridico della CRA, la bozza della linea guida della Commissione UE e le linee guida degli esperti UNIFE

Panoramica del testo legale del CRA
Il testo del CRA fornisce il quadro giuridico formale e gli obblighi vincolanti per la conformità.

Linea guida preliminare della Commissione UE
La bozza delle linee guida della Commissione UE offre raccomandazioni non vincolanti per favorire l'attuazione dei requisiti legali della CRA.

UNIFE Expert Guidance
La guida degli esperti UNIFE fornisce consulenza e best practice specifiche per il settore che integrano il quadro giuridico e le bozze delle linee guida.

Chiarimento dello status giuridico
Ogni documento ha uno status giuridico diverso: il testo CRA è vincolante, la bozza UE è consultiva, le linee guida UNIFE sono consultive.

Applicabilità a prodotti con elementi digitali e date chiave

Panoramica della regolamentazione CRA

Il regolamento CRA impone la conformità per i prodotti con elementi digitali per garantire sicurezza e protezione.

Date regolatorie chiave

Il CRA entra in vigore il 10 dicembre 2024, con segnalazione delle vulnerabilità dall'11 settembre 2026 e piena applicabilità dall'11 dicembre 2027.

Ambito di applicabilità

La regolamentazione si applica specificamente ai Prodotti con Elementi Digitali (PDE), influenzando i requisiti di progettazione e rendicontazione.

Bozza UE linea guida CRA

Messaggi chiave rilevanti per il settore ferroviario: valutazione del rischio, modifiche sostanziali, riutilizzo delle prove e mancanza di esenzione ferroviaria

Prodotti progettati prima del CRA

I prodotti progettati prima del Cyber Resilience Act non necessitano automaticamente di un re-design.

Cybersecurity Valutazione del rischio

L'attenzione è posta sulla valutazione dei rischi relativi alla cybersecurity piuttosto che sui processi formali di riprogettazione dei prodotti ferroviari.

Regole per modifiche sostanziali

Modifiche significative ai prodotti danno origine a nuovi obblighi ai sensi del Cyber Resilience Act.

Riutilizzo delle prove

Le prove esistenti di progettazione e test possono essere riutilizzate se il rischio rimane invariato.

Nessuna esenzione ferroviaria

Non esiste ancora un'esenzione esplicita basata su progetti per la ferrovia secondo le normative attuali.

Development, objectives, and legal disclaimer of UNIFE guidance

Sviluppo delle Linee Guida

Le linee guida UNIFE sono state sviluppate in collaborazione dalle principali organizzazioni del settore ferroviario per rispondere alle esigenze del settore.

Disclaimer legale

Le linee guida includono una dichiarazione di non responsabilità legale esplicita che afferma di non essere legalmente vincolante o applicabile.

Obiettivi di Orientamento

Il suo obiettivo è tradurre i concetti CRA in applicazioni ferroviarie pratiche ed evitare interruzioni nelle autorizzazioni e nelle catene di approvvigionamento.

Concetti ferroviari specifici introdotti dalla guida UNIFE

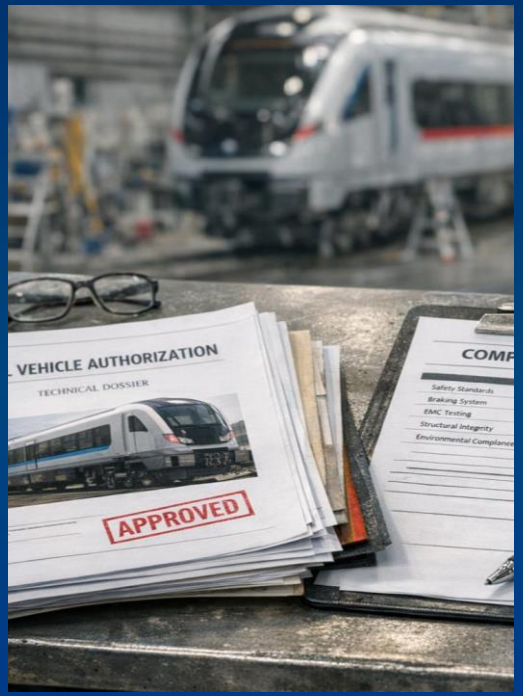
Aree di Conformità Distinte
Le linee guida UNIFE differenziano chiaramente la conformità alla cybersecurity dall'autorizzazione dei veicoli ferroviari.

Visione del ciclo di vita basata su progetti
UNIFE introduce una prospettiva basata su progetti sull'intero processo di gestione del ciclo di vita ferroviario.

Giustificazione basata sul rischio
L'uso di giustificazioni basate sul rischio e accettazione residua del rischio viene sottolineato nelle linee guida.

Gestione del legacy e dell'obsolescenza
Le linee guida trattano approcci pratici per prodotti legacy, obsolescenza e gestione dei pezzi di ricambio.

Separazione della conformità CRA dall'autorizzazione dei veicoli ferroviari e punti chiave



Separazione dalla conformità CRA
La conformità CRA è indipendente dall'autorizzazione dei veicoli ferroviari, chiarendo le responsabilità normative.

Ruolo dell'ERA e delle NSA
ERA e NSA verificano la dichiarazione CRA nel DoV EC ma non valutano tecnicamente la conformità CRA.

Validità delle autorizzazioni esistenti
La CRA non invalida i tipi di veicoli ferroviari autorizzati prima dell'11 dicembre 2027, garantendo la stabilità della transizione.

Impatto sui produttori
Questa chiarezza è fondamentale per i produttori di materiale rotabile comprendere i limiti di conformità e autorizzazione.

Linee guida UNIFE per mitigazioni pratiche e conformità a livello di prodotto

Nessuna invalidazione automatica
I tipi di veicoli esistenti non saranno automaticamente invalidati secondo le nuove linee guida, preservando i beni legacy.

Conformità CRA a livello di prodotto
La conformità CRA viene gestita a livello di prodotto attraverso valutazioni approfondite del rischio e giustificata non applicabilità.

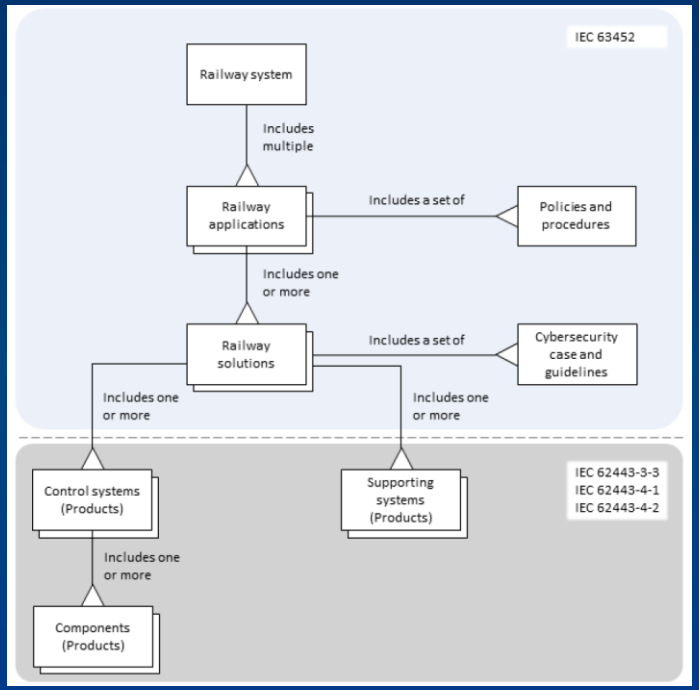
Compatibilità con sistemi legacy
Garantire la compatibilità tra i nuovi standard e i sistemi ferroviari legacy per facilitare un'integrazione fluida.

Flotte miste consentite
Le flotte miste composte da veicoli preCRA e postCRA sono autorizzate a operare insieme sotto questa linea.

Cybersecurity – proteggere un ecosistema ferroviario connesso

Sicurezza Industriale (IEC62443) vs Sicurezza Ferroviaria (IEC63452)

- IEC 63452 è la standardizzazione della specifica tecnica TS 50701
- Adatta i requisiti della serie di standard IEC 62443 ai sistemi ferroviari
- fornisce indicazioni su come il processo di sicurezza possa essere interfacciato con il ciclo di vita generico della RAM (IEC 62278)
- Supporto alla gestione del rischio per proteggere gli interessi critici dagli attacchi informatici
- Fornitura di linee guida per la garanzia della sicurezza durante le fasi di costruzione, gestione e manutenzione
- Definisce i punti di sincronizzazione tra gli stakeholder e propone responsabilità
- Si basa sulla norma IEC 62443-4-x per la valutazione della conformità di fornitori e prodotti



Cybersecurity – proteggere un ecosistema ferroviario connesso

Requisiti del Cyber Resilience Act (CRA) 1/3

1. **Sicurezza per progettazione e per default**
   - Assenza di password deboli o predefinite
   - Disabilitazione di servizi e interfacce non necessarie
   - Configurazione di rete sicura a partire dalla messa in servizio
2. **Analisi del rischio e requisiti essenziali**
   - Protezione contro accessi non autorizzati
   - Garantire l'integrità di software e firmware
   - Protezione dei dati
   - Resilienza agli attacchi di rete
3. **Processo di sviluppo sicuro**
   - Secure Boot
   - Firma applicativa e firmware
   - Gestione sicura delle chiavi (PKI, HSM)
   - Test di sicurezza (scansioni delle vulnerabilità, test di penetrazione)

Cybersecurity – proteggere un ecosistema ferroviario connesso

Requisiti del Cyber Resilience Act (CRA) 2/3

4. **Gestione delle vulnerabilità e aggiornamenti**
   - Capacità di correggere vulnerabilità
   - Aggiornamenti di sicurezza sicuri
   - Protezione contro il rollback
   - Questi obblighi si applicano per tutta la durata di supporto dichiarata del prodotto.
5. **Vulnerabilità e notifica degli incidenti**
   - Vulnerabilità attivamente sfruttate
   - Gravi incidenti di sicurezza che hanno colpito il prodotto
6. **Documentazione tecnica e SBOM**
   - Documentazione tecnica sulla cybersecurity
   - Una Distinta Base del Software (SBOM) per garantire la trasparenza nella catena di approvvigionamento software

Cybersecurity – proteggere un ecosistema ferroviario connesso

Requisiti del Cyber Resilience Act (CRA) 3/3

7. **Valutazione della conformità e marcatura CE**
   - Valutazione della conformità CRA
   - Dichiarazione di conformità dell'UE→ Questo è un prerequisito per l'applicazione del marchio CE e l'accesso al mercato europeo.
8. **Sicurezza nel ciclo di vita**
   - Monitoraggio delle vulnerabilità
   - Gestione degli Incidenti
   - Mantenere il livello di sicurezza fino alla fine della vita del prodotto

Cybersecurity

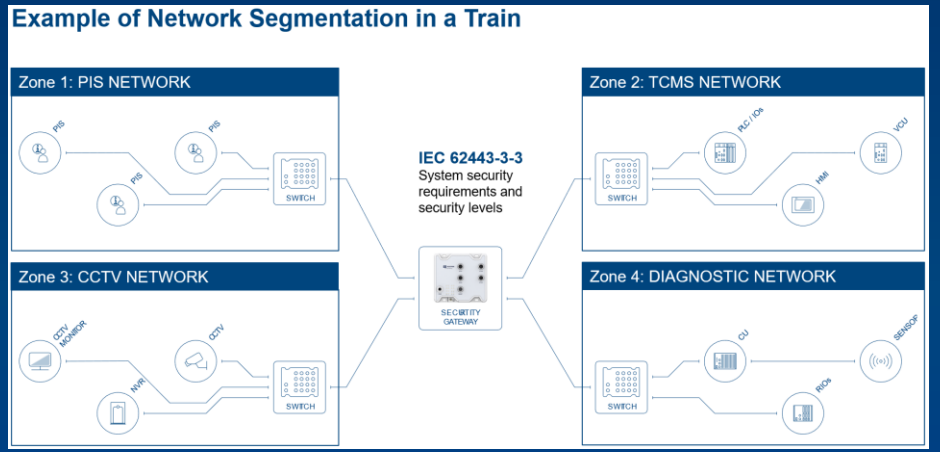
SELECTRON

Cybersecurity – proteggere un ecosistema ferroviario connesso

Un approccio olistico…

- Concetto di difesa in profondità per la sicurezza
  Composto da diversi strati di protezione
- Processo di sviluppo prodotto sicuro secondo IEC 62443-4-1
- Diverse aree protette da security gateway (SGW)
  Accesso sicuro
- Certificati di Sicurezza e PKI
  Assegnare identità digitali a dispositivi e software, incluse le applicazioni client

- Sistema di Allerta Precoce con Soluzione di Rilevamento Minacce (TDS)
  Rilevamento di anomalie nel traffico dati



Massima sicurezza tramite "Cybersecurity by design"

SELECTRON

Cybersecurity ferroviaria - Esempio:

Analisi strutturata dei rischi

Protezione della configurazione del sistema utilizzando « Hardware Secure Modules » (HSM)

Caratteristiche meccaniche
- Inviluppi rigidi, viti di sicurezza
- Rilevamento di manipolazione (interfacce sigillate, lacca/colla, punti di rottura predeterminati)

Produzione sicura
- Area esclusiva di Selectron all'interno dell'EMS
- Ambiente controllato per la gestione degli « e-fuse » di sicurezza
- Distribuzione dei Certificati di Identificazione dei Dispositivi

SCPU 201-TW

Cybersecurity ferroviaria - Esempio:

Firma delle Applicazioni per un PLC Selectron

-Sicurezza a ogni livello - Software

Comunicazioni Sicure

- Comunicazione di sistema criptata (OPC UA, HTTPS)
- Supporto alla segmentazione di rete (VLAN)
- Protezione base dal DoS tramite limitazione di rate o frame
- Disabilitate interfacce fisiche o logiche non utilizzate

Imposizione delle autorizzazioni

- Gestione account con ruoli e utenti personalizzabili

Funzionalità di backup migliorate

Log di sicurezza

Crittografia per la protezione dei dati

- Crittografia a livello di filesystem per garantire l'autenticità di configurazioni e dati

Cybersecurity ferroviaria - Esempio:

Firma delle Applicazioni per un PLC Selectron

Sicurezza ad ogni livello – Secure Boot / IEC-Application

Autenticazione software
- Solo il software Selectron autentico viene avviato sui dispositivi

Protezione Rollback
- Il software superato non può essere ricaricato una volta effettuato un aggiornamento

Integrazione dell'applicazione IEC del cliente
- Servizio di firma utilizzando la PKI Selectron
- Autorizzazione basata sul progetto specifico

Hardware basato sul “root of trust”
- Segreti memorizzati o garantiti da HSM

Firme digitali generate tramite PKI
- Nessuna chiave privata incorporata nel dispositivo

Opzioni di sviluppo
- Le funzionalità possono essere attivate/disattivate
- Consente processi di sviluppo semplificati

Cybersecurity ferroviaria - Esempio:

Firma delle Applicazioni per un PLC Selectron

Sicurezza ad ogni livello – Secure System Communication

OPC UA
- Comunicazione di sistema standardizzata
- Endpoint non sicuri opzionali per scopi di sviluppo/monitoraggio

Gestione utente basata sui ruoli e completamente configurabile

Certificati server
- Possibilità di installare certificati clienti
- Truststore separato per gli strumenti

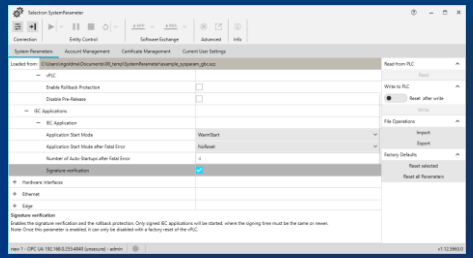
OPC è lo standard di interoperabilità per lo scambio sicuro e affidabile di dati nel settore dell'automazione industriale e in altri settori. È indipendente dalla piattaforma e garantisce il flusso fluido delle informazioni tra dispositivi provenienti da più fornitori.

Cybersecurity ferroviaria - Esempio:

Firma delle Applicazioni per un PLC Selectron

Garantire l'autenticità e l'integrità dell'applicazione IEC

- Processo di firma digitale delle applicazioni IEC e verifica di questi certificati durante il processo di avvio.
- Questo certificato digitale protegge il codice IEC e i dati di configurazione del PLC
- Se questo meccanismo di protezione viene attivato, vengono avviate solo le Applicazioni IEC con firma valida.
- Per la protezione contro il rollback, viene controllato un timestamp della firma dell'applicazione IEC e, confrontandola con l'applicazione attualmente caricata, vengono avviate solo le applicazioni più recenti.
- La firma include un ID di progetto, sono consentiti solo gli aggiornamenti dello stesso progetto.



SELECTRON

Cybersecurity ferroviaria - Esempio:

Rilevamento intelligente di minacce e anomalie a bordo tramite la rete Ethernet (Switch/Router) e non solo… (anche per CAN e MVB)

- Analisi in tempo reale del traffico di rete a bordo
- Apprendimento dal comportamento del sistema (Machine Learning)
- Rilevamento delle anomalie comportamentali (IA)
- Rilevamento precoce di minacce informatiche note e sconosciute
- Correlazione intelligente degli eventi
- Funzionamento autonomo a bordo
- Allarmi contestuali
- Miglioramento continuo attraverso l'apprendimento

ECS/TBS/TBN

SGW

TDC/TDM

Mobilità ferroviaria: tecnologie digitali emergenti

La Cybersecurity per i dispositivi a bordo treno e la normativa CRA.

Roberto Bonomi
SELECTRON
Gruppo Knorr-Bremse
roberto.bonomi@selectron.ch

Riccardo Scalisi
SELECTRON
Gruppo Knorr-Bremse
riccardo.scalisi@selectron.ch

21 Maggio 2026

AICQ: Giornata di Studio e Dibattito
Settore AICQ-ETS Trasporto su Rotaia