
# THREAT DETECTION SOLUTION

## NETWORK INTRUSION DETECTION SYSTEM (IDS) FÜR SCHIENENFAHRZEUGE

Schutz vor Cyberangriffen auf Eisenbahnen. Proaktiv handeln, bevor Schaden angerichtet wird – dank frühzeitiger Gefahrenerkennung durch Echtzeit-Überwachung des Netzwerkverkehrs. Für einen sicheren und verfügbaren Bahnverkehr.

SELECTRON


**Cyber-Bedrohungen im digitalen Zeitalter**
Die Digitalisierung der Bahn ist in vollem Gange und ermöglicht die Einführung neuer und intelligenter Technologien. Eine rasante Entwicklung, verbunden mit bedeutenden Vorteilen für den Schienenverkehr. Gleichzeitig entstehen aber auch neue Cyber-Bedrohungen, die es zu bewältigen gibt. Durch die zunehmende Vernetzung und Verwendung offener Standards sind Bahnnetze anfälliger für das Risiko von Cyberangriffen. Angesichts der sich rasant entwickelnden und ausgeklügelten Cyber-Bedrohungslandschaft muss die kritische und sensible Bestandsinfrastruktur gegen bekannte und neuartige Bedrohungen geschützt werden. Die Auswirkungen eines Cyberangriffs können sehr schwerwiegend sein: Es stehen nicht nur finanzielle und imageschädigende Folgen auf dem Spiel – auch Menschenleben können in Gefahr sein.

**Erfüllen Sie die regulatorischen Anforderungen?**
Um die Auswirkungen von Cyber-Risiken zu begrenzen, sind Bahnbetreiber gesetzlich verpflichtet, sich mit der Cyber-Resilienz ihrer Infrastruktur auseinanderzusetzen. Vorschriften wie die EU-NIS-Direktive schreiben Schutzvorkehrungen für kritische Infrastrukturen – darunter auch die Bahn – vor. Dazu gehört die Überwachung der Flotten auf potenzielle Cyberattacken während des Betriebs und die Meldung von Sicherheitsverstössen. Das Nichteinhalten geltender Vorschriften kann hohe Strafen zur Folge haben. Für Bahnbetreiber ist es deshalb entscheidend, ihre Bahnnetze aktiv zu überwachen und zu schützen.

**Wie können Sie Ihre Eisenbahnen schützen?**
Threat Monitoring ist eine unerlässliche Sicherheitsmassnahme, um Cyber-Bedrohungen aktiv entgegenzuwirken und das Risiko einer Nichteinhaltung von Gesetzen und Vorschriften zu beseitigen – denn unüberwachte Systeme sind ungesicherte Systeme.

# Network Intrusion Detection – So funktioniert es

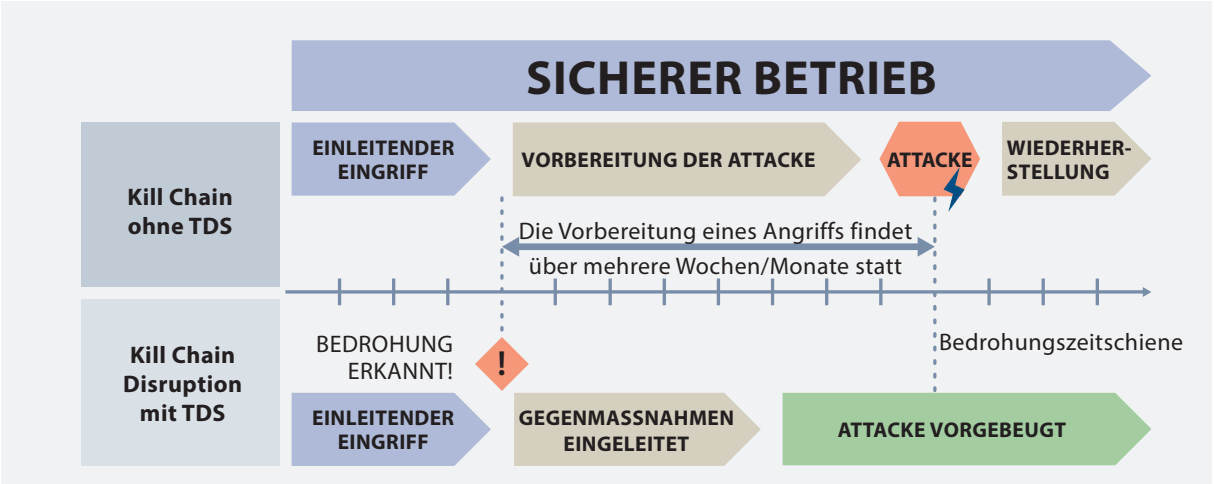
Das Selectron TDS ist ein speziell für Schienenfahrzeuge entwickeltes Angriffserkennungssystem, auch bekannt als Network Intrusion Detection System (IDS). Die Threat Detection Solution ist ein entscheidendes Instrument zur Bewältigung der einzigartigen Cyber Security Herausforderungen in der Bahnindustrie – denn Schutz von innen, ist Schutz nach aussen.

**Schützt Eisenbahnen vor Cyberattacken durch:**

1. **Überwachung** der Netzwerk-Systemaktivität
2. **Erkennen** von Anomalien im Netzwerkverkehr
3. **Analyse** verdächtiger Aktivitäten mit Hilfe der verhaltensbasierten Anomalieerkennung (Behavioral Anomaly Detection)
4. **Identifizierung** von Bedrohungen in der frühen Angriffsphase
5. **Meldung von Eindringungsversuchen** durch Senden einer Warnmeldung

**Keine Chance für Cyberangriffe mit Selectron TDS:**

- ✓ Eigenständige, zertifizierte Lösung für Neu- und Bestandsflotten
- ✓ Basiert auf maschinellem Lernen
- ✓ Flexibel, optimiert und ständig aktualisiert
- ✓ Entdeckt Verhaltensanomalien
- ✓ Entdeckt selbst Zero-Day-Schwachstellen




**Erfahren Sie mehr**

**Das Selectron TDS unterstützt Bahnbetreiber bei der Angriffsprävention sowohl für Neu- wie auch Bestandsflotten und ermöglicht das schnelle Einleiten von Gegenmassnahmen zur raschen Wiederherstellung eines sicheren Betriebs.**

# Holistische Cyber Security Architektur

Die holistische Cyber Security Architektur von Knorr-Bremse & Selectron kombiniert Safety-zertifizierte Bahn-Hardware mit leistungsfähigen Cyber Security Funktionen für Bestands- und Neusysteme.

Die Threat Detection Solution ist ein wesentliches Element innerhalb unserer holistischen Cyber Security Architektur. Das TDS schützt Ihre kritischen TCMS-Komponenten und ermöglicht es Ihnen, die Betriebssicherheit Ihres Kontrollsystems in Echtzeit zu überwachen.

Um einen Defense-in-Depth Schutz für Ihre Eisenbahnen sicherzustellen, lässt sich das Frühwarnsystem mit weiteren Lösungen aus unserem Cyber Security Portfolio ergänzen. Alle Komponenten werden nach den Anforderungen der IEC 62443 entwickelt und nutzen die unterschiedlichen Elemente unserer Sicherheitsarchitektur (u.a. PKI für Identitätsmanagement, Secure Boot und Integritätsprüfung).

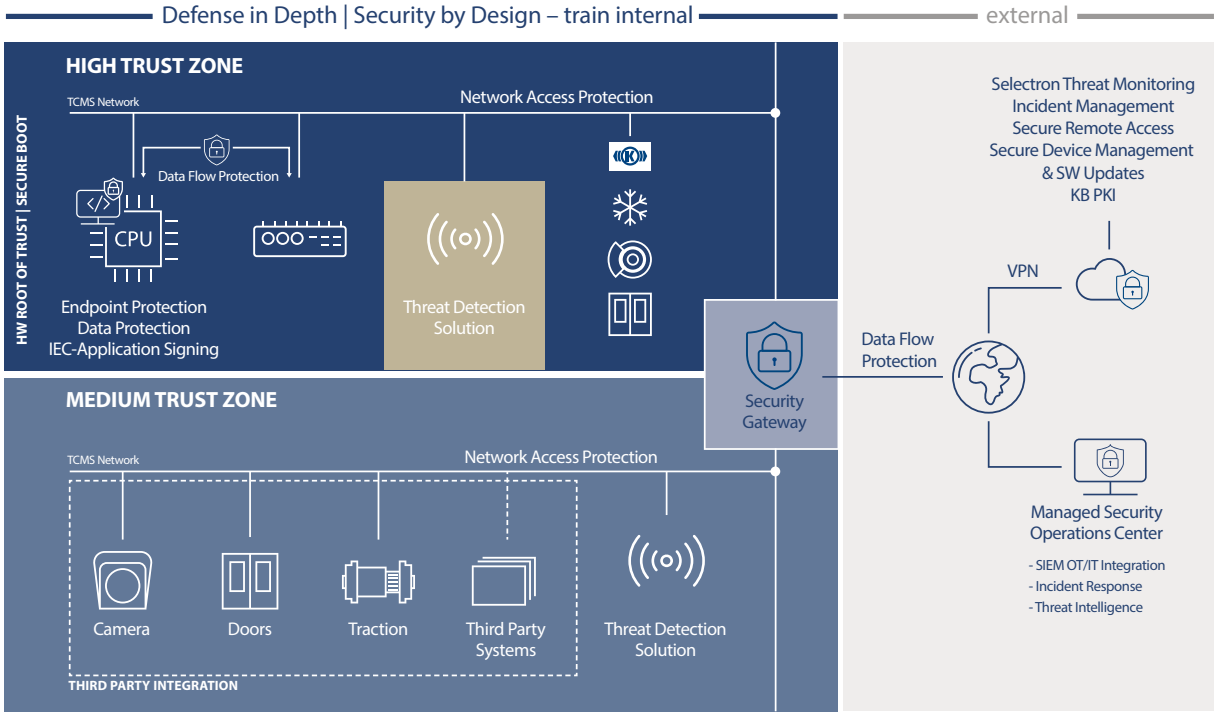
Dazu gehört die IEC-Anwendungssignierung, die die Vertraulichkeit und Authentizität der Anwendung jederzeit sicherstellt. Die Gefahr einer unbefugten Nutzung mit gehackten und manipulierten Anwendungen wird vermieden und das geistige Eigentum ist geschützt.

Die frühzeitige Entdeckung und Meldung von Anomalien ist für Bahnbetreiber massgebend, um Cyberangriffe zeitnah zu verhindern und die rechtlichen Vorschriften zur Cybersicherheit einzuhalten. Entscheidend ist die Entdeckung der Bedrohungen in der frühen Angriffsphase.

Innerhalb des Defense-in-Depth Ansatzes übernimmt das TDS die „Detection"-Funktion, die von der EU-NIS-Richtlinie, den IEC 62443 und TS50701 Standards und anderen Frameworks, wie dem NIST, gefordert wird.

Das TDS arbeitet auf zertifizierter Bahnhardware und wird eine Vielzahl von bahnspezifischen Protokollen abdecken, darunter alle relevanten Protokolle von Selectron und diejenigen der Knorr-Bremse Lösungen (Türen, HVAC, Bremsen und mehr).

Sein modulares und skalierbares Konzept ermöglicht sowohl eine optimale Integration in neue Flotten als auch die kostengünstige Nachrüstung bestehender Flotten.



# Funktionalitäten

- Erkennt und analysiert Anomalien im Netzwerk-verkehr mittels fortschrittlicher Heuristik, um die Gefahr schnellstmöglich einzudämmen, bevor der Angriff erfolgt
- Erkennungsregeln werden bei der Entdeckung neuer Security-Schwachstellen fortlaufend aktualisiert
- Zentralisierte und dokumentierte Ereignisverwaltung in der Cloud, mit Informationen von TDS-Sensoren in verschiedenen Netzwerken
- Die gesammelten Ereignisprotokolle ermöglichen eine schnelle und gründliche forensische Analyse und Risikobewertung im Falle eines Sicherheitsverstosses – mit schneller Lösungsfindung
- Ereignisinformationen sind gegen Manipulation gesichert, so dass Sie sie bei Bedarf unter Einhaltung der Chain-of-Custody-Vorschriften verwenden können.
- Warnmeldungen können von einer Backend-Komponente empfangen und auf einem grafischen Dashboard visualisiert werden
- Individuelle Zugangsdaten für alle TDS-Dienste (einschliesslich der cloud-spezifischen)
- Daten sind stets verschlüsselt – ob im Ruhezustand oder während der Übertragung
- Einfache Installation mit passiven Plug-and-Play-Sensoren und einem optimierten Konfigurationskonzept
- Überwachung von modernen und älteren Bahnnetzwerken: CAN, MVB und zukünftig auch Ethernet
- Kann in passivem Modus betrieben werden, ohne Beeinflussung des Zugleitsystems
- Standardschnittstellen ermöglichen die Übernahme von Informationen in Ihr SIEM/SOC, um die Cyberabwehr Ihrer Flotte zu verbessern
- Optionales Rail SOC für Security Operations & Intelligence kann als Managed Service angeboten werden
- Flexible Lösungen:
  - Lokale (Local) Version: Autonomes System basierend auf einer Whitelist
  - Erweiterte (Advanced) Version: Erweitertes IDS basierend auf maschinellem Lernen mit Cloud-Anbindung

## Die Vorteile auf einen Blick

- ✓ **Ermöglicht die Einhaltung von rechtlichen Vorschriften wie der EU-NIS-Direktive**
- ✓ **Rückwirkungsfreie Implementierung in Neu- und Bestandsflotten, ohne Neuzertifizierung des Fahrzeugs**
- ✓ **Sicherstellung der Verfügbarkeit und Sicherheit des Bahnbetriebs durch Aufbau eines effizienten Schutzschildes gegen Cyber-Bedrohungen**
- ✓ **Defense-in-Depth Schutz in Kombination mit anderen Cyber Security Lösungen von Selectron**
- ✓ **Schützt Ihre kritischen Vermögenswerte, einschliesslich Ihres Images und Ihres geistigen Eigentums**
- ✓ **Eine unterstützende Massnahme zur Erfüllung der EN50129:2019 Security Anforderungen und die einzige Lösung, welche die Security verbessert ohne andere Geräte anpassen zu müssen**

**Selectron Systems AG**
Bernstrasse 70
3250 Lyss
Schweiz
Phone: +41 32 387 61 61
Fax: +41 32 387 61 00
selectron.ch

KNORR-BREMSE

NEW YORK AIR BRAKE

IFE

MERAK

MICROELETTRICA

SELECTRON

KIEPE ELECTRIC

EVAC

ZELISKO

RAILSERVICES