



# THREAT DETECTION FOR LEGACY NETWORKS

## NETWORK INTRUSION DETECTION SYSTEM (IDS) FOR RAIL VEHICLES

Secures trains against cyberattacks through real-time network monitoring, detecting cyber threats before any damage is done. Designed to ensure availability and security of train operations.



**SELECTRON**

Automating and securing trains today.  
Empowering a smarter and safer mobility tomorrow.  
Because security and safety go hand in hand.



#### **Cybersecurity vulnerabilities in the digital age**

Digitalization of the railway is advancing and enabling the introduction of new and smart technologies. This brings along many significant benefits to the industry, but train networks are increasingly more susceptible to the risk of cyber threats as a result of ubiquitous networks and the use of open standards. With cyberattacks on the rise, critical and vulnerable legacy infrastructure is in danger and needs to be protected against both known and emerging threats. The impacts of a cyberattack can be very serious: Not just financial and reputational damage is at stake, but lives can be endangered.



#### **Are you complying with regulatory requirements?**

To limit the impact of cyber risks, regulatory bodies require rail operators to address the cyber-resilience of their infrastructure. Regulations such as the EU NIS Directive stipulate protective measures for critical infrastructures – including rail transport services. This includes monitoring fleets for potential cyberattacks during operation and reporting breaches after discovery. Non-compliance with applicable regulations can result in heavy penalties. This is making it crucial for rail operators to actively monitor and secure their train networks.







#### **What can you do to protect your trains?**

Threat monitoring is an essential protective measure to combat cybersecurity threats and ensure compliance with regulations – because unmonitored systems are unsecured systems.

# Network Intrusion Detection – This is how it works

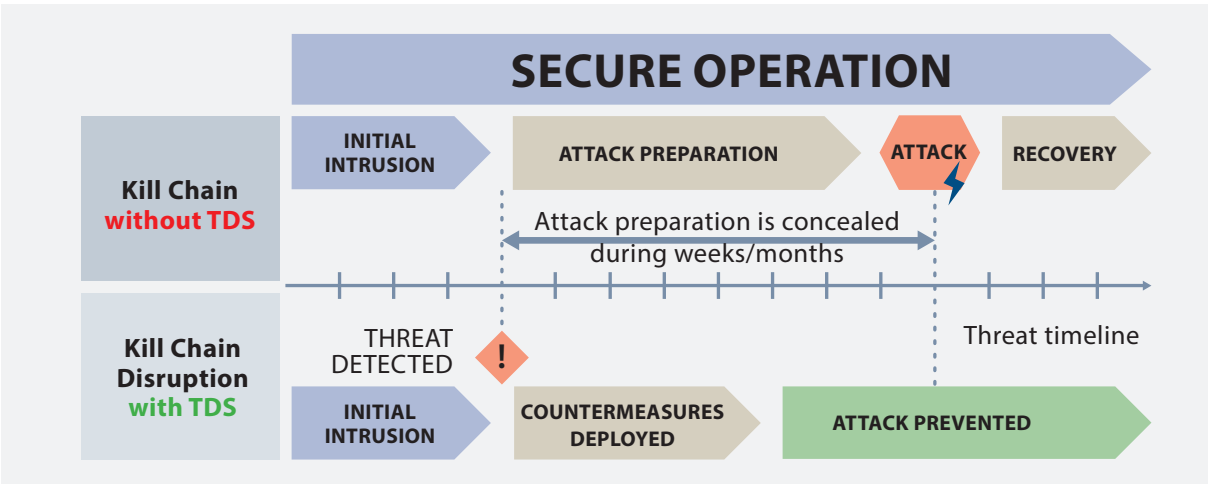
The Selectron Threat Detection Solution (TDS) is a Network Intrusion Detection System (IDS) for rail vehicles. Developed to address the unique cybersecurity challenges of the rail industry – because protection from inside, is protection to the outside.

**Prevents cyberattacks by:**

-  **1. Monitoring** network system activity
-  **2. Detecting** anomalies in the train network traffic
-  **3. Analyzing** suspicious activity using Behavioral Anomaly Detection
-  **4. Identifying** threats in the early reconnaissance phases
-  **5. Reports** intrusion attempt by sending an alert

**Cyber-risk-ready with Selectron TDS:**

- ✓ Standalone certified solution for new and legacy fleets
- ✓ Machine Learning-based
- ✓ Flexible, optimized and constantly updated
- ✓ Detects behavioral anomalies
- ✓ Able to discover even zero-day vulnerabilities



Learn more



The Selectron TDS empowers operators to prevent attacks in new and legacy fleets and to deploy rapid containment measures to rapidly restore secure operations.

# Holistic Cybersecurity Architecture

The Knorr-Bremse & Selectron holistic cybersecurity architecture combines safety-certified train hardware with powerful cybersecurity features for legacy and new systems.

The Threat Detection Solution is a key element within our holistic cybersecurity architecture. Besides protecting critical devices of your TCMS, you can now monitor operational security of your control system in real-time.

To ensure a defense in depth protection for your trains, our intrusion detection system can be combined with other solutions from our cybersecurity portfolio. Developed according to IEC 62443, it guarantees a holistic approach and allows integration with other elements of our security architecture, such as the PKI for identity management, secure boot and integrity verification.

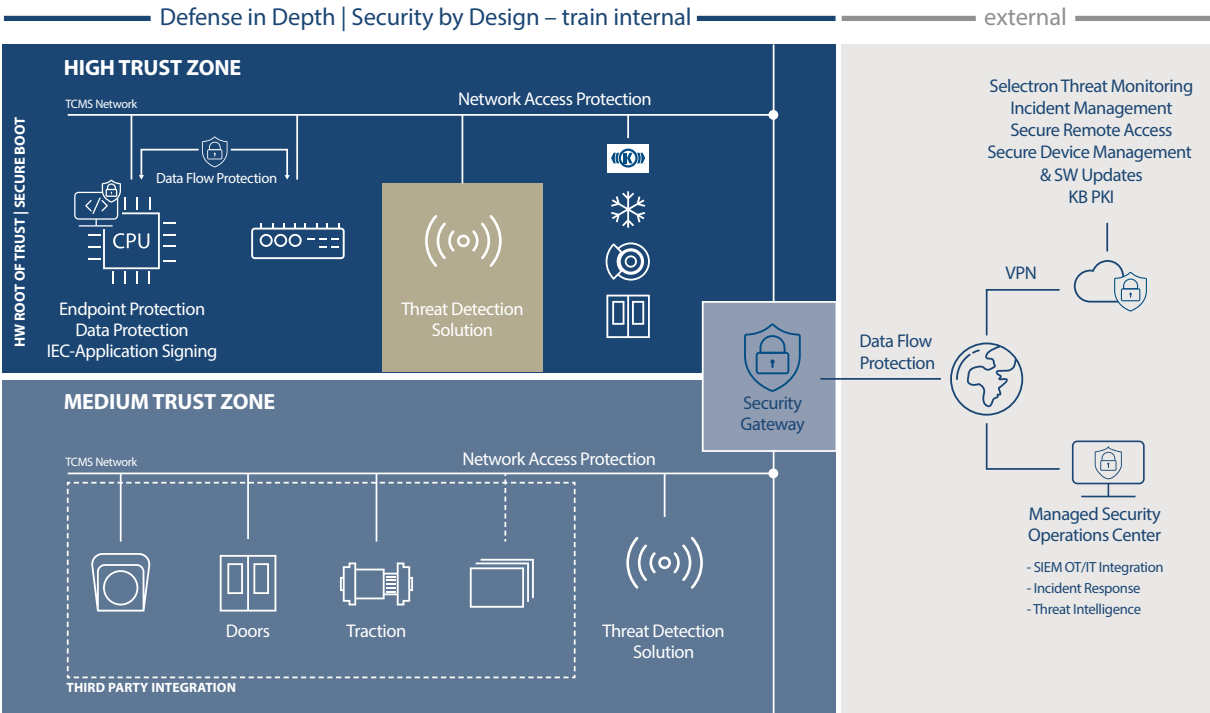
This includes IEC application signing, which ensures the confidentiality and authenticity of the application at all times. The threat of unauthorized use with hacked and manipulated applications is avoided and the intellectual property is protected.

Early detection and reporting of anomalies is imperative for rail operators to prevent cyber attacks in a timely manner and to comply with cybersecurity regulations. Discovering threats in the early research phase is crucial.

As part of our defense in depth approach, the TDS provides the DETECT function required by the EU NIS Directive, the IEC 62443 and TS50701 standards as well as other frameworks such as NIST.

The TDS runs on certified rail hardware and will cover a variety of train-specific protocols, including all relevant protocols from Selectron and those of Knorr-Bremse solutions (doors, HVAC, brakes and more).

Its modular and scalable concept allows both optimum integration into new fleets as well as cost-effective retrofitting of existing fleets.



## Functionalities

- Uses advanced heuristics to detect and analyze anomalies in the train network traffic, allowing quick remediation before the attack materializes
- Continuously updates detection rules when new vulnerabilities are discovered
- Centralized and documented event management in the Cloud, with information from TDS sensors in various networks
- Collected event logs allow for a fast and thorough forensic analysis and risk assessment in case of breach – with rapid resolution
- Event information is secured against tampering, allowing you to use it while respecting chain of custody rules, if required
- Alerts can be received by a backend component and visualized on a graphical dashboard
- All TDS services, including cloud specifics, are access-controlled with customer-specific credentials
- Data at rest and in transit is always encrypted
- Installation is straightforward with plug and play passive sensors and an optimized configuration concept
- Monitoring of modern and legacy train networks: CAN, MVB and also Ethernet in the future
- Can run in passive mode, so it never interferes with train control processes
- Standard interfaces allow feeding information into your SIEM/SOC to improve your fleet's cyberdefense
- Optional Rail SOC for security operations and intelligence can be provided as a managed service
- Flexible solutions:
  - Local: Autonomous system based on a whitelist
  - Advanced: Enhanced IDS with machine learning capabilities through a cloud connection

### Key benefits at a glance

- ✓ Ensures compliance with regulations such as the EU NIS Directive
- ✓ Simple implementation in new and legacy fleets without requiring recertification of the vehicle
- ✓ Ensures availability and security of train operations by building an efficient defense shield against cyber threats
- ✓ Defense in depth protection in combination with other Selectron cybersecurity solutions
- ✓ Preserves your critical assets, including your reputation and your intellectual property
- ✓ The only solution to improve security without having to touch other devices and a supporting measure to comply with the EN50129:2019 security requirements

## **Selectron Systems AG**

Bernstrasse 70

3250 Lyss

Schweiz

Phone: +41 32 387 61 61

Fax: +41 32 387 61 00

[selectron.ch](http://selectron.ch)



---

 **KNORR-BREMSE**

---

 **NEW YORK AIR BRAKE**

---

 **IFE**

---

 **MERAK**

---

 **MICROELETTRICA**

---

 **SELECTRON**

---

 **EVAC**

---

 **ZELSKO**

---

 **RAILSERVICES**

---