irdeto

Solution Overview

Irdeto Anomaly Detection System

The only way to protect connected and legacy operational control systems with early warning of cyberattacks.

The frequency of cyberattacks on the connected transport industry is on the rise. Digital connected technologies, however, reduce costs and help serve customers better – but are realized by complex, coexisting and interwoven systems. With every new connected service added, new opportunities are exposed to attackers for exploitation. That's why it is important to extend protection beyond production to the operating life of vehicles as well.

Threats

- OT tampering or degradation
- OT settings changed or misconfigured
- Intellectual Property lifted
- Unknown / malicious software installed
- Unknown / untrusted devices in the OT network

Impact

- Disruption in service operation
- Reduced availability of assets
- Passenger discomfort, disorder or panic
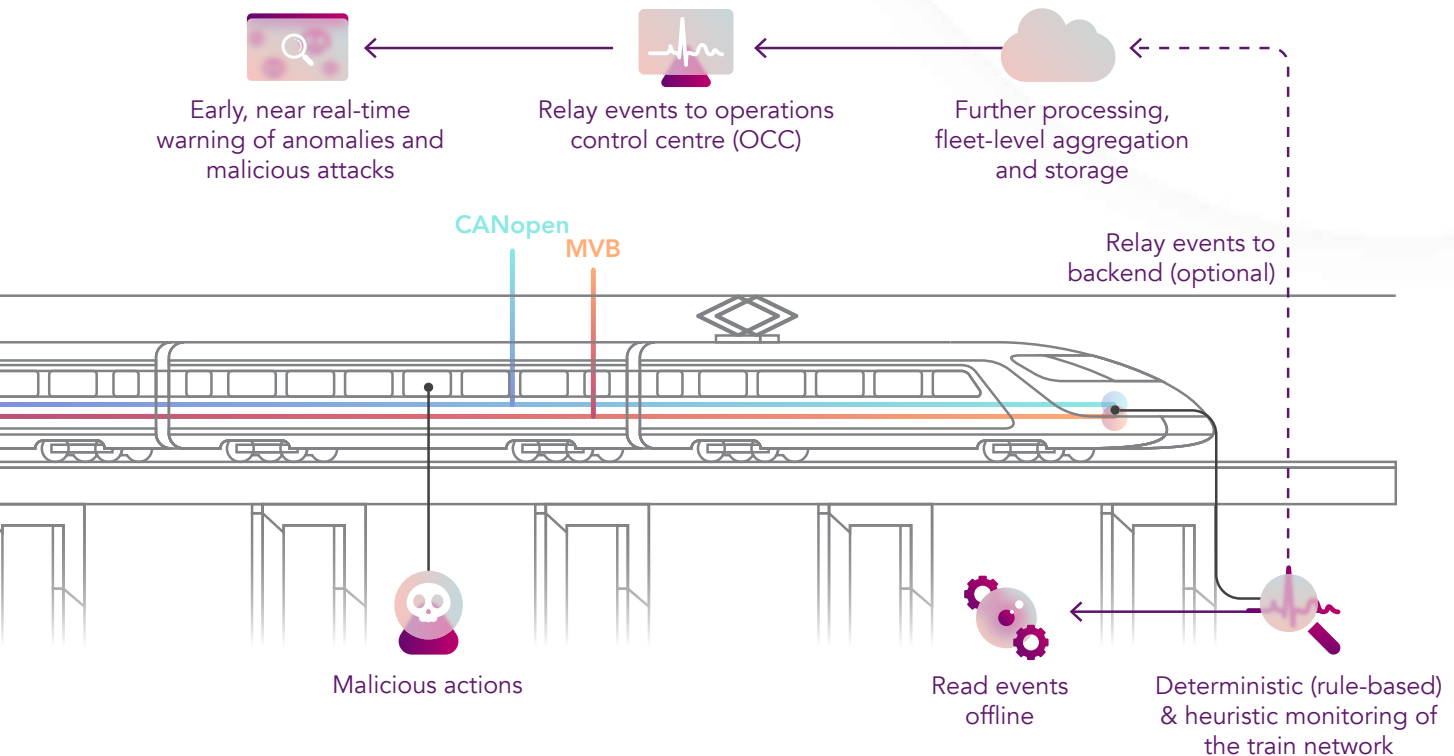- Reputation and brand damage
- Increased OPEX

KEY BENEFITS OF IRDETO ANOMALY DETECTION SYSTEM

Managing crises and incidents is part of the daily business in the railway sector. Irdeto helps introduce cyber resilience to manage your cyber risks and incidents.
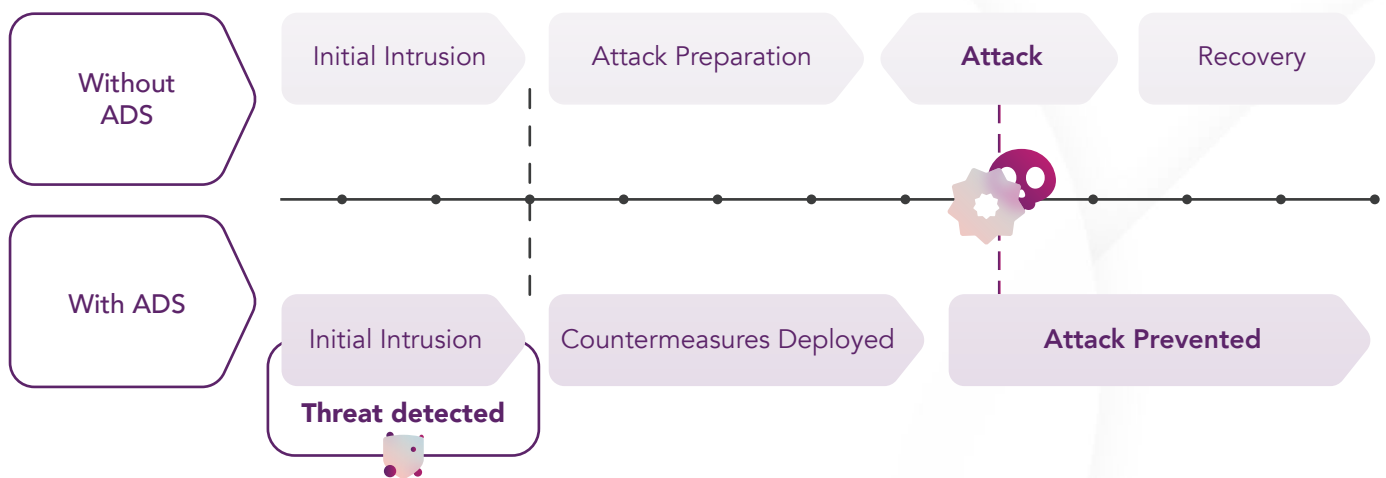
- Ensures availability and security of railway operations by building an early warning system against cyberthreats
- Preserves critical assets, including reputation and intellectual property – even from zero-day threats
- Simple implementation in new and legacy fleets without recertification of the vehicle
- Ensures compliances with existing and upcoming regulations, such as the EU NIS and NIS 2 directives
- Provides defense in depth protection in combination with other Irdeto cybersecurity solutions
- The only self-protecting system that works both with and without connectinvity

HOW DOES ANOMALY DETECTION SYSTEM WORK?

Early, near real-time warning of anomalies and malicious attacks

Relay events to operations control centre (OCC)

Further processing, fleet-level aggregation and storage

Relay events to backend (optional)

CANopen

MVB

Malicious actions

Read events offline

Deterministic (rule-based) & heuristic monitoring of the train network

HOW ANOMALY DETECTION HELPS FIGHT CYBERTHREATS?

Without ADS	Initial Intrusion	Attack Preparation	**Attack**	Recovery

With ADS	Initial Intrusion	Countermeasures Deployed	**Attack Prevented**

Threat detected

SELECTRON

Selectron Systems AG, the system solution arm for safe and secure Train Control & Management Systems (TCMS) of the Knorr-Bremse Group, selected Irdeto Anomaly Detection System to become a key software component of Selectron's Threat Detection Solution (Selectron TDS), which will be available in 2021.

FEATURES AT A GLANCE

Operating Modes
- Rule-based deterministic
- Behavioral machine learning
- Online with cloud analysis
- Offline with on-board analysis
- Hybrid with federated on-board analysis

Network Support
- CAN, CANopen, J1939
- Ethernet
- MVB

Event Handling
- On-board storage, cloud storage
- SIEM / SOC / OCC relay
- Operator dashboard

Self-Protection
- Anti Reverse Engineering
- Active Anti-Debug, Anti-Hook & Anti-Tamper

Standards Compliance
- IEC 62443 (SL-2)
- TS 50701

Irdeto is the world leader in digital platform security offering cyber services and technology solutions that protect platforms, digital assets and software applications across multiple industries. Irdeto's products meet the rapidly changing mobility demands and exceed cybersecurity regulations for automotive, rail and beyond. We provide solutions throughout the product lifecycle to prevent cyberattacks and help protect assets for connected cars, commercial fleet, rail and construction equipment. With a rich heritage of security innovation and rapid adaptation to the changing demands of the cyber security space, Irdeto is the preferred partner to empower a secure world where people can connect with confidence.