THREAT DETECTION SOLUTION

WHITEPAPER

SELECTRON

Cyber-risk-ready: Securing rail vehicles against cyber attacks and complying with the European NIS Directive

Acting is better than reacting: With its new Threat Detection Solution (TDS) Selectron offers a scalable cybersecurity solution for the individual needs of rail operators to master the increasing risk of cyber threats.

Introduction

Cyber risks become more and more eminent also in the railway industry. Regulations, such as the European NIS Directive, demand the railway infrastructure to be protected. This may also apply to train vehicles. Based on performed risk assessments, Selectron understands the attack vectors to the various electronic systems very well.

The new TDS acts as a passive element of the overarching cybersecurity architecture. Especially for legacy vehicle an in-deep active protection of already existing electronic devices can not be demanded from an economic point of view, as this would lead basically to a replacement of the electronic solution.

As from a risk-related point of view, the silent acceptance of the cyber risk must also not be accepted; Selectron offers the TDS as the most economical solution to protect legacy fleets.

Non-intrusiveness certified by a competent body, the TDS recognizes non-authorized functions and devices on Consist Bus (CAN / MVB) and puts out an alert, either on the driver's desk or on an existing communication channel. This signal enables operators to initiate respective countermeasures on time and thus protect the vehicle and its passengers from failing electronic devices due to cyber attacks. The most eminent risk is that an unauthorized device "spams" the network, leading to a shutdown of the main controller and thus blocking the entire electronic network.

How it works

For both, CAN and MVB, the TDS is based on an existing communication network. The CAN or MVB master files are converted into the TDS configuration file, leading to the typical whitelist listing all devices that are allowed to operate in the network. The TDS then is constantly reading the traffic on the bus and analyzes whether the respective devices are authorized. Once an unauthorized device is identified, the alarm LED is turned on and the digital output is activated. Additionally, it logs a configurable number of messages before and after the attack. This is achieved by analyzing the frame ID of each device.

"Selectron's Threat Detection Solution empowers operators to prevent attacks in new and legacy fleets before any damage is done."

Dr. Thomas Fischer, CEO Selectron Systems AG

The roadmap

The TDS is capable of analyzing the Consist Bus (CAN or MVB) with a multidimensional approach: technically, it can detect not only the devices active on the bus, but also the way they act i.e.

- the functions that the devices perform (authorized or not),
- the timeline in which they are performed,
- the modality (cyclic or non-cyclic),
- the expected bandwidth occupation (payload dimension).

Once a threat is identified, TDS is locally logging all events related to the threat and can also send all the logs acquired to a remote server using the standard Syslog Protocol.

Furthermore, using the Train Real-time Data Protocol (TRDP) customers can extract an arbitrary set of parameters collected by the TDS from the CAN or MVB buses, build a customized TRDP packet and send them to their own application using the ethernet network.

In addition, behavior-related rules will further enhance the level of protection. For example, the TDS will produce an alert if the signal to open the door is activated without prior checking of the vehicle-speed and/or beyond a critical speed limit.

All evolutionary updates apply only to the software; therefore, no new hardware device must be purchased. The fixed hardware price entitles the owner to unlimited updates during the entire life cycle of the product.

As of April 2022, Selectron released the SCCT (Selectron Communication Configuration Tool) that is a web application dedicated to customers aiming for an online, authenticated and secured configuration generator of Selectron devices, including the TDS.

The TDS was developed in accordance with IEC 62443 Security Level 2 (SL2). In addition, thanks to the Selectron Chain of Trust (Secure Boot and Secure Initialization), all data on the device is encrypted and signed by Selectron. This means that no one can maliciously change the configuration of the TDS (proprietary software and parameterization).

CAN and MVB versions are available since June 2022. The new Ethernet version (TDE) of this solution will soon be available for purchase.
For customers who do not use the Selectron TCMS product line, the three versions are also available as standalone products.

The TDS in its environment

Although many rail vehicles are connected to the ground infrastructure, Selectron aims to enable most functionality on the vehicle. If the user wishes to monitor its fleet remotely, the TDS can be connected to any already existing customer-specific infrastructure or Cloud device. To be fully transparent: Selectron will not store data on any own Cloud; data handling is fully at the customers' discretion.

TDS-WP002A_EN- Mai 2023

Selectron Systems AG

Bernstrasse 70
3250 Lyss
Switzerland
Tel: +41 32 387 61 61
Fax: +41 32 397 61 00
www.selectron.ch

KNORR-BREMSE

NEW YORK AIR BRAKE

IFE

MERAK

MICROELETTRICA

SELECTRON

EVAC

ZELISKO

RAILSERVICES