duagon

LEADING THE EMBEDDED FUTURE

SECURITY GATEWAY

duagon INTRUSION DETECTION SOLUTIONS

Intrusion detection & IT forensic analytics using duagon cyber security devices

D537 | D433

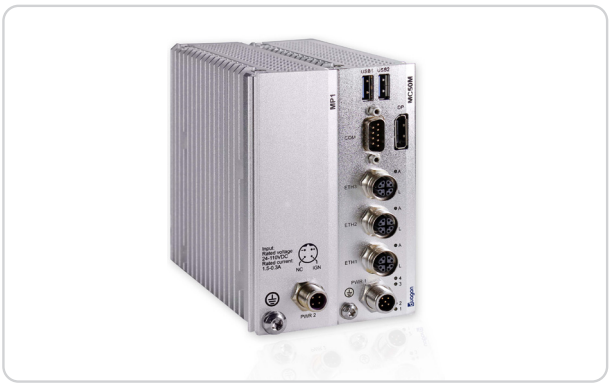
The train control network in modern trains is already targeted by cyber attacks. Hackers might try to take control of the train or to disrupt regular operation by ransomware or any other kind of typical cyber attack strategies.

duagon devices help to protect your rolling stock material against most of the common cyber security threats. We offer cyber security intrusion detection devices for Ethernet (D537 versions) and MVB (D433 versions), the most common train communication protocols. The D537 versions come with the additional support for typical ECN real-time Ethernet protocols like TRDP, PROFINET, CIP, IPTCom.

As the global expert for onboard communication systems, duagon intrusion detection devices are based on our long-standing experience in rail projects using all common train communication busses and protocols.

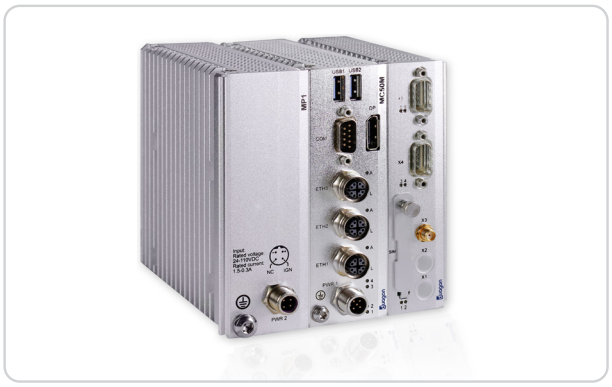
Our intrusion detection devices (IDD) are able to trace IT security violations in accordance with IEC 62443 (and its railway counterpart TS 50701) and assist you to achieve the required security levels. In addition, the devices can be used to achieve rolling stock compliance with national regulations (e.g., with the EU NIS directive).

ECN Intrusion Detection



duagon ECN intrusion detection devices are based on duagon's well known computing and control platforms. The devices are designed to provide intrusion detection capabilities together with a highly secure separation of different security zones present inside the rolling stock. Intrusion detection runs on the interface to the zone with higher security requirements and enables train operators to detect anomalies in the networks on their existing fleet. This is done, for example, by supervising the network traffic and ensuring only the desired devices communicate together. Then, in case of a security event or incident, an immediate response action can be put in place thanks to the alert provided by the intrusion detection device. The ECN intrusion detection devices can analyze real-time traffic as well as non-real-time traffic. All duagon ECN intrusion detection devices offer a secure web interface for the device configuration and remote deployment of firmware upgrades.

MVB Diagnostics & Intrusion Detection



duagon MVB diagnostics and intrusion detection devices are designed to detect anomalies in MVB networks. The devices can easily be integrated into existing networks without altering the existing MVB traffic or changing the existing MVB configuration. This is possible thanks to the device's MVB read-only interface. Intrusion detection targets the discovery of unusual or abnormal MVB traffic. For example, it is possible to detect unknown devices or unforeseen process data telegrams. In addition, a device fingerprinting allows to detect malevolent device exchange. The advanced diagnostics functionality also monitors the signal quality of a specific MVB network. This renders condition-based maintenance on the MVB network. The devices can log and send alerts over their Ethernet interface so that appropriate mitigation actions can be initiated. All duagon MVB diagnostics and intrusion detection devices offer a secure web interface for the configuration and to deploy firmware upgrades remotely.

Configuration

The functionality of duagon intrusion detection devices can be jointly analyzed and continuously improved to detect emerging cyber security threats.
The devices can be configured via secure web interface or using an encrypted USB dongle.

Intrusion Detection Device Family

D537
Security Gateway with Intrusion Detection

D433
MVB Diagnostics with Intrusion Detection