VIAVI Solutions

Cybersecurity for Railway is a Minimum, Not a Plus

Detect and discover cybersecurity issues on GSM-R railway telecoms and ETCS signalling systems

Today’s railways face several challenges detecting and managing OT cybersecurity.

The railway sector is increasingly vulnerable to cyber-attacks from malware, ransomware, and even data breaches, and the consequences could be disastrous.

Compliance with industry standards strengthens your systems’ protection. For railway, the most relevant are IEC 62443 (an international series of standards that address cybersecurity for operational technology in automation and control systems) and the new TS-50701 railway cybersecurity standard.

Our cybersecurity solutions can meet the certifications and are designed to provide engineers and management with the tools to detect and discover cyber-related issues on railway telecoms and signaling systems.

These include detecting for example: denial of service attack on RBCs, unusual mobile station usage (in order to help perform early detection of SIM card robbery), flooding (to perform DoS attack) and radio jamming.

Benefits of Meeting Cybersecurity Standards:

- Monitor access from untrusted networks
- Audit records generated by equipment
- Protect the integrity of transmitted information
- Prohibit unnecessary ports, protocols and services
- Track unsuccessful login attempts
- Produce a report list of components
- Produce reports on unauthorized wireless devices
- Recognize changes to information during communication

DISCOVER
Assets, activities and communications dashboards

DETECT
Messages and activities on ERTMS systems

ALERT & INVESTIGATE
Vulnerabilities or abnormal behavior

RESPOND
Automated reports and forensic analysis

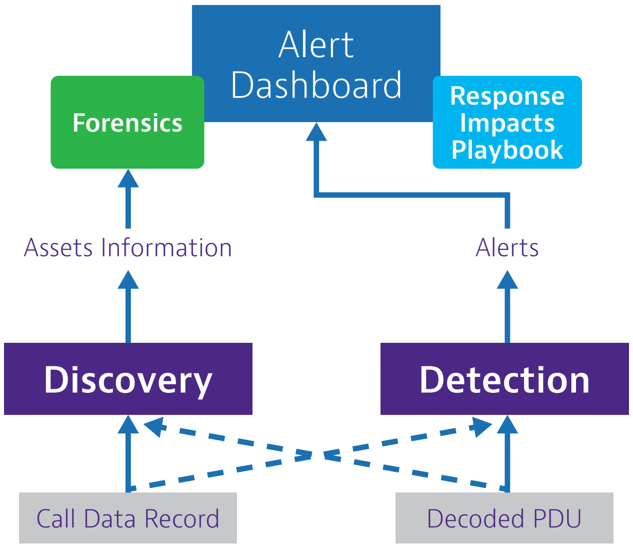
Cyber Systems Security

First introduced in 2000 GSM-R, the telecoms component and ETCS, the signaling component, make up ERTMS (European Rail Traffic Management System), the single European signaling and speed control system.

Without GSM-R communications or operational ETCS signaling, the trains cannot run. However as with any industrial technology that’s over 20 years’ old the equipment and infrastructure can be more vulnerable to modern cyber-attacks as a result.

QATS Cybersecurity can be integrated with a customer’s SIEM solution if required. They are available as a standalone system or can be integrated into an existing QATS Railway solution.

Using the same data lake and QATS probe infrastructure, means you can integrate new cyber functionalities to discover system vulnerabilities, detect attacks, monitor current statuses, and manage issues more quickly and effectively.



Vulnerabilities in ETCS signaling systems	**Possible impact or risk**
Stolen SIM card	Traffic disturbance
ETCS L2 service degradation attempt on RBC	Train speed reduction Inter-train distance increased
ETCS L2 service degradation attempt on train	Safety (train accident)
Intrusion attempt on ETCS Network	Information leaks
Global GSM-R disturbance attempt	Train stop
Local GSM-R disturbance attempt	Train stop, REC Alert inhibition
Alteration of train presence on a track section	Safety (train accident)

Summary of VIAVI Railway OT Cybersecurity Functionalities:

Forensics from alert dashboard

- Attack vector identification: source and target of the attack
- Scenario identification
- Raw data of event(s) triggering alerts
- Historical information

Response in alert dashboard

- Potential impacts available to SOC
- Remediation guidance with ERTMS expertise

VIAVI Solutions

Contact Us **+1 844 GO VIAVI**
(+1 844 468 4284)

To reach the VIAVI office nearest you,
visit viavisolutions.com/contact

expandium.sales@viavisolutions.com

© 2022 VIAVI Solutions Inc.
Product specifications and descriptions in this document are subject to change without notice.
Patented as described at
viavisolutions.com/patents