VIAVI Solutions

Cyber Security Is a Minimum, Not a Plus

In this article, Eric-Vittorio Li Destri, the Railway & MCx Cyber Security Product Line Manager at VIAVI Solutions, explains the new EU NIS2 and Cyber Resilience Act regulations and why railway operational technology is so vulnerable to attack.

Eric-Vittorio Li Destri,
Railway & MCx Cyber Security Product Line Manager at VIAVI Solutions

EU cyber security regulation, as everywhere in the world, is currently evolving.

A big bang event, larger than GDPR, will take place in the next 18 months across Europe. Member States will need to integrate the EU (Network and Information Systems) NIS2 Directive and also comply with the new Cyber Resilience Act (CRA).

These new cyber security regulations cover a wide range of industries and sectors, including railway, both from an IT and an OT (operational technology) perspective.

EU NIS2 Regulation

Before we examine railway OT and its potential cyber-vulnerabilities, let's first clarify the new regulations and what they mean for the railway industry, especially regarding telecoms and signalling systems.

NIS2 was published on 28 November 2022, giving EU Member States 21 months to incorporate it into their respective national cyber security laws (i.e. by August 2024). Outside the EU, other countries such as the UK and USA are generally expected to follow this approach.

Centred on three pillars – capabilities, risk management and reporting, and co-operation and information exchange – the NIS2 Directive seeks to enhance cyber security by:

- Defining a minimum set of measures
- Ensuring there is a risk-based approach to managing cyber security
- Enforcing management accountability
- Reporting and sharing information on significant incidents

The penalty for failure to comply is significant – from EUR 10m for small companies, to up to 1.4% (and even 2%) of annual group turnover worldwide, if the requirements are not fulfilled. And it's not just the company which can be fined, so can its board!

Cyber Resilience Act

Publication of the CRA is planned for this year but no date has yet been set.

Using a new legislative framework, manufacturers, distributors and importers will need to meet new

cyber security rules for applying to both hardware and software related products. This goes beyond basic laptops, computers and gaming devices, as the definition of 'digital elements' also includes remote data processing solutions. Certain sectors/products such as cars and medical devices will be excluded from the new legislation (as they are already sufficiently well-regulated for cyber security), everything else will be covered, including SaaS products.

All products will be expected to carry a new CE mark and to meet the stated cyber essentials requirements for 5 years (or for the product lifecycle, if less). The requirements include ensuring that the products are delivered free from vulnerabilities, and that a process is in place to log and manage vulnerabilities discovered subsequently.

Whilst around 90% of products are expected to fall into the default, 'self-assessment' category, we anticipate that due their mission-critical nature, railway telecoms and signalling systems will fall into the 'highly critical', mandatory EU certification category.

Further details will become available once the Act is published and the penalties will also be punitive for non-compliance – for example, from EUR 15m to 2.5% of annual turnover.

Railway Vulnerabilities

The ERTMS perimeter (pictured below) is a complex structure using a mix of new and antiquated technology and it is common knowledge that known (and unknown) vulnerabilities need to be identified and managed as part of the new regulations.

With cyber-attacks are becoming more and more frequent, in general, OT is a strong potential next target for any industry, including railways – which is why OT cyber security has been described for rail (in CENELEC / TS 50701, for example).

The regulations require alerts to be provided to a SOC, which means that the SOC needs remediation guidance (playbooks) and analysts need powerful investigation tools.

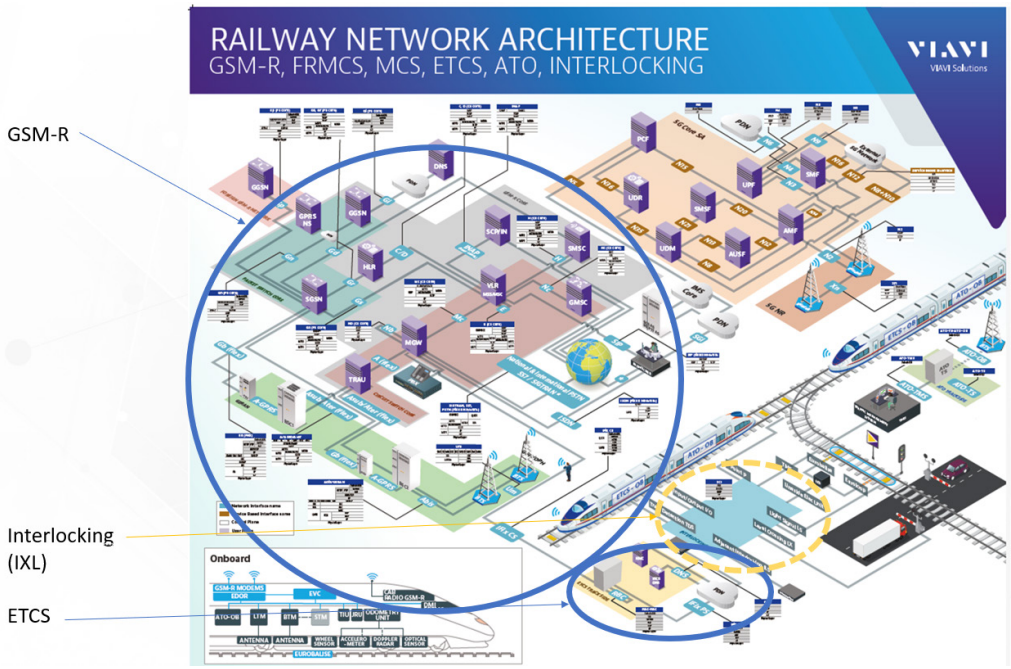
Practical Cyber Security Solutions

Continuous monitoring of critical services/ infrastructures should be part of the cyber defence of the SOC, ensuring that abnormal and transactional behaviour is identified through a continuous monitoring solution.

Therefore, anyone managing railway OT cyber security needs a comprehensive solution for cyber security detection and remediation.

This should encompass the following areas:

- Visualisation: gets an exact status of its pools of mobile stations and network elements
- Detection: identifies and reports incidents, suggests configuration changes



- Alerting and investigation: alerts on potential vulnerabilities
- Response: procedures to limit the incident's impacts

To better understand this in detail, the cyber security solution should typically include a set of detection engines using:

- **Learning and machine learning**
  - Asset detection
  - Behaviour analysis
  - Network topology analysis
  - Advanced statistics using historical information
  - Advanced traffic analysis
- **Dictionary of signatures**
  - Known GSM-R attacks
  - Known ETCS attacks
  - Common attacks such as flooding, spoofing
- **Analysis and forensics**
  - Sigma-compliant alerts in order to integrate with the most common SIEM and SOAR platforms and be able to share playbooks and give direct access to relevant dashboards
  - Forensics tools uses Elastic stack and especially Kibana with data rendered after asset and topology detection in order to speed up forensic operations
  - Realtime dashboards

"For those organisations who already have solutions to test, measure and monitor ETRMS networks, including GSM-R and associated interlocking (IXL), it can be possible to add cyber security solutions in a very cost-effective way by using existing equipment. And for others, a standalone solution can be arranged."

Because cyber security should be a minimum, not a plus, solutions need to be practical and cost-effective. That's why we have developed solutions that can either be integrated into a customer or provider's SIEM, or are available as a standalone system.

If you'd like to know more, please visit **www.viavisolutions.com/railway** or contact us at **sales.railway@viavisolutions.com**