Directory

Data & Monitoring

Nomad Digital
connected transport, intelligent solutions

The Cybersecurity Landscape for Rail

© Canva

The rail industry is a critical component of the global transportation network and is a significant part of most countries' critical national infrastructure.

As the industry undergoes rapid digital transformation, advances in technologies such as automated signalling systems, Internet of Things (IoT) devices and cloud-based operational platforms, are reshaping and revolutionising rail network operations. Across the business world – and particularly in rail, technology is becoming increasingly complex and interconnected.

Network-based services that help operators to improve their passengers' experience whilst also adding value to their fleet operations are an increasing part of the landscape, but as we expose more services to the public, there must be an increased focus on cybersecurity and protection to ensure that services do not present opportunities for vulnerabilities to be exploited.

The number of complexities and severities of cyber attacks on all industries, including rail is increasing rapidly. Sophisticated toolkits can be easily obtained which could potentially allow relatively inexperienced people to conduct complex cyber attacks which can lead to loss of service, data and revenue and to reputational damages.

Having said that, not all attacks on IT infrastructure rely on sophisticated tools or advanced technical skills – during the 2024 Paris Olympics, the rail network experienced a significant attack designed to disrupt the games and deliver press coverage worldwide. In that case, the attack was on physical network infrastructure which halted major parts of the rail network.

Navigating Cybersecurity Standards in the Rail Industry

As cybersecurity threats have evolved, various standards and guidelines continue to emerge to help safeguard critical infrastructure. However, solution providers often face challenges in determining which standards to follow. Some of the most significant include:

- The NIS2 Directive (Network and Information Systems Directive 2) aims to enhance the cybersecurity and resilience of critical infrastructure and essential services across the European Union. Building upon the original NIS Directive (2016), NIS2 addresses the ever-evolving cyber threat landscape by expanding the regulation scope, introducing tighter security requirements, and supporting cooperation among EU member states.

- The EN62443 series of standards for industrial control systems has been widely recognised as useful within the rail industry, even though it is not specifically focused on rail transport. It provides a very comprehensive framework for all elements of system design, development, component supply chain, manufacturing, testing, deployment and maintenance.

- The EN50701 standard has been proposed by a broad group of rail industry suppliers and operators (also referred to as TS 50701) which acts as a rail specific variation of the EN 62443.

Governments are also taking proactive steps to combat cyber threats. Governmental and national bodies have long been considering laws to improve the cybersecurity of organisations and protect the rights of individuals. The European Union has recently released the Cyber Resilience Act (CRA) with its goal being to enhance the cybersecurity of digital products. The CRA requires manufacturers selling products to EU member countries to embed security features into products from the design and development phase, commonly known as 'security by design'. Included in the act is the requirement to provide, free of charge, regular updates and patches to fix potential vulnerabilities.

For train operators, this means increased visibility into the security of their digital infrastructure. Leading operators will likely establish – or already have processes to review security updates and assess their impact on fleet safety. Those without streamlined software upgrade procedures may need to refine their change management processes to maximise the benefits of CRA.

Supporting the Future of Rail Cybersecurity

At Nomad Digital, we are committed to helping train operators strengthen their cybersecurity posture and protection. By working proactively with industry stakeholders, we aim to ensure that rail networks remain secure, resilient and prepared for the challenges of an increasingly connected world.

Nomad Digital's Security-as-a-Service offers a comprehensive approach to cybersecurity that goes beyond a 'software-only' solution to aid the detection and response to an actual or suspected cyber-attack as well as enhancing important security processes such as risk & vulnerability management.

Speak to Nomad Digital's experts today to find out more. You can also find Nomad Digital and Alstom at **The Rise of IoT & Big Data in Rail Event 14–15 May 2025, Cologne**.

THE RISE OF
IoT & BIG DATA
BY ROTAIA MEDIA IN RAIL

For more information visit our **website** or **contact** our team.

© Canva

www.nomad-digital.com

www.alstom.com

State-of-the-art cybersecurity protection for rail

24/7 monitoring to enhance threat detection and response to cyber-attacks

Visit Nomad Digital & Alstom at 'The Rise of IoT & Big Data in Rail' event 14-15 May 2025, Cologne

© Alstom SA 2025, Shutterstock

Alstom, a world leader in mobility solutions, actively shapes and implements rail cybersecurity standards. With over 20 years of experience, Nomad Digital offers secure connectivity solutions for rail. Together, Alstom and Nomad Digital deliver state-of-the-art cybersecurity solutions tailored to the rail industry.