# The Future Of Rail

## Innovations Shaping the Safety, Efficiency and Compliance of Travel

Petards Rail
intelligent train technology

# The Future of Rail: Innovations Shaping the Safety, Efficiency and Compliance of Travel

**The rail network is set to experience a huge expansion in the years and decades to come.**

Network Rail has predicted that there will be an additional one billion journeys made on Britain's railway alone by the mid-2030s. With the Department for Transport 2024 Rail Factsheet revealing that there were 1,612 million passenger rail journeys made across the country in the financial year ending March 2024, it quickly becomes clear how much this network is expected to grow.

Those in the rail industry are also facing challenges because of the following market pressures: cybersecurity, sustainability mandates, driving economic growth.

## Contents



## Cybersecurity

There are several reasons why cyber criminals continue to target businesses in the rail sector. For example:

- A cyber attack on rail has the potential to cause a lot of disruption, due to it being part of a country's critical infrastructure.
- Rail businesses hold a lot of sensitive and valuable data.
- The movements and conditions of trains in operation are being more regularly monitored by systems which could be exploited if vulnerabilities are found.

There is still fragmented communication between various operational teams within the rail industry, with this disjointed approach at risk of being exploited by cyber criminals. It also must be acknowledged that operational technology systems in rail often have long replacement lifecycles, with some in use for 15 to 20 years at a time. This means that advanced technology being introduced to the sector is having to work with unsupported legacy infrastructure which have become outdated. The entire setup is then vulnerable to a cyber attack. Cybersecurity therefore needs to be carefully considered by rail businesses, otherwise an attack or successful breach of a system has the potential to cause:

- Business interruption
- Data loss
- Extortion
- Reputational damage
- Costly fees to pay for breach remediation measures
- Legal claims
- Regulatory fines

## Sustainability mandates

Countries across the world understand that the concept of sustainability must be treated very seriously today, so that climate change can be fought and the environment better protected.

In the UK, for instance, everyone needs to be doing their bit to help achieve the following:

- Meet the government's aim for greenhouse gas emissions to be reduced by at least 68 per cent by the end of this decade, when compared to the levels recorded in 1990.
- Meet the government's legal commitment for net zero carbon emissions to be reached by 2050.

When it comes to the nation's rail industry here, the Office of Rail and Road has adopted an approach to environment and sustainable development with the use of regulatory activities of the national rail network.

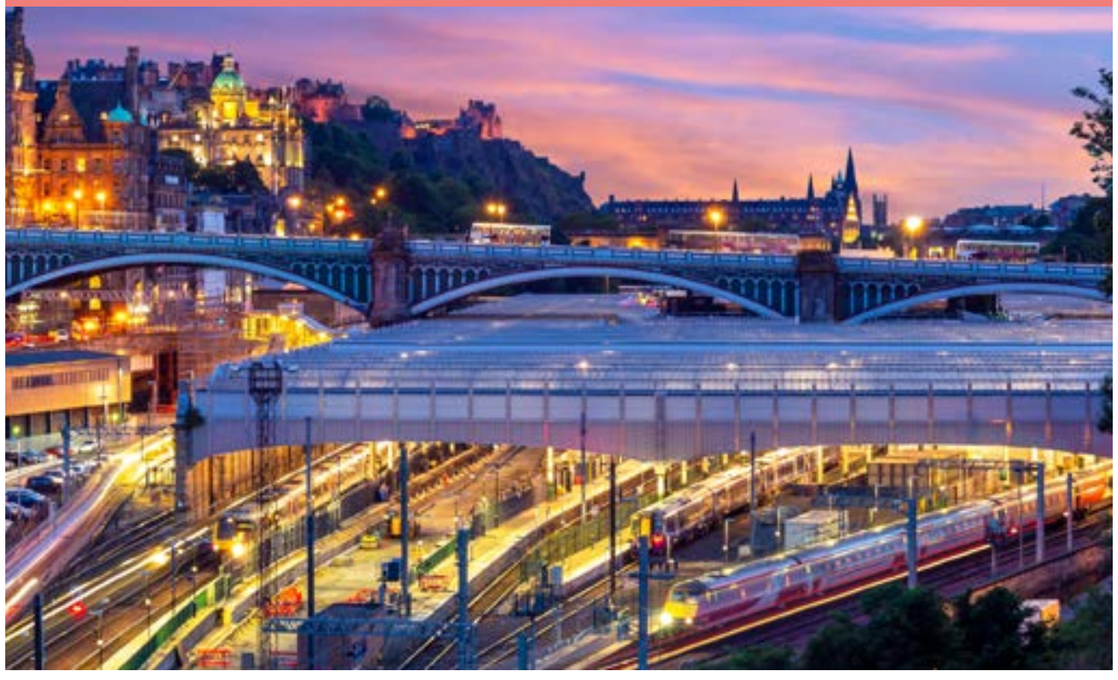
Specifically, they have these two statutory duties under the Railways Act 1993:

1. To contribute to the achievement of sustainable development.
2. To have regard to the effect on the environment of activities connected with the provision of railway services.

As a business, PJL are leading the sustainability journey within the rail industry. The firm received the Platinum Award from globally recognised sustainability rating platform EcoVadis in recognition of their 2023 Corporate Social Responsibility (CSR) initiatives and commitment.

This Platinum rating puts PJL in the top one per cent of all organisations evaluated and means they have demonstrated exceptional performance in the areas of environmental awareness, labour and human rights, ethics and sustainable procurement. It also showcases their industry-leading sustainability efforts, robust governance, and a strong commitment to Environmental, Social, and Governance (ESG) principles.

There is still plenty of work to be done in the rail sector around this topic though, especially if the Department for Transport 2024 Rail Factsheet is anything to go on.





## Driving economic growth

The UK's rail sector serves as critical transportation infrastructure, allowing people, goods and services to move across the nation with ease.

A study undertaken by independent researchers at Oxford Economics and commissioned by the Railway Industry Association in 2022 highlights just how important the industry is to the UK. The report found that:

**£43 Billion**
GVA in economic growth

**The rail network generates £2.50**
of income in the wider economy for every £1 spent.

**710,000 jobs**
Supported by the Rail Network

**£14 Billion**
Provided in Tax Revenue.

Businesses within the rail industry must keep doing their bit to make sure the sector continues to play such an important role in the UK's economic growth.

To address the various challenges being faced in the industry and to prepare for the future, the rail sector is currently witnessing significant steps being taken around digital transformation.

Everything from scheduled maintenance procedures and traffic management systems to improved real-time passenger information tools and the adoption of artificial intelligence (AI) are being looked at during this push to revolutionise the rail network.

There are three key benefits of getting a digitalised railway system in place:

1. Digital transformation will improve the passenger experience across the network.
2. Digital transformation will increase how efficient the sector is.
3. Digital transformation will modernise and optimise rail operations.

Petards Rail is a consultative, innovative partner looking to help businesses achieve digital transformation in rail by providing world-leading, high-quality data and video technology and services to the industry, both on a UK scale and internationally.

Experts in intelligent rail technology with over 35 years of experience in business, they have:

**Over 30,000**
Cameras in action

**Over 60,000**
Line Replaceable Units (LRUs) in service

**Six Generations of Equipment**
provided to major train builders, operators, rolling stock companies (ROSCOs) and other organisations tied to the rail industry.

Always looking ahead, Petards Rail has a vision to be the leading company in intelligent train technology across the globe. Aiming to help the industry navigate change, they will be providing their customers with advanced solutions and dynamic services which help them to improve rail safety, enhance passenger satisfaction, and save time and money.

# Cybersecurity – Building Cyber Resilience Across the Rail Ecosystem

**The UK rail industry has long recognised the potential consequences of cyber threats and has taken proactive steps to strengthen its digital defences.**

With the convergence of legacy OT and modern IT-based systems, ensuring the resilience of rolling stock and infrastructure has become not only a technical necessity but also a regulatory obligation.

Today, rail operators, suppliers, and infrastructure managers must align with a growing body of standards and legal frameworks designed to safeguard the sector from cyber disruption.


## Strengthened by Legislation: The Cyber & Resilience Bill

At the forefront of this evolving regulatory landscape is the **UK Cyber and Resilience Bill**, a landmark piece of legislation introduced to bolster national resilience against cyber threats across critical sectors, including rail.

Building upon the foundation laid by the NIS Regulations 2018 and considering the more recent NIS2 directive, this new Bill is expected to **tighten oversight, increase reporting obligations, and raise the bar for security preparedness among Operators of Essential** Services. It introduces ongoing security patching and maintenance, which includes:

- More rigorous enforcement mechanisms
- Enhanced coordination with the National Cyber Security Centre (NCSC)
- Broader expectations around supply chain assurance, incident response, and business continuity planning

For rail operators and system suppliers, the Cyber and Resilience Bill reinforces the urgency of building cyber resilience into every stage of system lifecycle management—not just meeting compliance requirements. It's not just a one-off compliance exercise either, but a continuous security strategy that safeguards service and passenger safety amid evolving threats.



## NIS Regulations and the Role of the Department for Transport

The **NIS Regulations**, established under the EU's Network and Information Systems Directive and retained in UK law, classify rail transport as a **critical national service.** This legal framework mandates that train operators, infrastructure managers, and service providers implement proportionate technical and organisational measures to mitigate cyber risks.

The **Department for Transport (DfT)** serves as the competent authority for enforcement in the rail sector, supported by the NCSC's guidance and the Cyber Assessment Framework.

Compliance with NIS involves:

**Conducting regular cyber risk assessments**

**Implementing layered security controls**

**Maintaining up-to-date incident response and recovery plans**

**Ensuring continuous monitoring and assurance across all connected systems.**

With the convergence of legacy OT and modern IT-based systems, ensuring the resilience of rolling stock and infrastructure has become not only a technical necessity but also a regulatory obligation.

Today, rail operators, suppliers, and infrastructure managers must align with a growing body of standards and legal frameworks designed to safeguard the sector from cyber disruption.

## Industry Standards & Technical Guidance

Alongside statutory frameworks, the UK rail industry draws on a range of **sector-specific standards** to define secure development and deployment practices:

**RSSB RIS-0745-CCS:**
Offers guidance on cyber assurance for software-based railway control and safety systems, aligned with standards such as **EN 50128** and **EN 50657** for legacy systems and **EN 50716** for new systems. It supports rail organisations in setting technical requirements for suppliers and validating security during procurement and commissioning.

**RSSB TN2312:**
A technical note aimed at the rolling stock industry, highlighting the importance of cybersecurity awareness. It also provides guidance on complying with international standards, physical securing of assets, how to manage engineering change, and evaluating system interfaces. It offers a comprehensive summary for significant businesses within the rail industry.

**IEC 63542:**
This emerging international standard supersedes **CENELEC TS 50701** as the primary reference for applying cybersecurity in railway systems. Aligned with **IEC 62443,** IEC 63542 provides a **comprehensive framework for integrating cybersecurity and functional safety** across rolling stock, signalling, and infrastructure. It promotes a defence-in-depth approach that includes strong authentication, software whitelisting, encrypted communications, system zoning, secure patching, and lifecycle risk management. Crucially, it formalises the **co-engineering of safety and security,** ensuring that

cybersecurity risks are addressed in harmony with safety requirements—an essential step for safety-critical systems in both new and legacy rail applications. By bridging assurance processes, IEC 63542 supports more effective, standards-aligned system development and long-term resilience.

**IEC 62443 family:**
Critical family of standards that define requirements for systems **(IEC 62443-3-3)** and products **(IEC 62443-4-2).** They create a baseline for cybersecurity and integrating these principles into business development processes. It also encourages standardisation and provides strategies to manage legacy integrations to modern systems.

These standards work together to promote a **secure-by-design approach,** encouraging suppliers and operators to integrate cybersecurity alongside safety and performance criteria from the earliest stages of system development.

## Ongoing Risk Assessment & Sector-Wide Collaboration

**The Office of Rail and Road (ORR)** has also taken an active role, conducting **risk-ranking assessments** to identify the most cyber-critical systems in UK rail operations.

This helps inform inspection priorities and focuses attention on those systems—such as digital interlockings, train control, and remote diagnostics—that would pose the highest safety risk if compromised.

Collaboration across the industry has also deepened. Initiatives like the **Rail Cyber Security Working Group** and use of the **CiSP (Cyber Security Information Sharing Partnership)** platform allow government and operators to exchange threat intelligence and best practices.

Regular **tabletop exercises, supplier audits, and cyber drills** are helping to prepare organisations for both targeted attacks and broader digital disruption too.

## Adapting to the Future: Innovation & Resilience

As digital innovation in rail accelerates—**driven by technologies like driverless trains, condition-based maintenance, remote diagnostics, and real-time passenger services**—the threat landscape is becoming more complex.

Securing these systems requires not only technical controls, but also **organisational resilience:** the ability to recover from incidents quickly, limit the spread of damage, and maintain safe service delivery under stress. To support this, rail companies are investing in:

- **Real-time intrusion detection & logging**
- **Network segmentation & system zoning**
- **Secure remote access protocols, redundant backups and manual fallbacks for critical functions.**

The Cyber and Resilience Bill, together with NIS2, RSSB standards, and international best practices, provides the policy and technical scaffolding for a **rail sector that is not only digitally capable, but also cyber-resilient.**



## Key Differences Between IT & OT Cybersecurity

**While both IT and OT systems are vulnerable to cyber threats, their security priorities, environments, and response strategies differ significantly:**

| Aspect | IT Cybersecurity | OT Cybersecurity |
|---|---|---|
| **Primary Objective** | Protect data confidentiality and availability | Protect safety, reliability, and operational continuity |
| **Key Assets** | Emails, documents, databases, usercredentials | Industrial control systems (PLCs,SCADA, signalling, braking, etc.) |
| **Main Threats** | Data breaches, ransomware,phishing | System downtime, equipment damage, safety incidents |
| **Typical Environment** | Office-based networks, cloud infrastructure | Field-based systems, often airgapped or legacy-connected |
| **Update Frequency** | Regular patching and updates (monthly/weekly) | Infrequent updates (months/years) due to system certification needs |
| **Downtime Tolerance** | Some tolerance – backups and redundancy in place | Minimal or none – downtime can halt operations or cause accidents |
| **Security Focus** | CIA: Confidentiality, Integrity, Availability | AIC: Availability, Integrity, Confidentiality (safety > privacy) |
| **Response Strategy** | Detect, contain, recover quickly | Prevent, isolate, preserve safe states first |
| **Regulatory Drivers** | GDPR, NIS, ISO 27001 | IEC 62443, ISO 27001, RIS-0745-CCS, and industry-specific standards |

### IT cybersecurity

Focuses on protecting data and business operations from theft or disruption, typically emphasising *confidentiality first.*

### OT cybersecurity

Prioritises *availability and integrity* to ensure physical systems like trains, signals, and interlockings continue to operate safely and without interruption.

OT systems often involve legacy hardware, strict safety regulations, and long certification cycles, making them harder to patch and more sensitive to downtime. A cyber-attack on IT may result in lost data; on OT, it could threaten **human safety and critical infrastructure.**

Therefore, OT cybersecurity requires a different mindset—balancing cyber resilience with **fail-safe operations** and physical risk management.

## Aligning our Development & New Product Introduction with IEC 62443 for Resilient Rolling Stock at Petards Rail

As digital systems become increasingly integral to modern rolling stock—powering everything from onboard diagnostics and remote monitoring to train control and passenger systems—**cybersecurity must be embedded into the product lifecycle** from the outset.

Aligning our **development and New Product Introduction (NPI) processes** with the internationally recognised **IEC 62443** standard enables a structured, risk-based approach to security that reflects the unique requirements of rail's OT environment. IEC 62443 provides a comprehensive framework for securing industrial automation and control systems.

It guides manufacturers and integrators through asset risk assessments, system architecture design, secure software development, and product assurance.

Integrating these practices during NPI ensures that our products meet not only cybersecurity best practices, but also the safety and availability expectations of the rail sector.

This alignment supports compliance with emerging regulation, such as the UK's implementation of the NIS2 Regulations, and rail-specific standards like RIS-0745-CCS, RSSB TN2312 and IEC 63452. of the NIS2 Regulations, and rail-specific standards like RIS-0745-CCS, RSSB TN2312 and IEC 63452.

## Enhancing Cyber Resilience Through Cross-Stakeholder Collaboration

Achieving robust cybersecurity for rolling stock requires more than compliant products—it demands **collaboration across the full lifecycle of the fleet,** from concept to end-of-life. Closer, earlier, and more transparent engagement between **Tier 1 suppliers, OEMs, Train Operating Companies (TOCs),** and **ROSCOs (Rolling Stock Companies)** is essential to building resilient, interoperable, and supportable systems.

Each stakeholder holds a unique piece of the puzzle:

**OEMs - define platform-level architecture and integration points**

**Tier 1s - develop and supply critical subsystems**

**ROSCOs - manage long-term asset value and upgrades**

By working together—sharing threat models, defining joint security requirements, and conducting integrated security testing—we can reduce duplication, uncover system-level vulnerabilities earlier, and ensure that ownership of cyber risk is clearly defined and maintained throughout the asset lifecycle.

This collaborative approach also enables more effective response to incidents and vulnerabilities when they arise. With coordinated processes for vulnerability disclosure, patch distribution, and system revalidation, the industry can respond faster and more safely to emerging threats.

Over time, this reduces operational risk, improves regulatory confidence, and ensures that fleets—both new and legacy—remain safe, secure, and aligned to future digital transformation goals.



## Securing Our IT Infrastructure Alongside OT Systems

Alongside securing our OT systems in line with IEC 62443 and safety-critical practices, we've strengthened our corporate IT infrastructure through Cyber Essentials Plus and ISO/IEC 27001 certifications. These demonstrate robust protection against cyber threats and a comprehensive, standards-based approach to information security across risk, governance, data handling, and incident response.

Together, these measures show our commitment to end-to-end cybersecurity—from train systems to enterprise data—giving clients and regulators confidence that security is built into everything we do.

## Petards Rail: Delivering Trust and Resilience Through Secure Solutions

At Petards Rail, we embed cybersecurity into every layer of our operations—from safety-critical OT systems to enterprise IT infrastructure. Our alignment with IEC 62443 ensures that onboard technologies like CCTV, driver displays, and data platforms are designed to withstand evolving threats and support long-term resilience.

We back this up with Cyber Essentials Plus and ISO/ IEC 27001 certifications, demonstrating strong data protection and secure business operations.

Recognising the challenges of ageing fleets, we collaborate with OEMs, TOCs, and ROSCOs to secure both new and legacy systems. Our expertise in integration, assurance, and secure retrofitting helps identify vulnerabilities and extend asset life—without compromising performance.

By securing our products and our enterprise, and partnering across the rail ecosystem, we reduce cyber risk and support the safe, resilient operation of the UK's national rail infrastructure.

**By aligning our product development with the IEC 62443 standard, Petards Rail embeds cybersecurity into the foundation of safety-critical rail systems.**

This ensures long-term resilience against evolving threats.

# Cybersecurity – The Evolving Cyber Threat Landscape in Rail

**Cybersecurity is no longer a back-office concern—it is now a frontline issue for the entire rail sector.**

As rail systems become increasingly digitised, interconnected, and data-driven, the risks posed by cyber threats are escalating rapidly. From train control and signalling to real-time passenger information and remote maintenance systems, every digital touchpoint is a potential entry vector for attackers. The consequences of a cyber breach in the rail domain go far beyond data loss—they can disrupt services, impact safety, and undermine public trust in what is considered critical national infrastructure.

The scale and severity of the threat landscape are starkly illustrated in the Cyber Security Breaches Survey 2025, a government-backed study conducted by the Department for Science, Innovation & Technology and the Home Office. The report estimates that, in the 12 months to April 2025:

**8.58 million**
cybercrimes targeted UK businesses.

**30 cyber incidents**
were suffered on average by each business victim across all types

For the rail industry—where operational technology (OT) systems interface with IT networks, and digital systems control the movement of trains and people—these figures are a wake-up call.

The sector cannot rely solely on physical security or legacy safety protocols. Instead, it must embrace a cybersecurity mindset that spans every asset, from onboard systems and trackside equipment to enterprise IT and third-party integrations.

Join us as we explore how the rail industry can rise to the challenge—tackling emerging cyber threats, securing legacy infrastructure, and building digital resilience for the future of rail.



## Actual Cyber Incidents (UK Rolling Stock & Rail Infrastructure)

**2015–2016: Multiple Network Intrusions**
Cybersecurity firm Darktrace revealed that the UK rail network suffered at least four cyber intrusions within a 12-month period. These breaches appeared **exploratory** rather than disruptive – hackers infiltrated railway IT systems (including information displays and possibly control systems) but did not cause service outages. The incidents raised alarm because access to critical management systems (e.g. those controlling signals and trains) was demonstrated, highlighting the real possibility of hackers causing damage if they had malicious intent. UK officials stressed that rail operators were strengthening security as more rail technology goes digital.

**April 2021: Merseyrail Ransomware Attack**
Merseyrail, a regional UK train operator, was hit by a **LockBit ransomware attack** in early 2021. The attackers **compromised internal systems** and even **hijacked a director's corporate email account** to publicise the breach. In an email sent to staff and media, the hackers (posing as the Merseyrail Director) revealed a weekend IT outage was caused by ransomware and that **employee and customer data had been stolen.** Merseyrail confirmed the cyber-attack and notified authorities. While train operations continued (the outage was brief and mainly IT-focused), the incident underscored the risk of ransomware in rail and led to an investigation. (Financial costs were not disclosed, but the attack likely incurred recovery expenses and could attract regulatory scrutiny for the data breach.)

**July 2021: Northern Trains Ticketing System**
In mid-2021, a cyber-attack struck **Northern Trains' newly installed ticket vending machines** across its network. A ransomware infection took the machines **offline for about one week,** forcing passengers to use alternative payment methods. The ticket machines (which had cost ~£17 million to install) could not vend tickets during the outage. While this attack did **not affect train movement or safety,** it disrupted ticket sales and potentially led to revenue loss and customer inconvenience. Northern Trains and government agencies treated it as a serious incident, given that it directly targeted rail infrastructure hardware used by the public.

**September 2024: Station Wi-Fi "Cyber Vandalism"**
An investigation found that a bizarre attack occurred in 2024 when public Wi-Fi networks at 19 major UK railway stations were **compromised to display an extremist message.** Users who connected to free WiFi at stations (including London Bridge, Euston, Manchester Piccadilly, etc.) saw an Islamophobic terror-alert message. Investigation found that an **insider account** from a third-party Wi-Fi provider was used to deface the captive portal page (an "unauthorised change" via a legitimate admin login). In response, Network Rail **suspended the station Wi-Fi service** for several days as a precaution while the issue was fixed. No personal data was compromised, and train operations were unaffected, but the incident highlighted a security gap in passenger-facing systems and caused public alarm until resolved.

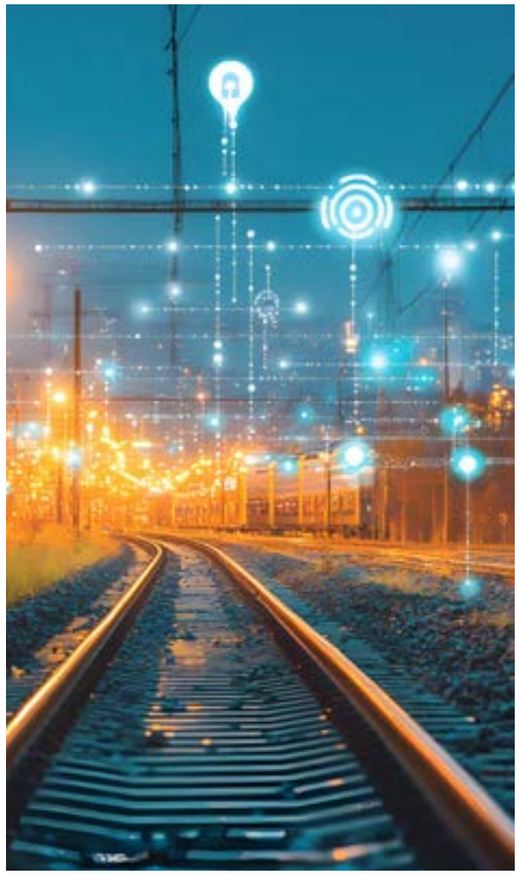
# Theoretical & Projected Threats to UK Rolling Stock

Industry experts and academics warn that cyber threats to UK rolling stock are growing as rail systems become more digitized and connected. **Risk assessments** by the Department for Transport (DfT), National Cyber Security Centre (NCSC), and rail regulators outline several potential vulnerabilities and attack scenarios that could impact trains and rail infrastructure:

## Key Vulnerabilities in Modern Rolling Stock Systems

**Onboard Control Systems & Signalling:** The shift to digital train control (e.g. the European Rail Traffic Management System, ERTMS) introduces new attack surfaces. Security researchers have cautioned that advanced malware could target signalling or onboard computers to manipulate train behaviour – for instance, sending false speed data or signal aspects. A successful compromise could theoretically cause collisions or derailments by overriding safety protocols. Professor David Stupples (UK government advisor) noted that clever malware in an ERTMS-based system might trick a train into misjudging its speed or braking, creating a risk of accident. While these safety-critical networks are isolated and "well protected from outside attacks," the greatest threat may come from **insiders** (disgruntled or bribed staff/contractors) introducing malware or malicious updates into train control systems.

**Remote Diagnostics and Maintenance Links:** Today's trains continuously send operational data to remote maintenance centres for diagnostics and performance monitoring. For example, newer rolling stock can **transmit huge datasets to the cloud** for analysis on IT systems. This IT/OT convergence means that a breach in the maintenance network or cloud platform could be a conduit to onboard systems. If hackers infiltrate remote diagnostics channels (or compromise the portable devices and software used by maintenance engineers), they might inject false data or malicious commands into trains. A worst-case scenario is an attacker issuing unauthorised control inputs or disabling critical subsystems (brakes, signals, etc.) via the maintenance interface. The rail industry recognises this overlap of enterprise IT and operational train systems as a security weak point, since traditional rail OT was not designed with internet connectivity in mind.





**Passenger-Facing Systems and Third Parties:** Systems like on-train Wi-Fi, entertainment, or station kiosks are less critical to safety, but can still be avenues for attack. As seen in the 2024 Wi-Fi incident, an insider or attacker who gains admin access to a third-party service can deface or disrupt operations without touching core signalling. However, there's concern that passenger-facing networks (e.g. onboard Wi-Fi or power outlets) might be used to jump into train control networks if not properly segregated. Researchers have demonstrated theoretical exploits where a virus on a passenger device could spread to train subsystems if firewalls are misconfigured. Similarly, third-party suppliers (train manufacturers, software vendors) are part of the supply chain – a breach at a vendor could expose technical details or backdoors affecting UK rolling stock. The **insider threat** extends to contractors and suppliers, not just railway employees, underlining the need for strict access controls and vetting across the rail ecosystem.

**Legacy Systems and Upgrades:** Much of Britain's rail infrastructure is an integration of legacy equipment (decades-old signalling interlockings, SCADA systems, etc.) with newer digital overlays. Older systems often lack built-in cyber protections and can be vulnerable if networked. As upgrades occur, any gap in securing the interface between old and new systems can be exploited. For example, a legacy signalling system brought onto a network for remote monitoring could be attacked to cause a **denial-of-service on signals** (forcing them to fail-safe to red and stopping trains). Ensuring backward compatibility while plugging security holes is a constant challenge. The Office of Rail and Road (ORR) has warned that **"poorly designed or maintained software-based systems"** in railway operations pose safety risks – meaning cybersecurity must be engineered in from the design stage, especially when retrofitting digital control onto legacy rail lines.

## Projected Attack Scenarios & Impacts

While the UK has yet to experience a catastrophic rail cyber-attack, **simulations and expert models** paint a picture of what a large-scale incident could entail:

### Mass Service Disruption

A coordinated cyber-attack on critical rail control systems could **bring train operations to a halt** across one or multiple regions. For instance, if malware took down the signalling and train management system on a busy mainline, all trains on those routes would stop until systems are restored. A UK government **scenario analysis** (looking at cyber impacts on infrastructure) found that in a severe case, over 800,000 train journeys per day might be disrupted – effectively paralysing commuter and freight movement. This kind of disruption would have cascading effects on the economy, as workers can't reach workplaces and goods are delayed. The indirect impact goes beyond passenger delays: missed deliveries, knock-on congestion, and public safety concerns among stranded travellers.

### Safety-Critical Failures

Though purely theoretical and *extremely guarded against,* the nightmare scenario is a cyber-induced train collision or derailment. Experts warn that if sophisticated attackers (potentially state-sponsored) gained control of signalling logic or onboard braking systems, they could override fail-safes. For example, an attacker might disable a trackside sensor or tamper with an interlocking so that two trains are cleared onto the same track. Another vector is manipulating the train control software (as posited with ERTMS) to prevent a train from automatically stopping at a danger signal. A successful attack of this nature could lead to loss of life and **catastrophic damage,** on par with a major train crash.

### Ransomware on Rail Operations

Ransomware attacks on rail operators' IT systems (like scheduling, signalling control, or train control) could force operators to suspend services for days. A real-world example occurred in Denmark in 2022, when a rail operator's IT supplier was hit by ransomware, causing a nationwide train stoppage for several hours. In the UK context, an attack encrypting Network Rail's signalling control centre or a major train company's dispatch system could result in **widespread train cancellations and delays** until backups are restored. The **financial cost** of such an incident is difficult to overstate. Beyond ransom payments or IT restoration costs, operators must refund tickets, arrange alternative transport, and may face regulatory fines. Based on analogous infrastructure scenarios, a multi-day outage across UK rail could easily cause **direct economic losses in the £billions.**


**A major cyber crisis could lead to £7.2 billion in direct losses and £4.4 billion in indirect costs, with rail playing a significant role.**

Even brief disruptions can cost millions daily and damage public trust in rail safety.

## The Need to Adopt a Proactive, System-Wide Cybersecurity Mindset Today

The rail industry stands at a critical juncture where digital transformation has brought both significant innovation and unprecedented cyber risk. As real-world incidents demonstrate, attackers no longer need to compromise physical infrastructure to cause disruption—digital vulnerabilities now present clear and present dangers to safety, service continuity, and public confidence. This ranges from ransomware attacks on ticketing systems to insider-enabled vandalism of public Wi-Fi.

What makes the rail sector uniquely vulnerable is its reliance on legacy systems integrated with modern technology, often with limited native security controls. As operational technology becomes increasingly connected—to the cloud, to enterprise systems, and even to passenger devices—the attack surface widens considerably. Simulations and risk assessments suggest that the consequences of a successful, targeted cyber-attack could be catastrophic, ranging from mass service disruption to, in worst-case scenarios, safety-critical failures.

This evolving threat landscape reinforces the urgent need for the rail sector to adopt a proactive, system-wide cybersecurity mindset. Securing the future of rail is no longer just about physical protection or compliance—it demands embedded cyber resilience, continuous risk assessment, and a shared responsibility across stakeholders to defend what is undeniably critical national infrastructure.

# AI & Smart Monitoring: The Next Generation of Rail Safety & Efficiency

**The rail industry is undergoing a digital revolution driven by artificial intelligence (AI) and smart monitoring. Over the last decade, these technologies have reshaped how railways manage: maintenance, operations safety and passenger experience.**

Especially in the UK and across Europe, rail operators are leveraging data-driven tools to anticipate problems, streamline operations, and improve reliability.
As stated by Europe's Rail, AI is proving to be a gamechanger that can optimise complex railway systems, improve safety, enhance the passenger experience, and streamline operations.

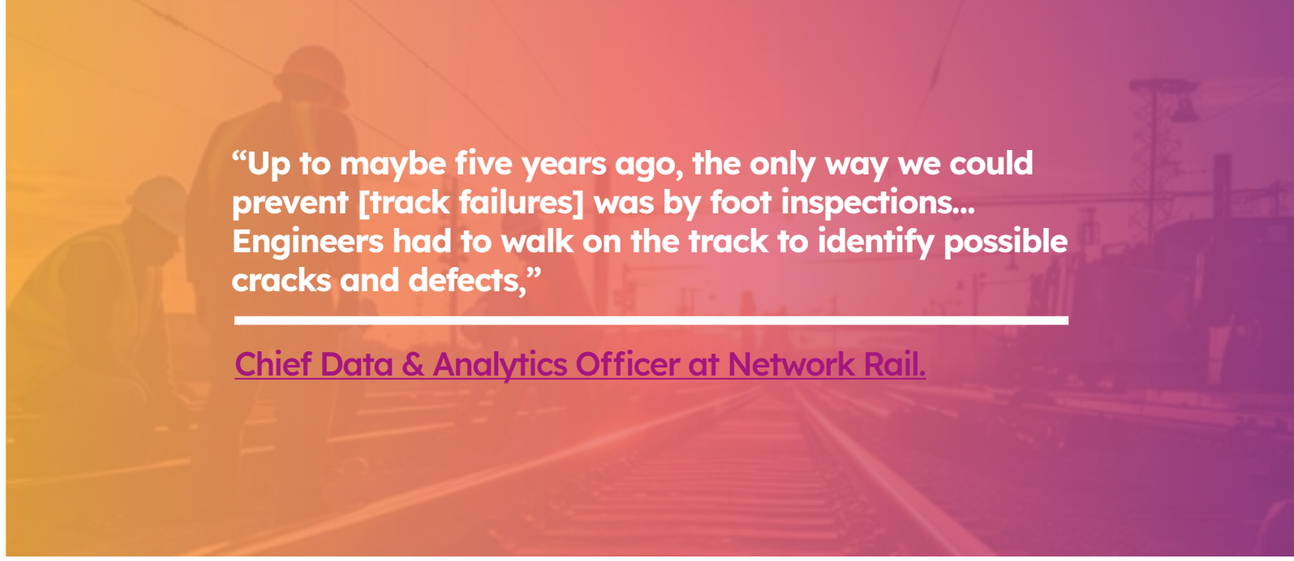
This chapter of the whitepaper explores how AI is transforming key aspects of the rail industry, the benefits it delivers, and how government and industry are enabling this transition. Petards are forward thinking in the field of AI, having continuously developed our future portfolio to better solve the needs of the industry.

## AI Applications in Rail Predictive Maintenance & Asset Management

Traditionally, railway maintenance followed fixed schedules or relied on manual inspections. This approach was reactive and inefficient. AI is enabling a shift toward predictive maintenance, where vast data from IoT sensors is analysed to forecast failures before they occur.

Embracing a **predictive maintenance** mindset is a significant shift for the industry. As an example, UK's Network Rail (which manages railway infrastructure) historically inspected tracks on foot to find problems, a laborious and reactive process.





> **"Up to maybe five years ago, the only way we could prevent [track failures] was by foot inspections... Engineers had to walk on the track to identify possible cracks and defects,"**
>
> Chief Data & Analytics Officer at Network Rail.

In the UK, Network Rail's Intelligent Infrastructure programme collects data from over 30,000 sensors across the network.

These include:

- **High-definition cameras**
- **LiDAR scanners**
- **Vibration monitors**

AI systems process this data to identify degradation in tracks, signalling, and electrical systems. Alerts are generated well in advance—sometimes up to a year—allowing engineers to fix issues proactively, reducing downtime and delays.

From 2019 to 2023, track issues resulted in 341 days of delays a year—representing a significant loss in operations.
Across the EU, similar projects are under development. The DAYDREAMS project integrates machine learning with physical asset models to not only predict failures but recommend optimal maintenance actions.

AI is helping to:

- **Reduce unplanned maintenance**
- **Extend asset life**
- **Improve workforce safety by minimising trackside exposure**

# Operations Optimisation

**AI enhances traffic control, scheduling, and real-time decision-making.**

In complex rail networks, adjusting operations to delays, weather, or demand fluctuations is critical. AI systems use historical and live data—train positions, speeds, weather forecasts—to predict disruptions and optimise traffic flow.

Projects across the EU, under the Europe's Rail initiative, are testing digital twins and AI-based traffic management platforms. These systems help reroute trains dynamically, reduce delays, and improve throughput without infrastructure expansion.

**10-15%**

energy savings are achieved as AI supports energy optimisation, with algorithms advising train drivers on optimal acceleration and braking.

While full autonomy is not yet mainstream, partial automation is emerging through AI-assisted driving and accurate train positioning using radar and SLAM-based models. This boosts line capacity and service resilience.

A key emphasis is to use AI in rail to augment staff, not replace them. This is in a similar manner to the Japanese quality improvement term "Jidoka" meaning automation with a human touch. Allow staff to focus their skills and problem-solving abilities where it is needed.



# Passenger Experience & Flow Monitoring

AI improves passenger service by analysing movement patterns and managing crowds. In the UK, LiDAR and AI crowd-monitoring systems were trialled at London Waterloo. These systems detect congestion and alert staff to intervene before safety risks emerge. Real-time heatmaps help redirect foot traffic and adjust station operations. AI also forecasts passenger demand by analysing ticket sales, events, and mobile data.

This enables operators to:

1. **Optimise train lengths**
2. **Reduce overcrowding**
3. **Enhance comfort**

AI-based **computer vision** systems are used in stations to analyse CCTV feeds for safety threats and personalise user applications. Modern CCTV paired with AI can **automatically detect if someone enters a restricted area** (e.g. on the tracks), if a dangerous crowd crush is forming, or even flag suspicious objects left unattended.

In one case, a European railway experimented with AI cameras that could identify **different behaviours.** There are even trials of cameras that estimate passenger demographics (such as age groups).

Overall, **real-time crowd analytics** help railway operators improve the flow through stations. This data supports dynamic signage, improving layouts, and congestion mitigation.

Few applications have seen this benefit more than passenger counting, which has allowed operations to tailor timetables and provide greater customer information to the public to manage the busy schedules of the rail industry.

# Safety & Security Monitoring

AI strengthens safety across infrastructure and operations.

Onboard obstacle detection systems using thermal cameras, night vision, and machine learning detect hazards like fallen trees or vehicles on tracks up to 1000 meters away—far beyond human visibility. At level crossings, AI-based monitoring identifies technical failures and potential intrusions. In stations, AI-integrated CCTV analyses crowd behaviour, detects unattended items, and flags suspicious activities.

These tools reduce risk and enable faster responses from control centres. Beyond this, the information can be processed on train and integrated to the trains control systems to provide an early warning to the driver (or the train's automated control system), which means more time to brake or act, potentially preventing collisions.

**Automatic obstacle detection is "an important first step towards autonomous driving and control of trains,"**

Valeria Vittorini, the coordinator of the RAILS project

AI also supports safer working conditions. With predictive tools, maintenance teams can operate more efficiently and remotely, limiting exposure to live tracks. By reducing emergency callouts, AI helps avoid high-risk, last-minute repairs. Finally, it's worth noting that by improving **overall system reliability,** AI indirectly boosts safety too.

A railway that experiences fewer equipment failures and fewer operational surprises is inherently safer. There are fewer chances for catastrophic failures (like broken rails or signal failures that can lead to incidents), and fewer instances where hurried actions or improvisations might lead to mistakes.

This is reflected in industry observations that, for example, predictive maintenance and passenger flow management through AI have a direct impact on safety outcomes.

By minimising conditions that could cause harm—whether mechanical faults or dangerous overcrowding—AI and smart monitoring are elevating the safety standards of rail transport, already one of the safest modes of travel.

## Benefits of AI & Smart Monitoring

**Improved Reliability, Safety, and Punctuality:** Predictive analytics drastically reduce service disruptions. By fixing infrastructure issues before they fail, railways experience fewer breakdowns and delays.

**30% fewer train breakdowns**

are possible with AI-based predictive maintenance, which also significantly reduces unexpected downtime, according to some estimates.

Using predictive maintenance enhances safety through preventing dangerous breakdowns and reduces time spent for workers in hazardous environments. In stations, crowd monitoring AI helps avoid dangerous overcrowding and can alert security to potential threats. Collectively, these improvements can lower insurance and liability costs for operators.

**Cost Efficiency**
Predictive systems lower maintenance costs significantly and extend asset lifespans.

**25% savings**

were reported by Deutsche Bahn through reduced downtime and improved performance.

**Capacity & Sustainability**
Optimised traffic management and energy-efficient driving increase throughput and reduce emissions. Smarter signalling, such as ETCS, and real-time adjustments reduce bottlenecks and headways, effectively increasing line capacity without new construction.

In the long run, these tools help railways meet growing travel demand and shift more traffic from road to rail in line with the UK net zero approach.

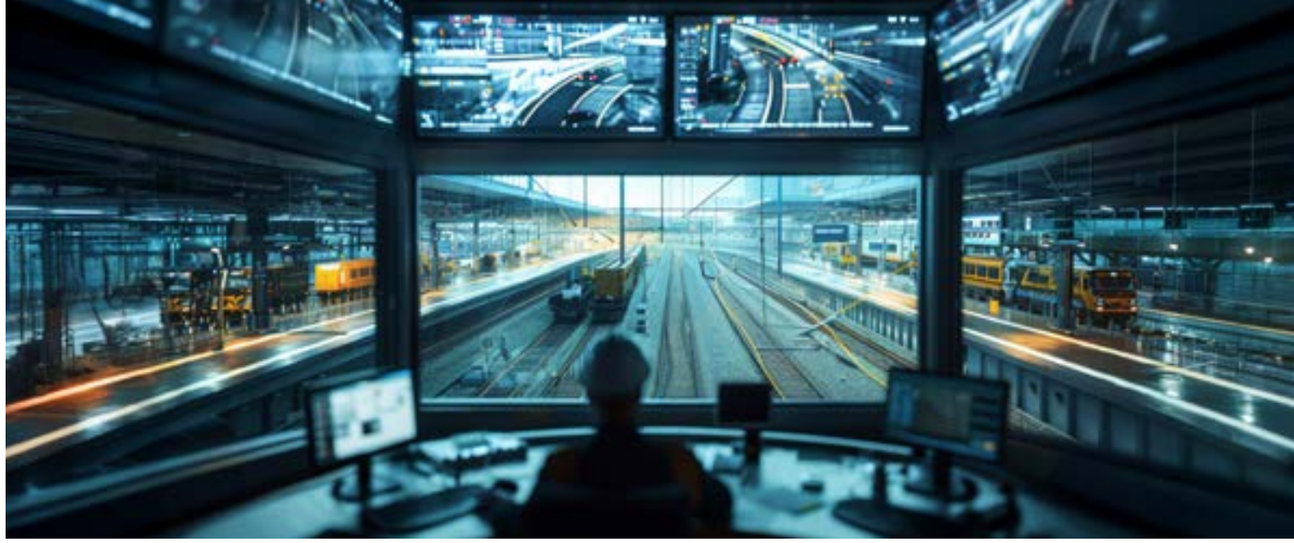
**Economic Growth and Innovation**
On a broader level, embracing AI and digital tech in rail positions the industry for long-term gains.

The UK government noted that AI will not only grow the economy but also improve public services like rail by cutting delays and maintenance times. A digitally transformed rail system can operate more affordably and handle more traffic, which supports economic activity by moving people and goods efficiently.

**3-8% revenue boosts**

are possible through AI optimisation of ticketing and pricing (yield management), allowing reinvestment in better services or infrastructure.





## Government & Industry Support

### UK Initiatives

**£58 million**

has been invested by the UK government in AI and rail innovations through programmes like **First of a Kind (FOAK),** funding 179 projects. These include:

**AI-based crowd monitoring**

**Predictive maintenance**

**Energy optimisation tools.**

Strategic frameworks, such as the 2023 Transport Data Strategy, aim to improve data sharing and stimulate digital innovation.

### EU Programmes

The Europe's Rail Joint Undertaking, successor to Shift2Rail, drives rail R&D across the EU. With public and private backing, it funds projects like DAYDREAMS, My-TRAC, and SMART that demonstrate AI's benefits in predictive maintenance, passenger engagement, and safety.

In line with these industry and government advances, companies like Petards are contributing to AI powered innovations.

### Petards and AI-Powered Rail Monitoring

Petards contributes to the AI transformation in rail through innovations such as:

**EyeTrain,** which uses forward-facing cameras and AI to identify issues like overgrown vegetation before they impact operations.

**Automatic Passenger Counting,** now enhanced with object classification (e.g., wheelchairs, bicycles) and achieving 98% accuracy—improving functionality while reducing installation costs.

**Pantograph Surveillance,** which leverages AI and HD IP CCTV with infrared to monitor overhead lines and detect events like arcing or contact loss, even in low-light conditions.

### Joining the Smarter Rail Journey

AI and smart monitoring are fundamentally reshaping how the rail industry operates. From preventing track failures to managing passenger flows and optimising energy use, these technologies deliver concrete improvements.

While challenges remain—data quality, interoperability, and workforce adaptation—the momentum is strong. AI is not replacing rail professionals; it is empowering them with better tools to deliver safer, more reliable, and more efficient services.

As adoption scales up, these innovations will become the foundation of a truly intelligent rail network.

# Digital Transformation & the Smart Rail Revolution – Innovations Shaping the Future

Digital transformation is no longer a buzzword but a strategic imperative across industries. In the UK alone, the digital transformation market generated approximately $52 million in 2024, with an expected annual growth of 29.5% through 2030 resulting in a forecasted $235 million revenue in 2030.

This momentum is reflected in business priorities: 94% of large organisations in the UK and US now have a formal digital transformation strategy, and over half plan to increase spending on such initiatives in 2025.

Government policy further reinforces this drive – the UK's digital strategy envisions every business in every sector becoming more productive through digital practices.
These trends underscore a broad recognition that emerging technologies can fundamentally improve:

- **Efficiency**
- **Customer experience**
- **Competitiveness**

The **rail industry** is poised to reap major benefits from this digital revolution. Rail networks worldwide face growing pressures:

- **Rising passenger and freight volumes due to urbanisation.**
- **Strict environmental targets for carbon reduction.**
- **Ever-high expectations for safety and reliability.**

A digitally enabled rail network offers powerful ways to tackle these challenges. Advanced technologies can modernise aging infrastructure and make rail transport safer, greener, and more efficient than ever before. From smart sensors on trains to AI-driven analytics in control centres, digital tools are reshaping how rail operators manage assets, serve passengers, and respond to issues in real time.



## Digital Transformation in the Rail Industry

Digital transformation in rail spans a wide range of applications, each addressing key operational and strategic needs. Notable areas where digital technology is making an impact include:

**Asset Management & Maintenance:**

Predictive maintenance systems use IoT sensors and analytics to monitor the health of trains and infrastructure in real time. Early signs of wear or faults can be detected and addressed before they escalate into failures, reducing unplanned downtime. This shift from reactive fixes to proactive maintenance extends asset life and improves service reliability.

**Real-Time Passenger Information:**

Digital platforms aggregate and disseminate live data on train schedules, platform assignments, delays, and disruptions. By delivering up-to-the-minute information to passenger smartphones and station displays, operators enable travellers to make informed decisions and adjust their journeys on the fly. Better information flow translates into improved passenger satisfaction and smoother operations during service changes.

**Signalling & Traffic Management:**

High-tech, computerised interlocking and traffic management systems optimise train routing and scheduling across busy networks. By automatically adjusting for optimal spacing and timing, digital signalling increases network capacity and throughput without compromising safety. It also enhances safety by reducing human error, enforcing speed limits, and maintaining safe distances between trains.

In essence, digital transformation allows rail operators to handle more trains and passengers with greater efficiency and safety. It is also a key enabler for rail to meet sustainability goals – for example, by optimising energy use through smarter driving profiles and regenerative braking systems.

## The Role of IoT in Connected Rail Ecosystems

The Internet of Things (IoT) has emerged as a cornerstone of the connected rail ecosystem. Modern trains are increasingly filled with smart devices and sensors, effectively turning each train into a rolling IoT hub.

These interrelated devices – from engines and brakes to door systems and CCTV cameras – continuously collect and exchange data with on-board computers and cloud platforms.

**30.9 billion**

**IoT-connected devices are projected globally by 2025, according to Statista - up from about 13.8 billion in 2021.**

Rail is part of this significant growth, as operators deploy IoT-enabled solutions to improve nearly every aspect of service. An IoT-connected rail network can **improve operations and passenger experience in numerous ways:**

**Passenger Flow Monitoring:**

Smart sensors (e.g. intelligent cameras or weight sensors) can monitor the flow of passengers through stations and train cars. This data helps identify crowding, optimise boarding procedures, and adjust train compositions or frequencies to match demand. Real-time occupancy data from such IoT systems can be fed back to passengers (via apps or station signs) to direct them to available seats and less crowded coaches.

**Data for Analytics & Personalisation:**

IoT devices continuously collect operational and environmental data – from temperature and vibration readings to usage statistics. Aggregating this data enables advanced analytics that support better decision-making. For instance, usage patterns can inform timetable adjustments or rolling stock allocation.

### Automation of Safety Alerts:

By combining IoT sensors with AI rail, operators can automate safety and security monitoring. Smart cameras and detectors can recognise hazards – like track obstructions, onboard smoke or fire, or dangerous behaviours – and automatically trigger alerts and responses. This improves the speed and consistency of safety interventions.

### Asset Tracking & Efficiency:

Beyond trains and passengers, IoT tracking devices can be attached to assets like luggage carts, maintenance equipment, or even railway infrastructure components. This provides real-time visibility of asset locations and statuses, improving logistical coordination. In train operations, IoT telemetry from locomotives and cars can be used to streamline operations – for example, monitoring fuel or energy consumption and adjusting for efficiency.

All these IoT-driven capabilities contribute to what is often called the **"smart rail" revolution.** By connecting devices and systems that were once isolated, IoT unlocks a holistic view of the rail network's status at any given moment. However, the proliferation of connected devices also introduces new challenges, particularly in **data management and cybersecurity** as discussed in Chapters 1 and 2. Vast amounts of data are generated every day, and making sense of this information requires robust analytics platforms.

## Data Intelligence & Predictive Analytics in Rail

Modern railways generate an immense volume of data from trains and infrastructure, and harnessing this data has become crucial for safety, maintenance, and efficiency.

Today's trains function as rolling IoT hubs, with sensors and subsystems logging everything from engine performance to door operations. **Every train produces gigabytes of log data daily, and turning this raw data into actionable information is key**. By analysing these datasets, rail operators can detect early warning signs of equipment issues and **prevent failures before they disrupt service, reduce maintenance costs, and enhance passenger safety.**

## Breaking Down Data Silos for Fleet Wide Intelligence

One major challenge has been the historical siloing of data across many independent systems on a train.

Traditionally, each onboard subsystem – whether an Automatic Selective Door Operation (ASDO) unit, an on-train CCTV system, or a braking controller – would store its own logs locally. **Valuable information often remained trapped on individual trains,** making it difficult to spot fleet-wide patterns or emerging issues that span multiple vehicles.

To address this, rail operators are investing in centralised data platforms that **automatically aggregate and sync logs from across entire fleets,** usually via secure wireless links to a cloud or central server, thus **breaking down the data silos** and ensuring maintenance teams have a comprehensive, fleet-level view of how all systems are performing.

In the UK, Network Rail's Intelligent Infrastructure programme illustrates the benefits of integration: their new "Insight" system consolidates data from multiple maintenance databases into one interface, making asset histories and alerts accessible in one place.

On the infrastructure side, a**nalytics on unified datasets can even predict failures before they happen.**

### 365 days in advance

—that's how early Network Rail can sometimes forecast when a section of track will likely develop a fault, thanks to aligning historical track geometry measurements from its monitoring trains. This kind of foresight was nearly impossible when data was scattered in separate systems.



## From Reactive to Proactive: Predictive Maintenance in Practice

Data intelligence is driving a shift in rail maintenance from a reactive approach to a **proactive, predictive maintenance** model. Instead of relying on time-based inspections alone, rail operators now use data analytics and machine learning to continually assess equipment condition and foresee problems.

For example, n**ew trains are increasingly delivered with built-in sensors and telematics that enable condition-based maintenance,** as noted by a UK fleet engineering director. By monitoring components in real time, maintenance can be scheduled based on actual wear and performance rather than a fixed interval, reducing unnecessary work on healthy parts and catching failing ones early.

To illustrate, a UK Rail Safety and Standards Board initiative uses an AI-driven tool that analyses data from trackside sensors to predict wheel defects on freight wagons **before they require urgent repairs.** By catching wheel wear and damage early, the tool helps avoid derailment risks and unplanned removals of freight trains from service, improving safety and saving costs.

This is one of many examples where data-driven anomaly detection is moving rail maintenance from fighting fires to preventing them.

## Benefits of Data-Driven Rail Operations

Implementing data intelligence and predictive analytics yields a range of benefits for rail operators and their customers. Some of the key advantages include:

**Fleet-Wide Visibility & Trend Analysis:** Aggregating data from all trains and infrastructure gives operators a birds-eye view of asset health. Patterns that would be invisible in isolated datasets become clear, enabling system-wide improvements. This big-picture view helps target the weakest links in the fleet and guides long-term asset management strategies.

**Early Fault Detection & Proactive Maintenance:** Predictive analytics tools use techniques like pattern recognition and anomaly detection to spot early signs of failures. By identifying issues such as intermittent sensor faults or abnormal vibrations in advance, maintenance can be performed before a breakdown occurs. This minimises unplanned downtime and avoids the costly domino effects of in-service failures.

**Optimised Maintenance Scheduling:** Data-driven insights allow maintenance to be scheduled at the optimal time – neither too early (wasting component life) nor too late (after a failure). By replacing components only when data indicates wear-out, rail companies extend asset life and reduce waste. Conversely, when data shows a high failure risk, maintenance can be accelerated to prevent incidents. Overall, this condition-based approach increases reliability and lowers lifecycle costs

All these benefits contribute to the broader goal of more resilient and efficient rail operations. When maintenance is predominantly proactive rather than reactive, trains spend more time in service and less time out of action. Failures that do happen are anticipated and contained, causing fewer service disruptions. Passengers experience more reliable journeys with fewer delays, and operators get more value out of their assets with lower overall maintenance spend.

The rail industry's embrace of data intelligence is still accelerating. Initiatives by bodies like the UIC and the European Union Agency for Railways (ERA) are fostering international collaboration on rail data standards and analytics, ensuring that lessons learned in one network can be applied globally.

In the UK, the Rail Safety and Standards Board and Network Rail continue to fund research and deploy new data-driven tools for everything from track geometry forecasting to AI-based inspections.

The direction is clear: **railways are moving decisively from hindsight to foresight.**

**"Innovation has always been critically important in the rail industry. And now more than ever, it's key to addressing the challenges ahead – from climate change to increased demand,"**

David Muse, Petards Rail's Chief Technical Architect.

## Petards Rail's Role in the Smart Rail Revolution

Delivering on the promise of digital transformation requires innovation, and Petards Rail has positioned itself at the forefront of rail tech innovation. Petards Rail's philosophy is rooted in collaboration and forward-thinking design, focusing on both cutting-edge software and rugged hardware solutions. The company's portfolio of **eyeTrain** products – ranging from advanced CCTV and sensing systems to back-office analytics – aims to make railways **safer, smarter, greener, and more efficient.**

## EyeBOS and EyeTrainConnect: Enabling Fleet-Wide Insights

The EyeBOS and EyeTrain Connect subsystems exemplify Petards Rail's data-centric approach to innovation:

EyeBOS: (the **eye**Train **B**ack-**O**ffice **S**ystem) is the central data syncing platform that **aggregates diagnostic and performance logs from across an entire fleet** into one place.

EyeTrainConnect: is the analytics engine and user interface that mines this rich data for actionable insights.

By eliminating data silos between individual trains and subsystems, Petards has given operators a fleet-wide "digital twin" of their operations that can be interrogated for trends, anomalies, and opportunities.

## Shape the Future by Joining the Smart Rail Revolution

The **smart rail revolution** is being realised through technologies like IoT connectivity, predictive analytics, and autonomous control systems, which together create a more responsive and resilient railway.

But technology alone isn't the full story – equally important are the **people and vision** behind these innovations. Petards Rail contribute by pushing the boundaries of what's possible and collaborating across the industry to implement new solutions.

Our EyeBOS and EyeTrainConnect subsystems are unlocking the power of data for fleet-wide intelligence, while ASDO and other eyeTrain products are delivering tangible improvements in safety and efficiency on the ground.

The result is a railway that:

- **Learns from its data**
- **Anticipates problems**
- **Adapts to changing needs in real time**

As rail networks continue to evolve digitally, passengers and operators alike stand to gain from a transport system that is smarter, more reliable, and more secure – truly shaping the future of rail mobility.

# The Future of Rail Security – Navigating Evolving Regulations & Compliance

**The UK rail industry is experiencing a surge of new regulatory requirements driven by technological change and policy goals.**

Operators and infrastructure managers must now address emerging risks across cyber, digital, safety and environmental domains.

For example, **cybersecurity** has become a top priority. The ORR emphasise that cyber threats are a "real and present risk" for rail, with clear safety implications. ORR stresses that duty holders must manage cyber risk "in the same way as any other safety risk" – integrating software and IT/OT security into their Safety Management Systems.

At the same time, the industry is modernising its **digital infrastructure** (e.g. digital signalling and networked control systems) to increase capacity and resilience, introducing new safety and security challenges. The combination of legacy technology and new has lead to recent discussions on interoperability to clarify impacts of digital infrastructure and other topics such as emissions and health and safety improvements.

Regulators are also renewing focus on **safety management:** for instance, in March 2025 ORR issued 10 recommendations to improve health & safety interventions, aiming to enhance decision-making, consistency and industry collaboration.

Finally, **environmental compliance** has joined the agenda: UK rail policy now explicitly targets decarbonisation and sustainability. ORR's remit includes duties to promote sustainable development and consider climate impacts; it explicitly highlights reducing diesel emissions and climate resilience. The ORR regulates the Department for Transport's 2021 Rail Environment Policy which commits to net-zero rail emissions by 2050, with all diesel-only trains off the network by 2040.



## Evolving Compliance Focus Areas

**Cybersecurity:**
Cyber threats to rolling stock and networks are treated as safety critical. Developments to the NIS2 guidance and the UK's cybersecurity and resilience Bill have introduced further measures to protect systems as well as expanding compliance to the wider supply chain. (See chapter 1 of Petards whitepapers on the future of rail cybersecurity).

**Digital Infrastructure:**
The UK's Digital Railway programme is accelerating digital signalling (e.g. ETCS), smart asset monitoring and automated control. While these advances boost efficiency, they bring new compliance needs. Railway electronics like cameras must meet rigorous standards and operators must demonstrate system safety under updated UK/EU Interoperability rules.

**Safety Management and Enforcement:**
The core UK safety regime remains the ROGS regulations (Railways and Other Guided Transport Systems (Safety) Regulations 2006), which requires all mainline operators to maintain a formal Safety Management System (SMS). Under ROGS and the Railway Interoperability Regulations, operators must comply with relevant safety standards – both compulsory technical standards (for vehicles and infrastructure) and those incorporated by contracts or SMS policies. UK regulators are also applying the EU-derived Common Safety Methods (e.g. on risk evaluation and conformity assessment) in domestic safety oversight.

**Environmental and Sustainability Compliance:**
Environmental regulation is embedded into rail oversight. Operators must manage climate-related risks (extreme weather impacts on infrastructure) and reduce pollution. ORR cites, for example, the need to cut diesel exhaust and plan for climate resilience. Government policy (e.g. the 2021 Rail Environment Policy) sets out priorities like phasing out diesel, increasing biodiversity, managing waste, and building energy efficient infrastructure.

## Accessibility, Operational & Safety Standards (UK/EU Context)

Rail operators must navigate a complex web of standards and regulations at national and European levels. Key requirements include:

**ROGS (Safety Management):**
ROGS provides the overarching safety framework for all GB rail. Under ROGS, all GB rail systems must have a documented SMS and risk assessment. Compliance with ROGS (and related provisions of the Railway Interoperability Regulations) are enforced by ORR via safety certificates/authorisations and periodic audits and applies to all levels of a supply chain. ROGS will be reviewed in 2026.

**Accessibility Standards:**
The Persons with Reduced Mobility TSI (PRM-TSI) (an EU interoperability standard) and UK accessibility law (PRM) set minimum accessibility features for trains and stations. Under PRM-TSI and the Rail Vehicle Accessibility (Non-Interoperable Rail System) Regulations 2010 (RVAR 2010), new heavy-rail rolling stock must include features like handholds, passenger information displays, priority seats and wheelchair spaces. Non-mainline vehicles (e.g. London Underground, trams) fall under RVAR 2010. UK policy historically targeted 100% accessible fleets by 2020 (subject to exemptions). Operators must track compliance (and any granted exemptions) under the Rail Vehicle Accessibility Regulations (e.g. via certificates from DfT/ORR).

**EU/GB Interoperability and Technical Standards:**
The UK has retained or replaced the EU's

Technical Specifications for Interoperability (TSIs) with GB National TSIs (NTSNs) to preserve cross-compatibility. Thus, train/building standards (for gauge, power systems, communications, etc.) largely mirror EU rules, but with differences to allow for the technical variation in UK designs. Separate EU-derived regulations – e.g. on infrastructure access, licensing, and train driver certification – similarly continue in UK law (often amended by 2019 EU Exit Regulations).

**Common Safety Methods (CSMs):**
As noted, CSMs are EU-developed processes for safety certification, monitoring, and risk assessment. In GB, CSMs are embedded in ROGS: transport undertakings must follow CSM procedures when making changes to the system, and ORR uses CSMs when assessing safety certificates and interventions. For example, the CSM on Risk Evaluation & Assessment requires systematic hazard assessment for any technical or operational change.

**Industry Standards (RSSB/Network Rail):**
In addition to legal rules, the industry relies on technical standards. RSSB publishes Railway Group Standards (RGS) – e.g. for track, signalling, electrification, – which operators are contractually bound to follow. Network Rail issues its own NR/L2 standards for infrastructure maintenance and engineering. While not "law", these standards are enforced through Network Rail contracts and ORR's oversight of NR and train operators. Guidance from RSSB and ORR (for instance on dispatching procedures or platform-train interfaces) also influences best practice.

# CCTV Compliance: Standards & Applications

Modern CCTV surveillance is integral to rail security and must meet stringent standards. In the UK/EU context, key requirements include EN 50155 and ISO/IEC 62676, among others.

**EN 50155 (Railway Applications – Electronic Equipment):**
This CENELEC/IEC standard governs electronic devices mounted on trains (rolling stock). It specifies environmental and electrical criteria (such as temperature range or vibration) that on-board equipment must endure. In practice, CCTV camera and recorders certified to EN 50155 are built to withstand the rail environment, although compliance may vary based on the classifications met. For example, there are different classifications for temperature range compliance depending on the environment. Compliance with EN 50155 is mandatory for any surveillance cameras installed on trains in the UK.

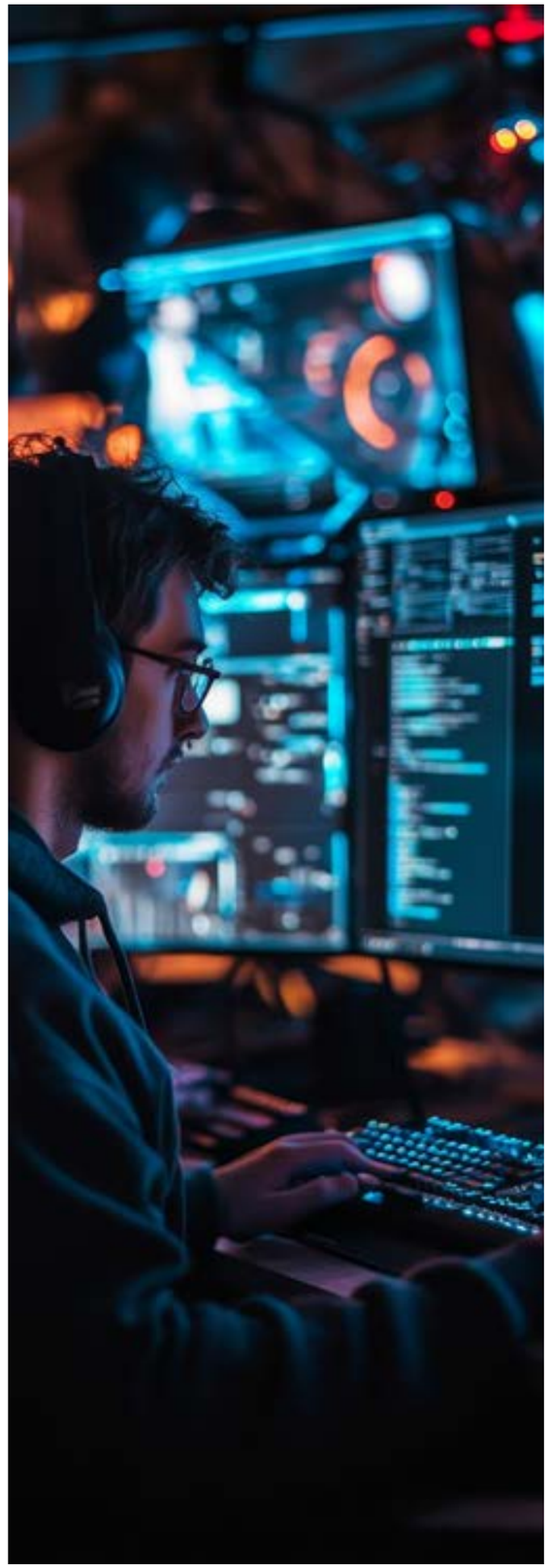
**ISO/IEC 62676 (Video Surveillance Systems):**
This international standard defines functional and performance requirements for CCTV systems used in security applications. It covers aspects like image quality, frame rates, video storage, metadata, and interoperability. For instance, ISO/IEC 62676-5-1 (2024) specifies measuring methods for camera performance and image quality. Conformance to ISO/IEC 62676 ensures that video equipment meets agreed standards for reliability, analytics support, and system integration. Rail CCTV installers often use ISO/IEC 62676 guidelines (and related BSI/BS EN documents) when designing surveillance networks for stations and depots.

**RSSB:**
The RSSB has a multitude of standards and guidance applicable to CCTV systems. The most common for on train CCTV are RIS-2712-RST (On train camera systems) and RIS-2703-RST (Driver controlled operation). These identify the requirements for view coverage and provide greater detail on interfaces and needs specific to the UK in collaboration with major operators and train builders.

**Critical to safety:**
These primarily consider EN50126, EN50716, and EN50128. These standards cover reliability of hardware and software for vital train functions, such as Automatic Selective Door Operation (ASDO) systems to digital signalling systems. The standards define a Safety Integrity Level (SIL) from 1 to 4 based on the likelihood and severity of a system failure. Strict reliability and redundancy requirements are necessary for approvals, along with third-party assessments to prove a system to these standards.

**Cybersecurity**
More recently, cybersecurity has become significant for the rail industry. Standards such as IEC 62443 have components that date back to 2009. Despite its availability, adoption within the rail industry has been slow. Now that Operational Technology (OT) and Information Technology (IT) have become intertwined, securing the digital functions of the rail industry has become crucial to maintaining operations. New standards, such as IEC 63452, are currently in draft and aim to provide specific guidance for rail to prevent vulnerabilities, highlight importance of continuous monitoring and patching, and supporting across the lifecycle of railway systems.

**Other Relevant Standards**
CCTV systems also intersect with other rail/industry standards. EN 50121 (EMC for fixed and train-borne installations) and IEC 62236 (EMC for rolling stock) ensure cameras do not interfere with train signalling or communications. EN 45545 (fire protection) ensures any mounted equipment is fire resistant. Any IT networks used for CCTV must follow UK government cyber standards (e.g. the NCSC's guidelines) to prevent unauthorised access.



## CCTV contributes to compliance in multiple ways.

**Safety monitoring:**
cameras enable constant observation of critical areas (platform edges, level crossings, depots, tunnels). For example, Network Rail explicitly states that it uses surveillance systems “to monitor and maintain safety and security” of stations and infrastructure and to deter crime. CCTV can automatically detect trespass or objects on the track (using video analytics), triggering alarms that help prevent accidents.

**Passenger security:**
high-definition CCTV deters vandalism and assault and provides evidence to the British Transport Police. When incidents occur, recorded video is invaluable for incident investigation. Footage can clarify causes of accidents (supporting RIDDOR reporting) and incidents such as slip-and-fall or assaults on trains. Industry standards recognize this role: for example, the RSSB’s RIS-2712 guidance on on-train cameras explicitly addresses how recorded data should be accessed by police and how systems must allow retrieval of evidence for investigations.

**Cybersecurity:**
is vital with modern CCTV being IP-based, so securing these systems is crucial. In practice, this means encrypting video feeds, segmenting networks, and following data-protection rules for passenger images.

## Petards’ Compliance Journey

### Safety Systems & SIL

Navigating international compliance is complex. As a supplier of critical safety systems, Petards have approved numerous Automatic Selective Door Operation (ASDO), and Driver Controlled Operation (DCO) systems, from Basic Integrity (formally known as SIL 0) to SIL 2. The learnings on reliability and software integrity have expanded our teams’ skills to face the modern challenges of the rail industry, such as maintaining operational uptime and cybersecurity resilience.

### Cybersecurity

One step of Petards journey has resulted in ISO 27001, Cyber essentials, and CS plus compliance to secure our business operations and data against cyber threats. Forming part of our Information Security Management System (ISMS), we are committed to protecting our digital assets and yours. We strive to achieve the lowest risk to our customer operations, so we work closely with cybersecurity experts to align our system to the IEC 62443 series and monitoring future releases.

### Industry Engagement

Having worked with RSSB frequently in industry in past projects, we have all our systems compliant with the applicable RIS standards. Recently, we have become a member of the RSSB, with part of the standard board for RIS-2703-RST providing our expertise to push for continued progress in the CCTV and safety system fields.

### Obsolescence Management

Considering the impact of obsolescence in the rail industry, and wider, Petards have aligned our obsolescence policy to IEC 62402 and our customer needs to minimise the impact. With decades supporting OEMs, ROSCOs, and operators in the rail industry, we are well versed in offering consultation on the appropriate standards and writing of technical specifications. This includes for everything from requirements such as REACH/ROHS and WEEE regulations, to international data and safety standards.



## The Need to Navigate Evolving Regulations & Compliance in Rail Security Today

In summary, UK rail compliance is becoming more stringent and wide-ranging. Operators must navigate a layered framework of regulations and standards – from ROGS and UK NTSNs, to accessibility laws (RVAR/PRM-TSI) and technical standards (e.g. EN 50155, ISO/IEC 62676) – all while adapting to new technological realities.

CCTV exemplifies this intersection:

- The hardware and data handling of these systems must meet electrical and safety standards.
- Its deployment must satisfy privacy laws.
- Its functionality, and software, must serve wider safety and security goals.

By understanding and anticipating these evolving requirements (through official guidance from ORR, international standard boards, RSSB), rail stakeholders can ensure their systems remain compliant and effective in protecting passengers, staff, and assets.

# ESG & CSR in the UK Rail Industry

Environmental, Social, and Governance (ESG) and Corporate Social Responsibility (CSR) have become central to the UK rail industry's strategy.

While CSR historically emphasised compliance and philanthropy, ESG introduces measurable sustainability performance indicators.

**9% of passenger miles**
were carried by rail in 2019, while it contributed only 1.4% of UK domestic transport emissions—highlighting its clear green advantage.

Now, the sector is expanding its focus beyond emissions to broader ESG goals:

- **Reducing environmental impact**
- **Enhancing social value (such as workforce diversity and safety)**
- **Strengthening governance (ethics, transparency, and accountability)**

This summary examines recent developments, benchmarks, future outlooks, and a case study reflecting ESG in action.

## Evolution Over the Last Five Years

Since 2020, ESG and CSR have shifted from peripheral concerns to strategic priorities. Key to this shift was government policy. The Social Value Model (PPN 06/20) mandated the inclusion of environmental and social value in public contracts, compelling suppliers to prove their societal contributions. Furthermore, climate disclosure regulations (effective from April 2022) required major transport companies to report climate-related financial risks in line with Task Force on Climate-related Financial Disclosures (TCFD) recommendations.

Industry initiatives also drove change. The 2020 Equality, Diversity & Inclusion (EDI) Charter, signed by over 200 organisations, signified a sector-wide commitment to inclusivity. Simultaneously, companies adopted science-based emissions targets, with Network Rail becoming the first global railway company to commit to the highest-level SBTi targets. Electrification efforts and trials of hydrogen and battery-powered trains advanced decarbonisation goals.

Investor expectations and recognition have evolved too. In 2025, FirstGroup plc earned top-tier ESG ratings and inclusion in a global sustainability yearbook. Bodies like the Rail Safety and Standards Board (RSSB) introduced initiatives such as the "Sustainable Rail Blueprint," which earned ESG leadership awards. Overall, UK rail has embedded ESG into strategies, reports, and leadership priorities.




## Current Benchmarks & Best Practices

UK rail companies are now assessed on ESG criteria alongside financial metrics. Most publish annual ESG or sustainability reports aligned with GRI or TCFD frameworks, covering data such as energy use, emissions (Scope 1–3), safety, workforce demographics, and social impact.

Key benchmarks include:

**Carbon Intensity**
$CO_2$ per passenger-km or ton-km, with 2019/20 showing record-low levels.

**EcoVadis Assessments**
Used by suppliers to benchmark ESG performance.

**Best practices** fall into three main categories:

### Environmental Stewardship:

Targets often align with the UK's 2050 net-zero goal, aiming for ~30% emissions reductions by 2030. Strategies include electrification, alternative fuels, smart energy use, and circular economy principles. Trials of battery-electric and hydrogen trains support long-term emissions cuts. Other efforts include improved recycling, water conservation, biodiversity protection, and climate resilience investments (e.g., infrastructure upgrades for extreme weather).

### Social Value and Inclusion:

Safety programs prioritise zero-harm workplaces. Over 200 firms support the EDI Charter, committing to actions like appointing EDI champions and increasing representation of women and minorities in leadership. Companies run apprenticeships and STEM outreach programs, focusing on underrepresented communities. Social responsibility extends to accessible travel and meaningful community engagement. These initiatives align with the UK Social Value Model themes, making social impact a competitive factor in contract bidding.

### Governance and Transparency:

Strong governance frameworks ensure accountability. Many rail firms have board-level ESG oversight and enforce anti-bribery policies across their supply chains. Transparent ESG disclosures aligned with TCFD recommendations and regular external audits provide stakeholder confidence. Ethical governance has become key to securing partnerships and financing—green bonds and other sustainability-linked instruments increasingly favour ESG-led companies.

Overall, UK rail companies are expected to deliver not just reliable service, but services that support low-carbon transitions, community wellbeing, and ethical standards.

## Future Outlook

The UK rail ESG agenda is set to intensify. Environmental ambitions will rise, particularly around decarbonising freight and eliminating diesel. Investment in electrification and clean propulsion will grow, and the Sustainable Rail Strategy is expected to provide a 30-year decarbonisation and circular economy roadmap. Future infrastructure will likely aim for zero-emission operations and increased use of renewable energy.

On the social side, addressing workforce skill gaps will be vital as older engineers retire and technology evolves. Talent strategies will increasingly focus on diversity and inclusion, supported by transparency and sector-wide targets. Operators will continue community engagement and enhance wellbeing—both employee and passenger-focused—to meet societal expectations and government objectives like “levelling up.”

Governance requirements will tighten. ESG reporting will expand to cover biodiversity and nature impacts, guided by frameworks like Taskforce on Nature-related Financial Disclosures (TNFD). Investors will demand stronger, assured data and evidence of impact. Procurement may assign even more weight to ESG credentials, and supply chains will need to align with sustainability standards set by major clients.

There are also suggestions from governance trends that ESG integration into executive pay and leadership structures will continue, reinforcing accountability.

## The Importance of Achieving Strong ESG Performance

ESG is no longer optional for UK rail; it’s integral to competitiveness, credibility, and long-term viability.

With rail central to achieving national net-zero goals, strong ESG performance reinforces the business case for rail expansion and investment. As investor and passenger preferences shift toward ethical and sustainable providers, the industry’s future will depend on sustaining and accelerating ESG excellence—delivering a rail system that is clean, inclusive, ethical, and resilient.



## Petards Joyce Loebl – From compliance to commitment

In 2021, Petards Joyce Loebl (PJL) undertook a strategic re-evaluation of its role in the UK rail market, supported by an independent third party.

This involved:

- **Interviews with employees**
- **Engagement with customers and supply chain**
- **Market research**
- **Competitor risk analysis**

The aim was to gather feedback from key stakeholders and conduct a structured Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis to understand how to build on strengths, address weaknesses, seize opportunities, and mitigate threats.

From this analysis, two key themes emerged:

1. Establishing PJL as a great place to work, through a positive and inclusive workplace culture.
2. Demonstrating PJL’s commitment as a responsible and ethical supplier, beyond technical delivery.

These insights led PJL to adopt a proactive and embedded approach to Corporate Social Responsibility (CSR), moving beyond compliance to make it a core business principle.

## Understanding CSR at PJL

CSR at PJL covers four key areas:

### Environmental Responsibility

Emissions reduction, waste management, resource conservation.

### Ethical Business Practices

Fair employment, anti-corruption, responsible sourcing.

### Community Engagement

Local outreach, charitable initiatives, education support.

### Workplace Responsibility

Employee well-being, diversity, and a safe, inclusive environment.

Although PJL was already ISO 9001 and ISO 14001 certified, with an established Integrated Management System and strong local presence, we challenged ourselves further: *Are we truly embracing CSR? How do we demonstrate this to stakeholders?*

This reflection led to a structured strategy to embed CSR into PJL’s values and operations.

## Embedding Core Values: The S.P.I.R.I.T. of PJL

In 2022, we relaunched our core values as S.P.I.R.I.T.:

**Safety** **Pride** **Integrity** **Respect** **Innovation** **Talent**

These values guide daily operations and were reinforced by a monthly S.P.I.R.I.T. Award. Winners receive personal recognition and a donation to a chosen charity, fostering a value-driven culture across PJL.

## Aligning with Global Standards: UN Global Compact

EcoVadis feedback highlighted two major gaps: lack of defined CSR objectives and weak alignment with global goals.

To address this:

**In 2023, PJL joined the United Nations Global Compact (UNGC), aligning with its ten principles covering Human Rights, Labour, Environment, and Anti-Corruption.**

**We published our first CSR Report in 2023, covering our 2022 performance, followed by the 2024 edition.**

These reports offer transparency and include:

- Mission, vision, and values
- SDG alignment
- Environmental and social KPIs
- Stakeholder impact assessments
- Continuous improvement strategies



## Skills Development: Apprenticeships

To strengthen future capabilities, PJL welcomed three Maintenance Operations Engineering Technician apprentices in 2023. The two-year program will conclude in June 2025, with successful candidates joining as full-time employees.

## Enhancing Certifications

In response to stakeholder expectations and EcoVadis feedback, PJL pursued two key certifications:

**ISO 45001:2018 – Occupational Health & Safety (OH&S) Management System**
Building on our strong safety culture, PJL implemented a structured OH&S system and achieved certification in November 2023, confirming our commitment to employee safety and risk management.

**ISO 27001:2022 – Information Security Management System**
Given our role in the Defence sector, PJL already upheld high security standards. In 2024, we formalised this by attaining ISO 27001 certification in May 2024, further safeguarding our data, systems, and stakeholders.

## EcoVadis 2023: From Silver to Platinum

In March 2024, PJL submitted its EcoVadis assessment for the 2023 calendar year, aiming for Gold status. The submission included improved policies, KPIs, and CSR results.

**Top 1% globally**
That's where PJL ranks with a Platinum Award—recognising our high standards in sustainability, ethics, and labour practices.

## Tangible Results: Environmental Performance

Our efforts have led to measurable improvements:

**26% reduction**
in Scope 1 and Scope 2 emissions since 2021: Greenhouse Gas Emissions.
Key initiatives include:

Key initiatives include:

- Energy-awareness campaigns
- Upgraded high-efficiency boiler
- Switching from gas to electric forklifts
- Operational restructuring for efficiency

**44% reduction**
in water consumption since 2021, due to water-saving fixtures and reduced facility usage post-COVID.
These outcomes demonstrate our focus on continuous environmental improvement and sustainable operations.

## 2025 & Beyond: Continued Momentum

PJL started 2025 with several significant recognitions:

- **Made in North East – Sustainable Manufacturer Award**
- **Alstom's Fighting Climate Change SME Award**
- **Shortlisted for the National Spotlight Rail Corporate Responsibility Award**

These achievements affirm PJL's ongoing leadership in CSR and ESG, highlighting our dedication to sustainability, ethical practices, and a people-first culture.




## The Need to Treat Sustainability & Social Responsibility with the Utmost Importance

The evolution of ESG and CSR in the UK rail industry underscores a broader transformation: sustainability and social responsibility are no longer optional add-ons but fundamental drivers of business viability and success.

Over the past five years, rail stakeholders – from government bodies and industry associations to operators, manufacturers, and suppliers – have collectively raised the standards for what responsible business means in this sector.

Today's rail companies are expected to deliver **cleaner, safer, and more inclusive transportation** while maintaining robust governance. The industry's progress is evident in the widespread adoption of ESG benchmarks and best practices, and in success stories like Petards Rail which demonstrate leadership at every level of the supply chain.

The journey, however, is far from over. As the UK navigates the path to net-zero and strives for greater social equity, the rail industry will play a pivotal role. Continued collaboration will be key – whether it's sharing innovations to cut emissions or partnering on skills and diversity partnering on skills and diversity initiatives – as will transparency in reporting outcomes.

Importantly, the alignment of ESG goals with business strategy means that doing the "right thing" and achieving commercial objectives are increasingly one and the same. Rail companies that excel in sustainability often find operational efficiencies, stronger stakeholder loyalty, and new funding opportunities (such as green financing), creating a positive feedback loop.

Conversely, falling behind on ESG could pose risks, from regulatory penalties to reputational damage in an era of heightened accountability.

In conclusion, the UK rail industry's embrace of ESG and CSR principles positions it as a **torchbearer for sustainable transport.** By retaining focus on environmental innovation, social value creation, and ethical governance, rail can solidify its status as the backbone of a greener and fairer mobility system.

The last five years have laid a solid foundation – and with continued commitment, the next chapters will likely see UK rail not only meeting its sustainability targets but also setting new benchmarks for others to follow.

## The trajectory is clear

*Rail's future will be driven by those who integrate ESG into every mile of track and every corporate decision,* ensuring long-term resilience and shared value for all stakeholders.

**Visit us: petardsrailsolutions.com**
**Contact us: rail@petards.com**

Petards Rail
intelligent train technology