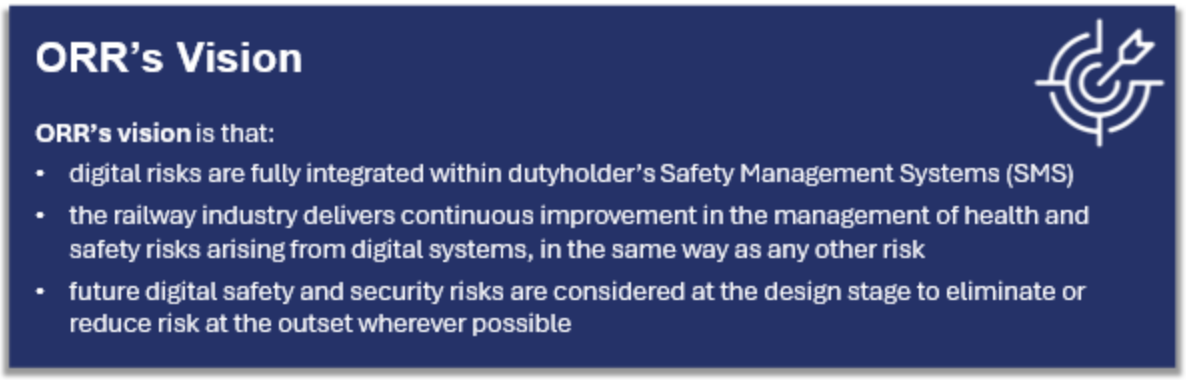
Digital safety

1. Executive summary

The rail industry depends on software-driven and digitally connected systems. These systems now influence, and in some cases control, safety-critical functions across rolling stock, signalling, infrastructure, communications and operations. This transformation is delivering clear operational benefits, including improved performance and efficiency. However, it also introduces an evolving category of safety risk. Unlike traditional engineering hazards, digital risks arise from system complexity, continuous change and the interaction between technology, data and human decision-making. These risks are often less visible, harder to detect and more difficult to manage using conventional approaches.

ORR's view is that digital safety risk is often not confined to individual systems but emerges across the wider railway given how digital technologies are designed, integrated, changed and operated. As reliance on automation and Artificial Intelligence (AI) grows, these risks are further influenced by evolving interactions between humans and systems, as well as the increasing role of data and decision-support tools.

Digital safety risk therefore affects all parts of the railway system, including passengers, workforce and the wider public. Failures may result in unsafe conditions directly, or indirectly through operational disruption, degraded working and increased reliance on manual intervention. The increasing connectivity of railway systems also means that risks may originate beyond the immediate railway environment, including within supply chains and external digital infrastructure.



To deliver this vision, ORR is focused on strengthening how digital safety is managed across the system lifecycle. This includes:

- improving governance of digital systems;
- ensuring that change is effectively controlled;
- enhancing industry competence in digital risk;
- promoting structured learning from incidents;
- improving resilience and recovery capability and
- encouraging effective collaboration between safety and security teams through an holistic approach to managing digital safety risk.

Dutyholders must understand how digital systems affect their operations and apply effective controls to manage associated risks. This includes clear governance and accountability, robust management of software and change across the system lifecycle, effective supply chain oversight, and the application of safe and secure design principles (see ORR's strategic risk chapter on Health and safety by design). Dutyholders must also apply human factors principles, understand system behaviour and incorporate learning from incidents to drive improvement.

ORR will continue to engage and challenge the industry to build capability, improve maturity and deliver continuous improvement. Where digital safety risks are not adequately controlled, ORR will take proportionate enforcement action.

- → Next 2. Our view of the risk

2. Our view of the risk

Understanding the digital safety risk

Digital technologies are embedded across the railway system. They influence or directly control safety-relevant functions across rolling stock, signalling, infrastructure management, passenger information systems and operational control systems. Examples include Automatic Train Operation (ATO), train control and signalling systems, traction and braking control functions, traffic management platforms and software-based asset monitoring systems. These systems deliver significant benefits to the railway. They enable improved safety and service performance, enhanced operational efficiency and increased network capacity. However, they also introduce new forms of safety risk that differ fundamentally from those traditionally associated with mechanical or electro-mechanical railway systems.

Digital safety risk primarily relates to Operational Technology (OT) and other digital systems that monitor, influence or directly control operational or safety-relevant functions. This is distinct from enterprise IT systems used for general business purposes, such as email or office applications, which may affect business continuity but would not normally create direct safety consequences if lost. The distinction matters because failure of OT systems, such as train control, signalling, traction or braking functions, can directly affect safe operation.

Digital safety risk arises where software-driven or digitally connected systems fail, behave unexpectedly, or interact with other systems in ways that create unsafe conditions or operational disruption with potential safety consequences.

Unlike conventional engineering failures, digital system failures can emerge from complex interactions between software, hardware, data and human decision-making. Failures may arise from design defects, configuration errors, system integration issues or malicious interference. They may also occur without visible physical damage to equipment, making them harder to detect and investigate. Effective management therefore depends on understanding the digital estate, system architecture and the traceability between functional requirements, software specification, software architecture and code, so that changes can be properly assessed, managed and recorded throughout the system lifecycle, supported where appropriate by frameworks such as BS EN 50716.

As the railway continues to adopt more complex digital technologies, including automation, artificial intelligence and connected infrastructure systems, understanding and managing the associated risks becomes even more critical.

Digital safety risk therefore concerns not only individual systems but the wider ecosystem within which they operate. Effective management requires dutyholders to understand how software systems behave, how they interact with other systems and how failures may propagate across operational and organisational boundaries.

Who is affected by digital safety risk

Digital safety risks can affect multiple groups across the railway system. Passengers may be exposed to safety risks where digital failures affect train movement, platform operations or passenger management systems. Operational disruption caused by digital system failures may also lead to secondary safety risks, such as crowding or unsafe evacuation scenarios.

Railway staff may be affected where digital systems support operational decision-making, maintenance activities or safety-critical procedures. Failures in these systems may create conditions where staff must operate under degraded modes or rely on manual processes. Due account must be taken of this in Business Continuity Plans (BCPs) and/or Disaster Recovery Plans (DRPs), ensuring that risks remain safely controlled in degraded operation.

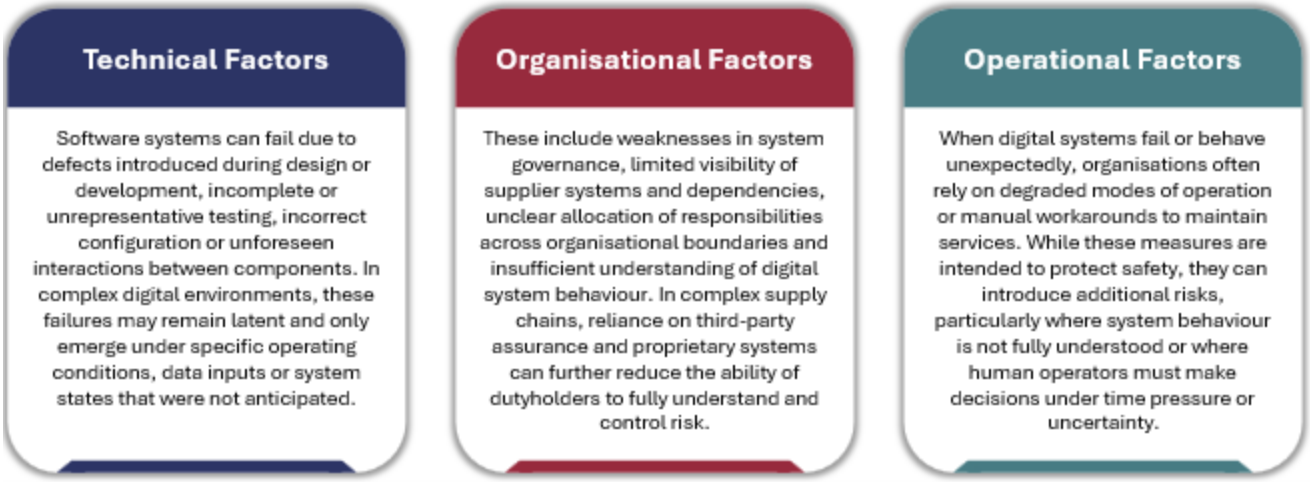
Infrastructure managers and operators are also exposed to system-level risks where digital failures affect signalling systems, train control systems, communications networks or asset monitoring systems.

In addition, the wider public may be affected where failures disrupt critical infrastructure or impact services that depend on railway operations.

The increasing integration of railway systems with wider digital infrastructure, including communications networks, cloud services and external suppliers, means that digital disruptions can also originate outside the railway sector itself, including failures in communications networks, cloud services or supplier-operated systems on which railway operations depend.

How digital safety risk emerges

Digital safety risks typically arise through a combination of technical, organisational and operational factors. These factors rarely act in isolation and often interact in ways that are not fully understood until systems are in operation.



Key cross-cutting risk themes

Analysis of recent incidents, stakeholder engagement and industry evidence identifies several recurring themes that shape digital safety risk across the railway sector.

Increasing dependence on complex digital systems

As rail operations become increasingly dependent on software-enabled systems, digital failures have greater potential to affect safety, performance and operational resilience. The principal risk is not the adoption of digital technology itself, but the growing complexity and interdependence of systems, data, communications networks and operational processes.

This creates a "system-of-systems" environment in which failures may emerge from interactions between components, organisations and technologies rather than from a single asset failure. As reliance on automation, AI and connected infrastructure increases, understanding and managing these interdependencies becomes a critical component of effective safety management.

Digital failures differ from electro-mechanical failures

Mechanical failures typically involve physical degradation or damage that can be observed and investigated directly. Digital failures, by contrast, often occur without visible physical indicators. Software defects may remain latent for extended periods before being triggered by specific operating conditions or data inputs. Furthermore, digital failures may emerge from subtle issues such as incorrect configuration parameters, unexpected data combinations or hidden dependencies within software logic. These types of failures may only manifest under rare operational scenarios that cannot be identified during testing. This reinforces the importance of

functional testing being proportionate based on the impact of change, including regression testing (testing to confirm that existing functions still work as intended after a change), before operational deployment, so that system behaviour can be validated under both normal and abnormal conditions before the system is relied upon in service. Operational deployment is typically a staged process; therefore, this allows problems to be identified early in an isolated part of a fleet.

Investigating digital failures also presents challenges. Accident investigators have noted that, unlike conventional engineering failures, digital incidents may leave little physical evidence. Instead, investigations must rely on system logs, software behaviour analysis and configuration data to determine the cause. These characteristics mean that digital systems require different approaches to safety assurance, monitoring and investigation than traditional railway equipment.

Cambrian Line ERTMS Incident (2017)

Following a routine overnight restart of the European Rail Traffic Management System (ERTMS) on the Cambrian Coast line, temporary speed restriction (TSR) data failed to reload correctly into the signalling system. As a result, TSR information was not transmitted to trains, reducing safety margins at multiple level crossings.

The control centre interface incorrectly indicated that the restrictions were active, meaning operators were unaware that safety-critical data had not been applied. There was no effective validation mechanism to confirm that the data had been correctly restored following system restart. The incident also highlighted the challenges associated with modifying and operating legacy digital systems, where system behaviour and data handling processes may not be fully transparent or understood.

Learning: This incident demonstrates how digital failures can occur without visible physical indicators and may remain undetected where system feedback is misleading. It highlights the importance of data validation, system transparency and robust assessment of changes to legacy systems, particularly where design assumptions and system behaviour are not fully understood.

Poorly controlled change is a primary trigger

Many digital safety incidents occur during periods of system change. Software updates, configuration modifications, maintenance activities or system upgrades may introduce faults, expose hidden defects or trigger unexpected system interactions. Since software systems evolve over time through multiple incremental updates, the cumulative impact of change (additionality under CSM-REA) can be difficult to assess. Change to digital systems must be properly controlled, to avoid introducing new and poorly managed safety risks.

Particular care is required where changes are made to existing or in-use systems. In many cases, original design assumptions, system behaviour and dependencies are not fully documented or understood. This can make it difficult to assess the impact of modifications and increases the risk of unintended consequences when changes are introduced.

Software patches and system modifications are sometimes implemented without the same level of scrutiny traditionally applied to mechanical engineering changes. In some cases, organisations rely heavily on supplier assurances that updates have been adequately tested. Effective change management therefore remains one of the most critical elements of digital safety assurance. Dutyholders must ensure that system modifications are properly assessed, tested and validated before deployment.

Standards such as BS EN 50716 provide guidance on the requirements that must be fulfilled for development and modification of software associated with railway applications.

Interface and integration risk

Risk often concentrates at interfaces between systems, organisations and technologies. Railway systems operate within complex integration environments where multiple subsystems interact with one another. These may include signalling systems, rolling stock software, operational control platforms and communications networks. Integration risks are particularly pronounced where new digital systems are introduced into existing infrastructure environments. Existing or in-use systems may use different architectures, data formats or operational assumptions than modern digital technologies. Safe integration therefore requires a clear understanding of system boundaries, responsibilities and operational dependencies across the wider railway ecosystem.

Four Lines Modernisation (4LM), London Underground

The Four Lines Modernisation (4LM) programme is implementing a digital train control system in a highly complex brownfield railway environment. The system is being deployed in several stages, on infrastructure never originally designed to support modern digital signalling, requiring integration between legacy assets, new technology and multiple operating services.

The programme highlights the challenges of implementing digital systems in constrained environments with mixed technologies and evolving requirements. Modifying and building upon legacy systems requires careful assessment of the assumptions and behaviour of the legacy design, which were not always fully documented as part of the original legacy development.

Safe operation also depends on accurate representation of the physical railway within the digital system. As errors can lead to incorrect system behaviour, such as trains misinterpreting their position, the quality and integrity of asset and location data are critical. Delivery is necessitating close coordination between operators, maintainers and the supplier, with risks distributed across organisational and technical interfaces.

Learning: This case study demonstrates that digital safety risk arises from system integration, data integrity and the complexity of modifying and deploying new technology within existing infrastructure. Effective management requires a system-level approach, clear understanding of legacy system behaviour and strong coordination across organisational boundaries.

Autonomy and automation shift risk boundaries

The increasing use of automation and AI is changing the relationship between human operators and railway systems. In a railway context, this may include automated decision support, automated train operation, traffic management assistance, condition monitoring or systems that influence operational control without direct human input at every stage.

Automation can improve operational performance and reduce human workload. However, it also introduces new risks where operators rely on automated outputs without fully understanding system behaviour. It is therefore important to clearly define the role of automation within operational processes. Dutyholders must ensure that human operators remain able to intervene where automated systems behave unexpectedly or where operational conditions fall outside normal parameters. This is particularly relevant where human operators become so reliant on the systems that they either don't know when they are not working as designed or cannot operate without them.

Supply chain and third-party dependency

Modern railway systems depend heavily on complex supply chains. Digital systems are often developed, configured and maintained by external suppliers. In many cases, dutyholders rely on

proprietary software systems where full visibility of internal design and functionality may be limited due to intellectual property restrictions. This reliance on suppliers can create safety risks where system behaviour is not fully understood by dutyholders or where responsibility for system assurance becomes unclear. Effective management of supply chain risk therefore requires robust change management and procurement practices, clear governance arrangements and appropriate oversight of supplier systems throughout the lifecycle of digital assets.

RIS-0745-CCS provides safety assurance guidance to dutyholders when procuring high integrity software-based systems for railway applications.

Danish Rail Cyber Disruption (2022)

A cyber security incident affecting a subcontractor providing digital services to Danish rail operators resulted in the precautionary shutdown of driver operational systems. Without access to these systems, train services were suspended nationwide.

Although the core railway infrastructure was not directly compromised, the dependency on a third-party digital service created a single point of operational failure.

Learning: This incident demonstrates how digital risks can originate within the supply chain and directly impact railway operations. It highlights the importance of understanding supplier dependencies, maintaining visibility of third-party systems and ensuring that critical operational functions are resilient to external disruption.

Data integrity

Digital railway systems depend on reliable and accurate data. Many operational decisions rely on data from digital systems, including train positioning information, infrastructure monitoring systems and passenger information services. Errors in these data streams can cause systems to behave incorrectly or trigger inappropriate operational responses. Data governance, validation processes and robust data management practices therefore form a critical component of digital safety assurance.

Fail-safe and resilience risks

Fail-safe mechanisms are intended to prevent unsafe train movements and behaviours by placing systems into a safe state when faults occur. In digital systems, this may involve shutting down signalling systems, disabling train functions or preventing further operations until the issue is resolved. While these responses protect safety, they can also create operational disruption and

potentially result in falling back to a safe mode where a system may be more vulnerable. Large-scale system shutdowns may lead to passenger crowding, stranded trains or degraded operational performance. Balancing fail-safe protection with operational resilience therefore represents an important challenge for digital safety management. The national grid disturbance in 2019 illustrates this in practice.

National Grid Disturbance and Train Lockouts (2019)

A disturbance on the UK electricity grid triggered protective shutdown mechanisms across multiple electric train fleets. Onboard systems interpreted the disturbance as a critical fault and activated fail-safe lockout logic.

As a result, 31 trains were immobilised simultaneously, with many requiring manual technical intervention before services could resume. The event created widespread disruption and secondary safety risks associated with stranded passengers and degraded operations. Different fleets responded differently. In some cases drivers were able to reset the train, while in others updated software required technical intervention before the train could be returned to service.

Learning: This incident demonstrates how fail-safe mechanisms, while preventing unsafe conditions, can create system-wide operational impacts when applied uniformly. It highlights the need to balance fail-safe protection with operational recovery, and to assess the wider safety and resilience implications of software changes and configuration differences.

Malicious disruption risk

Cyber attacks or malicious interference may disrupt railway operations with potential safety consequences. While confirmed safety-critical cyber incidents remain rare, attacks on critical infrastructure sectors demonstrate that digital systems can be targeted for disruption. In many cases, organisations choose to shut down operational systems as a precaution when cyber incidents occur. This can result in the loss of the digital forensic chain, which is a problem for OT systems as this would result in the loss of logging information and ability to investigate the root cause.

The increasing connectivity of railway systems means that cyber resilience is an important element of digital safety management. Operators must consider not only accidental system failures but also the possibility of malicious interference. Maintaining secure digital infrastructure therefore contributes directly to safe railway operation.
Nevertheless, BCPs and/or DRPs, must take due account of loss of key digital systems and of how associated operational risks can be safely managed.

Cyber Attacks on UK Retail Infrastructure (2025)

Major UK retailers, including Marks & Spencer, Co-op and Harrods, were affected by ransomware-linked cyber attacks that led to the shutdown of digital systems to contain the intrusion. In several cases, services were suspended and systems required extensive recovery and rebuilding.

Although these incidents occurred outside the rail sector, they demonstrate how cyber attacks can rapidly remove system availability and force precautionary shutdown of critical digital services.

Learning: These incidents illustrate how malicious disruption can lead to loss of system availability and large-scale operational impact. They highlight the need for strong cyber resilience, effective incident response and an understanding that precautionary shutdown of digital systems may itself introduce safety and operational risks.

Sector maturity variability

Digital maturity varies significantly across the railway sector. Different sectors, including mainline rail, metro systems and light rail networks, operate with varying levels of digital capability and experience. Some organisations manage highly complex digital infrastructures, while others rely more heavily on traditional engineering systems. This variability affects how organisations manage digital safety risk. Some operators have well-developed digital engineering capabilities, while others are still developing the necessary skills and governance frameworks.

- ← Previous Digital safety
- → Next 3. Compliance Expectations

3. Compliance Expectations

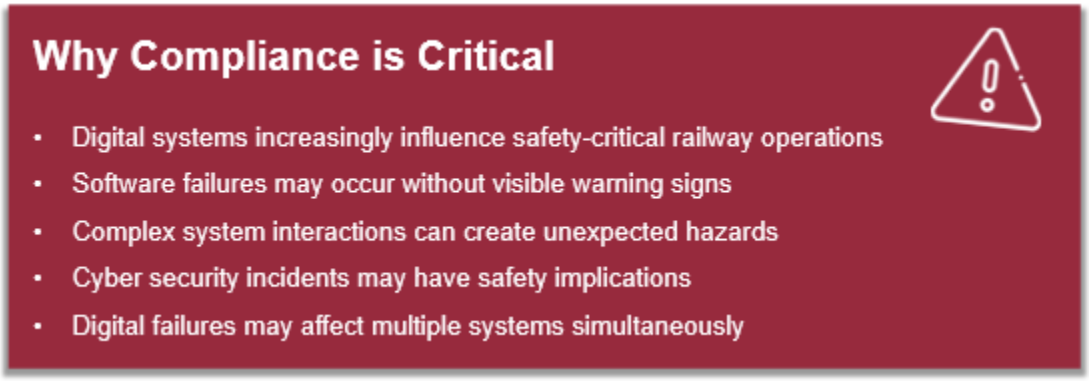
Why compliance matters

Digital technologies play a critical role in the safe operation of the railway system. Software-driven systems are used to control train movements, monitor infrastructure, manage operational decision-making and support maintenance activities. These systems can directly or indirectly influence the safety of passengers, staff and the public.

As reliance on digital systems increases, the potential safety consequences of digital failures also increase. Digital failures may arise from software defects, system misconfiguration, integration failures, cyber security incidents or weaknesses in operational governance. While many digital

failures result primarily in operational disruption, some may create conditions that could compromise safety if not properly controlled.

The regulatory framework governing railway safety does not distinguish between digital risks and other forms of safety risk. Dutyholders are required to manage the safety risks arising from digital systems in the same way as any other safety-critical hazard. Effective compliance therefore requires organisations to understand the role that digital systems play within their operations and to ensure that these systems are properly governed throughout their lifecycle.



The legal and regulatory basis

The management of digital safety risk is underpinned by existing health and safety legislation. These legal duties require dutyholders to manage risks arising from software based and digitally connected systems so far as is reasonably practicable. ORR expects dutyholders to manage digital safety risks as part of their Safety Management Systems (SMS) and to demonstrate that safety and security risks are controlled throughout the lifecycle of the system.

The principal legislation relevant to digital safety includes:

- Health and Safety at Work etc. Act 1974 (HSWA)
- Management of Health and Safety at Work Regulations 1999 (MHSW)
- Railways and Other Guided Transport Systems (Safety) Regulations 2006 (ROGS)
- Provision and Use of Work Equipment Regulations 1998 (PUWER)

Under sections 2, 3 and 4 of the Health and Safety at Work Act, dutyholders must take reasonably practicable measures to secure the health and safety of employees and others. This obligation applies equally to risks arising from digital systems. Moreover, section 6 of the Health and Safety at Work etc. Act 1974 places a duty on those who design, manufacture, import or supply equipment

for use at work to ensure that it can be used safely.

The Act defines an “article for use at work” (s53(1)) as (a) any plant designed for use or operation (whether exclusively or not) by persons at work, and (b) any article designed for use as a component in any such plant.

Within this context, rail assets such as rollingstock, signalling systems and electrification infrastructure are all captured within this definition where they are used by workers. The software on any equipment would fall into the definition as a component in any such plant.

The Management of Health and Safety at Work Regulations place a specific duty on organisations to conduct suitable and sufficient risk assessments and to implement appropriate control measures. Regulation 3 requires dutyholders to assess risks to health and safety, while Regulation 4 establishes the general principles of prevention, often referred to as the hierarchy of control.

ROGS requires railway operators and infrastructure managers to implement an SMS capable of controlling risks arising from the operation of the transport system. These requirements apply to all risks, including those associated with digital technologies.

Regulation 18 of PUWER sets out the requirements for control systems to ensure they are safe and that they do not impede the operation of any stop controls required by Regulations 15 & 16.

Together, these legislative requirements establish the expectation that risks arising from digital systems must be assessed, managed and controlled in the same way as any other railway safety risks.

The following resources provide guidance on the identification, assessment and management of digital safety risks:

- Common Safety Method for Risk Evaluation and Assessment
- BS EN 50126:2017: Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)

Cyber security and NIS regulations

The Department for Transport acts as the Competent Authority for the rail sector under the Network and Information Systems Regulations 2018 (NIS) Regulations, with responsibility for

identifying Operators of Essential Services, assessing compliance and taking enforcement action where required. While ORR does not regulate cyber security directly, cyber incidents may still create safety risks. In such cases, ORR will regulate the safety implications of digital system failures under health and safety legislation.

The NIS regulations were introduced to improve the security and resilience of essential services and critical digital infrastructure across the UK. They apply to two principal groups:

- Operators of Essential Services (OES) – organisations providing services essential to societal and economic activity
- Relevant Digital Service Providers – including cloud computing services and online platforms.

Under the NIS Regulations, operators of essential services must:

- take appropriate technical and organisational measures to manage cyber security risks
- prevent and minimise the impact of incidents affecting network and information systems
- report incidents that significantly affect the continuity of essential services.

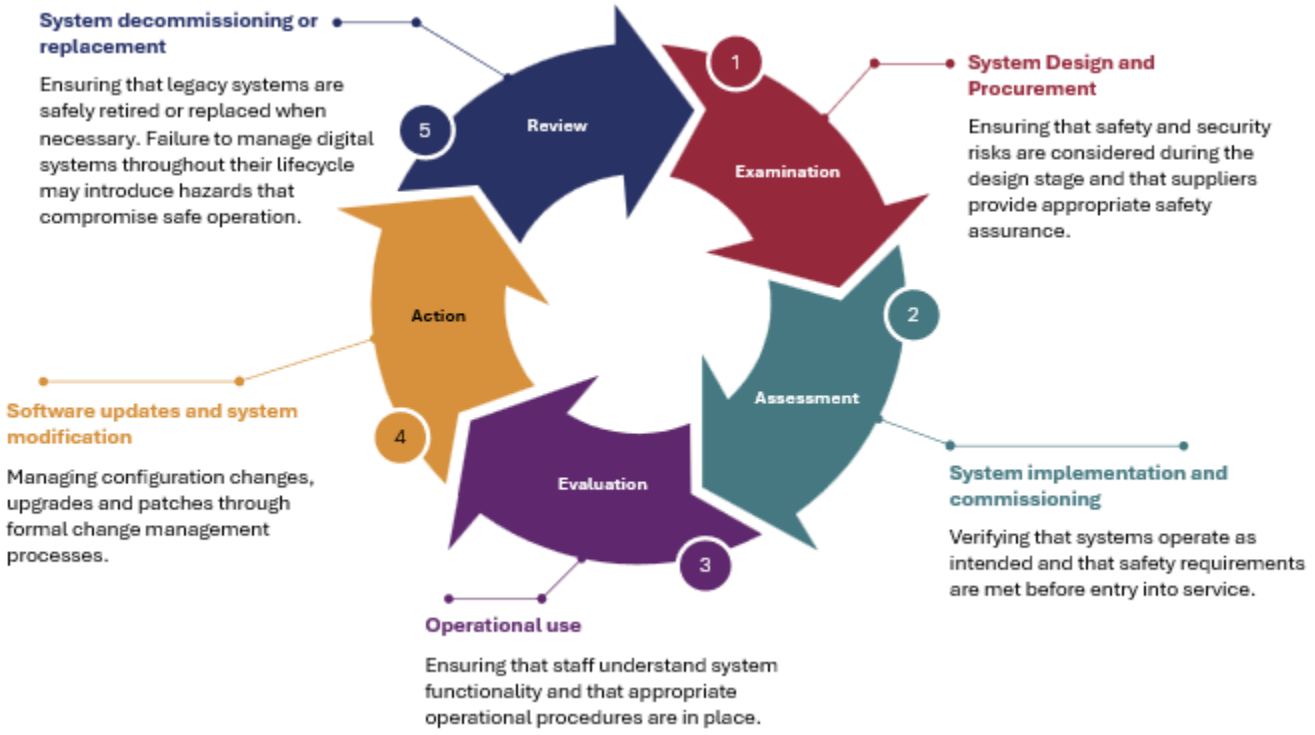
The Cyber Security and Resilience Bill (CSRB) currently going through parliament will strengthen and modernise the UK cyber resilience framework, by reforming and adding to the existing NIS regulations, including the designation of critical suppliers.

The following resources provide guidance on the identification, assessment and management of cybersecurity risks associated with Digital Systems:

- The Cyber Assessment Framework (CAF), developed by the National Cyber Security Centre (NCSC) is a tool that can be used to help organisations assess and improve their cybersecurity and resilience.
- The emerging IEC 63452 standard (Railway applications - Cybersecurity) provides cybersecurity requirements and guidance for all stages of the Digital System lifecycle.
- IET Code of Practice, Cyber Security and Safety is intended to support understanding of the issues involved in ensuring that an organisation's safety responsibilities are addressed in the presence of a threat of cyber-attack.

When compliance must be demonstrated

Compliance with digital safety obligations must be demonstrated throughout the entire lifecycle of a digital system. As another form of health and safety risk, digital safety risk must be managed through a dutyholder's SMS in the same way as other safety risk, in compliance with relevant health and safety legislation. Digital systems typically evolve through multiple stages, including design, development, procurement, installation, operation and modification. Each of these stages may introduce new safety risks if not properly managed. Dutyholders should demonstrate that digital safety risks are mitigated at each stage of the system lifecycle, as shown below.



ORR's expectations of dutyholders

ORR expects dutyholders to demonstrate that digital safety risks are properly identified, assessed and controlled within their SMS. This requires effective governance, appropriate technical competence and robust assurance processes to manage digital systems safely. Independent assurance should be employed for significant change, through use of Assessment Bodies (AsBos), independent safety assessment (ISA) and/or Independent Competent Persons (ICP) as appropriate.

In particular, dutyholders should be able to demonstrate that they:

- Maintain a clear understanding of where digital systems are used across their operations, including software that may be used in safety-critical contexts without being originally designed for that purpose;
- Treat all unexpected software behaviours as potential safety issues, identifying underlying causes and recognised risks associated with safety-critical defects are addressed;
- Demonstrate that operational mitigations or workarounds do not mask underlying safety defects or become a substitute for resolving system issues;
- Communicate and transfer safety risks between organisations, including suppliers and partners, with clear understanding of hazards, mitigations and responsibilities; and
- Define and maintain clear roles, responsibilities and ownership of digital systems and associated risks so that accountability remains visible and effective throughout the system lifecycle.

Dutyholder checklist:

- ← Previous 2. Our view of the risk
- → Next 4. Continuous Improvement

4. Continuous Improvement

Continuous Improvement in Digital Safety

Digital safety is a rapidly evolving area. Technologies, operational practices and risks are continually changing, and the railway sector must adapt accordingly. Unlike traditional railway systems, digital systems evolve throughout their operational life through software updates, configuration changes and integration with new technologies. This means that managing digital safety is not a one-off activity undertaken during system introduction. Instead, it requires continuous monitoring, learning and improvement.

Whilst dutyholders own any safety risk, continuous improvement requires coordinated action from both dutyholders and industry to strengthen the sector's ability to manage digital safety risks.

Industry Responsibilities for Continuous Improvement

Dutyholders are responsible for ensuring that digital safety risks are effectively managed within their organisations. Continuous improvement requires organisations to strengthen governance, develop technical capability and improve visibility of digital system performance.

Key areas for improvement include the following:

Preparing for emerging digital technologies

The railway sector is beginning to adopt a range of emerging digital technologies, including artificial intelligence, robotics and increasingly autonomous systems. While these technologies offer significant opportunities to improve operational efficiency and asset management, they also

introduce new safety challenges. A primary safety challenge associated with emerging digital technologies is not the technology itself, but how it is integrated into operational systems and decision-making processes.

Artificial Intelligence

Artificial intelligence is increasingly being explored for applications such as predictive maintenance, infrastructure inspection and decision support. ORR's expectation is that risks arising from AI should be managed in the same way as any other health and safety risk. The use of AI does not remove or change existing legal duties. Where AI affects health and safety, dutyholders must assess the risks it creates, undertake a suitable risk assessment and put appropriate controls in place so far as is reasonably practicable, including where relevant the management of cyber security threats. This approach is consistent with HSE's regulatory approach to AI.

A key safety challenge associated with AI lies in understanding how it changes system behaviour and decision-making processes. Unlike conventional software systems, AI-based systems may exhibit forms of autonomy or adaptive behaviour that are less predictable than traditional deterministic algorithms. It may not always be clear how an AI system has arrived at a particular output or decision. This requires careful consideration of where and how the technology is applied, particularly in safety-relevant contexts.

Furthermore, it is important to focus on the system-level impact of AI deployment, rather than attempting to assess AI in isolation. Key considerations include:

- clearly defining the role of AI within the operational system,
- understanding how human operators interact with automated outputs,
- ensuring that system changes introduced by AI are properly assessed under existing safety frameworks,
- ensuring that appropriate controls are in place to manage risks arising from data quality, system behaviour and cyber security.

Future technologies

Robotic technologies are increasingly being considered for activities such as infrastructure inspection and asset monitoring. However, many existing railway standards and operational rules were developed for human-operated equipment. This can create regulatory and operational

challenges when deploying autonomous technologies. Ensuring that emerging technologies can be safely integrated into railway operations will require continued collaboration between industry bodies, regulators and technology developers.

Other emerging technologies, including quantum computing and advanced sensing technologies, may also influence railway operations in the future. While these technologies are currently at an early stage of development, the sector must continue to monitor technological developments and assess their potential implications for safety.

ORR's role in supporting continuous improvement

ORR's role is to engage and challenge, where appropriate, the rail sector's capability to manage digital safety risks while holding dutyholders to account under existing health and safety legislation. ORR will support continuous improvement through capability development, targeted assurance, sector-wide collaboration and promoting learning. Effective engagement across different sectors will foster cross-sector learning as these technologies develop.

Building capability and understanding

ORR will continue to develop its internal capability to regulate digital systems effectively. This includes:

- strengthening inspector competence in software lifecycle governance, digital system assurance and cyber-related risks,
- refining inspection tools and approaches based on practical experience,
- building sufficient technical skills to deliver effective, informed, insightful and balanced inspections to address the need for ensuring consistent and proportional inspections.
- incorporating lessons from inspections and investigations into ongoing training and capability development.

Targeted assurance and inspections

ORR will undertake targeted inspections to assess how dutyholders manage digital safety risks in practice. This will focus on:

- software lifecycle and change management,
- safety assurance of digital systems,

- supply chain oversight and client-side assurance,
- integration of digital risks within Safety Management Systems

Inspection findings will be used to identify good practice, highlight areas for improvement and inform future regulatory expectations.

Industry engagement and system-level oversight

ORR will maintain active engagement with industry bodies and government stakeholders to support a coordinated approach to digital safety. This includes collaboration with:

- Department for Transport
- National Cyber Security Centre
- RSSB, RDG and LRSSB
- RAIB and other regulators
- International Bodies, including European Union Agency for Railways (ERA)

ORR will also assess how dutyholders manage digital risks across the system lifecycle, including procurement, design, change management and supply chain arrangements.

Driving sector learning and improvement

ORR will promote structured learning across the sector by:

- encouraging improved reporting and sharing of digital and cyber-related incidents
- using inspection and investigation findings to inform regulatory focus
- promoting the use of common language and terminology within and between stakeholders
- supporting industry efforts to improve digital safety maturity

As the evidence base develops, ORR will refine its approach to drive continuous improvement in digital safety management.

Enforcement

Where dutyholders fail to adequately identify, assess or control digital safety risks, ORR will take proportionate enforcement action in accordance with the ORR enforcement policy statement.

- ← Previous 3. Compliance Expectations
- → Next 5. Appendix

5. Appendix

Useful resources

- RIS/0745-CCS Iss 1, Client Safety Assurance of High Integrity Software-Based Systems for Railway Applications
- BS EN 50126:2017: Railway Applications - The Specification and Demonstration of Reliability, Availability, Maintainability and Safety (RAMS)
- BS EN 50716:2023: Railway Applications — Requirements for software development
- Common Safety Method for Risk Evaluation and Assessment (CSM-RA)
- IET Code of Practice, Cyber Security and Safety
- Risk Management Maturity Model (RM3)
- National Cyber Security Centre Cyber Assessment Framework (CAF)
- IEC 63452, Railway applications - Cybersecurity

Glossary of terms

Acronym or abbreviation	Full name
4LM	Four Lines Modernisation
AI	Artificial Intelligence
AsBo	Assessment Body

Acronym or abbreviation	Full name
ATO	Automatic Train Operation
BCP	Business Continuity Plan
CAF	Cyber Assessment Framework
CSM-RA	Common Safety Method for Risk Evaluation and Assessment
DRP	Disaster Recovery Plan
ERTMS	European Rail Traffic Management System
HSWA	Health and Safety at Work Act
ICP	Independent Competent Persons
ISA	Independent Safety Assessment
LRSSB	Light Rail Safety and Standards Board

Acronym or abbreviation	Full name
MHSW	Management of Health and Safety at Work Regulations 1999
NCSC	National Cyber Security Centre
NIS	Network and Information Systems Regulations 2018
OES	Operators of Essential Services
OT	Operational Technology
PUWER	Provision and Use of Work Equipment Regulations 1998
RAIB	Rail Accident Investigation Branch
RAMS	Reliability, Availability, Maintainability and Safety
RDG	Rail Delivery Group
RM3	Risk Management Maturity Model

Acronym or abbreviation	Full name
ROGS	Railways and Other Guided Transport Systems (Safety) Regulations 2006
RSSB	Rail Safety and Standards Board
SMS	Safety Management System
TSR	Temporary Speed Restriction

- ← Previous 4. Continuous Improvement
- → Next 2. Our view of the risk