Digital safety

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.

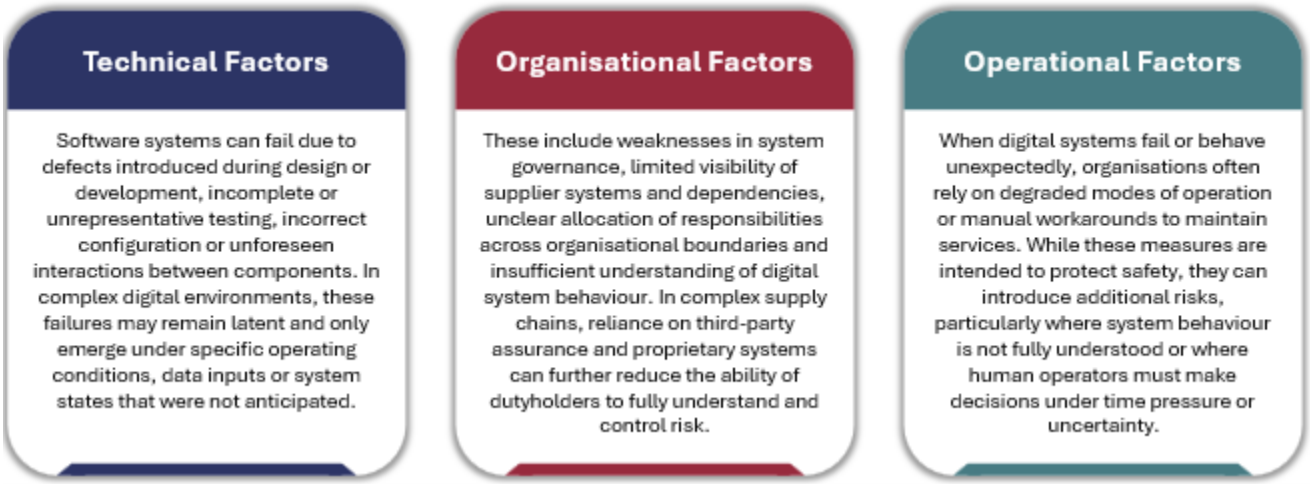
Infrastructure managers and operators are also exposed to system-level risks where digital failures affect signalling systems, train control systems, communications networks or asset monitoring systems.

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