



ORR digital safety strategy

Our digital safety strategy sets out our vision and approach for improving the management of health and safety risks arising from digital systems.

Why digital safety matters

The rail industry depends on complex, software-driven and digitally connected systems, which includes both conventional Information Technology (IT) systems and Operational Technology (OT). These systems influence, and in some cases control, safety-critical functions across rolling stock, signalling, infrastructure, communications and operations. This brings a need for clear understanding, robust governance and effective control of the health, safety and security risks they introduce. The following themes summarise the principal digital safety issues facing the rail sector. More detail is provided in the Digital safety strategic risk chapter.

Digital failures differ from electro-mechanical failures

Software may have hidden defects and can fail in sudden or unexpected ways. Furthermore, the complexity of digital systems, and the interactions between them, make failure modes difficult to predict and require different workforce capabilities (when compared with more traditional electro-mechanical systems) to design, maintain and to investigate and resolve failures.

Poorly controlled change is a primary trigger

Digital safety incidents are often linked to weak handovers between the manufacturer owner and operator, software updates, configuration changes, or modification without adequate reassessment.

Interface and integration risk

Risk often concentrates at interfaces between systems, organisations and technologies, particularly where legacy and new systems interact.

Autonomy and automation shift risk boundaries

Increased use of automation and artificial intelligence (AI) changes traditional decision-making processes and human roles. Where system logic (a set of rules and decisions that tell a system what to do and when to do it) is not transparent or repeatable, risks may be harder to understand and control. Therefore, digital change must be clearly defined and assessed at the system level.

Supply chain and third-party dependency

Risks may originate beyond the dutyholder purview, including within complex global supply chains.

Data integrity

Safe operation depends on reliable data. Corrupted, incomplete or misinterpreted data can undermine system behaviour. Comprehensive and secure system logging is key to enable effective incident investigation and facilitate timely identification of abnormal system behaviours.

Fail-safe and resilience risks

Fail-safe mechanisms protect safety but can compromise operational resilience. Risks include common-mode shutdown, reduced performance during manual fallback, increased human error under degraded operation and slow or complex recovery procedures.

Malicious disruption risk

Cyber or malicious interference may create operational disruption with potential safety consequences.

Industry maturity variability

Maturity in the management of digital safety risks varies across the rail industry, including mainline, metro and light rail operations. Oversight and expectations must remain proportionate to system complexity, autonomy and risk exposure.

- → Next ORR digital safety vision