

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.

ORR's Vision



ORR's vision is that:

- digital risks are fully integrated within dutyholder's Safety Management Systems (SMS)
- the railway industry delivers continuous improvement in the management of health and safety risks arising from digital systems, in the same way as any other risk
- future digital safety and security risks are considered at the design stage to eliminate or reduce risk at the outset wherever possible

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