Digital safety

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