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

ORR digital safety vision

1. 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 health, safety and security risks are considered at the design stage to eliminate or reduce risk at the outset wherever possible. Refer to the Health and safety by design strategic risk chapter (SRC) for more information.

2. ORR's role is to ensure that health and safety risks arising from digital systems are identified, assessed and controlled so far as is reasonably practicable.

- ← Previous ORR digital safety strategy
- → Next Regulatory aims and expected outcomes

Regulatory aims and expected outcomes

3. To deliver this vision, ORR will focus on strengthening dutyholder's identification and mitigation of digital safety risks across the system lifecycle, from design through to operation, change, renewal, decommissioning and disposal.

4. Our regulatory aims are to:

- Strengthen lifecycle governance of software and digital systems;
- Improve cooperation between digital safety and security disciplines;
- Enhance awareness of, and industry competence in managing, digital risk;
- Promote learning from digital safety incidents and application of health and safety by design; and,
- Improve digital resilience and recovery capability.

5. Dutyholders should be able to demonstrate they comply with the law by:

- Effective governance and accountability for digital systems and digital asset management;

- Effective management of the software lifecycle and digital change;
- Robust supply chain and procurement assurance;
- Application of digital safety and security by design;
- Threat-informed risk assessment and proportionate risk control;
- Effective management of human factors and autonomy;
- Recording and investigation of incidents, promoting continuous improvement; and,
- Sufficient management maturity, consistent with Risk Management Maturity Model (RM3) principles, to manage and continuously improve digital safety risk.

- ← Previous ORR digital safety vision
- → Next Legal context

Legal context

6. Dutyholders must manage health and safety risks arising from software-based and digitally connected systems so far as is reasonably practicable.

7. Under the Health and Safety at Work etc. Act 1974, the Management of Health and Safety at Work Regulations 1999 and the Railways and Other Guided Transport Systems (Safety) Regulations 2006 (ROGS) [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)], digital risks (including the use of Artificial Intelligence and cyber-related safety risks) must be identified, assessed and controlled within a suitable and sufficient SMS, throughout the life cycle of the system.

8. Section 6 of the Health and Safety at Work etc. Act 1974 also imposes duties on anyone who designs, manufactures, imports or supplies an article, for use at work, to ensure that can be used safely. An "article for use at work" is defined in s53(1) of the Health and Safety at Work Act 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.

9. The Network and Information Systems Regulations 2018 (NIS) imposes duties on Operators of Essential Services to take appropriate measures to prevent and minimise incidents affecting their systems, for which the Department for Transport (DfT) is the Competent Authority. DfT has sole authority and responsibility for regulatory decisions under the NIS regime. Where cyber security failures create health and safety risk, ORR will regulate those risks under health and safety law.

- ← Previous Regulatory aims and expected outcomes
- → Next ORR activity and industry leadership

ORR activity and industry leadership

10. ORR's regulatory focus is to strengthen the rail sector's maturity while holding dutyholders to account under existing health and safety legislation.

Developing competence

11. ORR has:

- Delivered specialist training to inspectors on cyber security and digital systems;
- Developed a question set to support scrutiny of digital safety arrangements by our inspectors; and,
- Undertaken initial inspections to test and refine our approach.

12. We will continue to develop inspector competency in software lifecycle governance, digital system assurance and investigation of digital failures. Lessons learned from inspections and investigations will be incorporated into ongoing training and capability development.

Targeted inspection and assurance

13. ORR will continue to undertake targeted inspections across the industry to develop our understanding of industry maturity and risk control arrangements. This includes examining:

- Management of software design, development, verification and validation processes;
- Change management and configuration control processes;
- Safety assurance arrangements for software-based systems;
- Cooperation between safety and security disciplines;
- Supply chain assurance and client-side oversight; and,
- How digital risks are incorporated within SMS.

14. Where concerns arise, we will use inspection findings to inform our future regulatory priorities and shape our industry expectations. If we identify that dutyholders are not complying with the

law, we can take enforcement action to ensure that passengers, the public and the workforce are protected.

Risk profiling and evidence-based prioritisation

15. ORR's Railway Safety Directorate (RSD) conducts an annual risk profiling exercise to assess industry performance across key health and safety hazards. This informs ORR's future regulatory priorities.

16. ORR will continue to assess and quantify the level of risk posed to the industry by digital systems, with software and cyber security-related risks expected to remain an ongoing area of focus. ORR uses the risk profiling outputs, alongside inspection and investigation evidence, to determine where regulatory effort should be focused to address digital safety risk.

Engagement and cross-sector collaboration

17. ORR recognises that effective digital safety oversight requires collaboration and sharing learning from across the whole rail industry, other transport modes and relevant industries, both in Great Britain and internationally.

18. In particular, ORR supports a collaborative approach, and we will promote shared learning in our engagement with the stakeholders below:

- Individual dutyholders;
- Department for Transport (as NIS Competent Authority);
- National Cyber Security Centre (NCSC);
- Rail Safety and Standards Board (RSSB);
- Rail Delivery Group (RDG);
- Light Rail Safety and Standards Board (LRSSB);
- Rail Accident Investigation Branch (RAIB);
- Other domestic and international regulators and bodies.

19. We will maintain proactive engagement with the DfT's cyber compliance and policy teams to ensure a coordinated approach where cyber security failures may create health and safety consequences, while respecting respective regulatory roles.

Supply chain and system-level oversight

20. Digital safety risks extend across the supply chain and throughout the system lifecycle.

21. ORR will assess whether:

- Dutyholders attain, and retain, sufficient technical understanding of the digital systems they operate;
- Robust assurance processes are in place for software and equipment procurement;
- Change management arrangements are effective; and,
- Safety and security considerations are addressed at the design stage.

22. We recognise the challenges posed by complex supply chains. However, dutyholders remain responsible for ensuring that digital safety risks are controlled, so far as is reasonably practicable.

Promoting industry learning and continuous improvement

23. Effective digital safety management depends on structured learning. ORR will:

- Promote improved recording and sharing of software and cyber-related incidents;
- Encourage learning from digital failures and near misses across the rail industry, including internationally; and,
- Use inspection and investigation findings to refine our regulatory approach.

24. As our evidence base develops, we will target our regulatory effort to where it will have the greatest impact.

Enforcement

25. The management of health and safety is a fundamental legal requirement. Where evidence demonstrates that digital safety risks are not being adequately identified, assessed or controlled, ORR will take proportionate enforcement action in accordance with the ORR enforcement policy statement.

- ← Previous Legal context
- → Next Continuous improvement

Continuous improvement

26. As digital technologies evolve, dutyholders must:

- Continually review their digital risk exposure;
- Share learning from incidents and near-misses;
- Strengthen and maintain digital competence across technical and safety disciplines; and,
- Improve resilience and recovery planning;
- Embed digital safety risk management throughout the supply chain and the life of the system;
- Ensure effective assurance processes and governance arrangements are in place to control these risks; and,
- Embed security and safety by design into new systems.

27. ORR will continue to use a combination of proactive inspection, investigation, stakeholder engagement and regulatory intervention where necessary to support continuous improvement in digital safety management across the rail industry.

- ← Previous ORR activity and industry leadership

- ← Previous Legal context
- → Next Continuous improvement