

ORR digital safety strategy

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