

Health and safety by design

2. Our view of the risk

What the risk is and who it affects

Health and safety by design is the elimination, reduction or control of health and safety risks by considering those risks at the design stage. Poor planning of new or modified works can fail to take simple steps to avoid future hazards to passengers and workers.

If the impact of a change on the whole railway system throughout the lifecycle is not considered early, risks may be designed in and require ongoing operational controls. These risks affect those constructing, operating, maintaining and using the railway.

A failure to identify and address risks early increases the likelihood of incidents and ill health, introduces unnecessary hazards, and results in systems and equipment that are more costly and less efficient to use, maintain or operate safely.

The Challenges

- Restrictive client briefs limiting flexibility
- Designers restricted by limited time or budget
- Insufficient briefing on intended uses and users
- Risk-averse approaches leading to “more of the same”
- Optioneering done merely to justify decisions already made



Risk drivers and long-term exposures

Decisions made at the earliest stages of a project can significantly influence safety outcomes across design, construction, operation, maintenance and de-commissioning. Risk management is iterative and begins at concept stage.

As design evolves, each option should be examined in increasing detail with the goal of identifying and eliminating hazards from the outset. If these opportunities are missed, hazards may persist for the whole life of infrastructure or equipment.

Cost, efficiency and performance risks

Early-stage decisions can overlook long-term safety and cost benefits. Applying health and safety by design principles leads to more effective, efficient and sustainable safety outcomes over the life of the project.

Designing out a hazard early can remove the ongoing cost of managing that hazard over the operational life of the system, infrastructure, equipment or rolling stock.

Systems that are designed to be simple to use and maintain are less costly to operate by lowering maintenance requirements. Systems can also be designed to learn over time, helping operations become more efficient.

Every incident or injury represents lost time, delays and additional costs and the potential for civil claims or enforcement action. Better planning, design and construction and manufacturing work to take advantage of newer methods and technologies can reduce exposure to health and safety risks.

System-wide and human factors risks

Health and safety by design requires taking a holistic view of how activities and projects interact. Disparate design decisions can combine to increase risk if systems interactions are not understood and planned for.

Risks can arise where designers lack sufficient briefing on potential uses and users of the systems they are planning, leading to incorrect assumptions and new risks being created.

Case Study: Common Railway Examples



Ongoing Issues

- Poor worker safety designs in depot layouts
- Poor user engagement and understanding of depot requirements leading to no continuous safe walking routes
- Insufficient clearance from live conductors

Changes Required

- New additional walking routes, resurfacing and protection from conductor rails in place

Cyber security and software risks

Cyber security is increasingly important for protecting digital systems and ensuring they are not tampered with. Risk arises if cyber security issues are not addressed in specification, design and purchasing.

Problems with technology and computer systems may also arise from poor planning, design, configuration or maintenance rather than hostile attacks. Clear requirements, simple logic, fail safe behaviour, human centred interfaces, controlled change, and whole life safety thinking are essential to reducing reliance on people, procedures, and supervision.

Software Risks



- Poor data quality
- Legacy systems and software leading to compatibility and interface issues
- Poor specification of functionality and behaviours
- Human-factors shortcomings in critical interfaces
- Need for structured, traceable change and validation

ORR's perspective on the risk

ORR wants industry to move from learning only after incidents occur to proactively identifying and designing out potential issues before they arise.

Where Health and safety by design is not applied, hazards may be embedded in systems or designs, requiring compensatory controls and increasing long-term risk, ill health, incidents and operational costs.

- ← Previous Health and safety by design
- → Next 3. Compliance expectations