

# Health and safety by design

## 1. Executive summary

Health and safety by design (HSbD) is the elimination or control of health and safety risks in infrastructure, equipment, products or processes by early consideration and dealing with those potential risks at the design stage. While this principle is simple, and offers numerous benefits, too often we find the planning of new works or modifications has failed to take simple steps to avoid hazards to the health and safety of passengers and workers.

It requires those planning new or modified works to consider, at the earliest stages, what the impact of the change will be on the whole railway system throughout its lifecycle. They should design out issues, or where elimination is not reasonably practicable, ensure that residual risks are capable of effective control and communicated to those who will manage them.

Better planning, consistent application of appropriate standards and early engagement with operators and users can avoid future hazards, reduce late design changes, and drive down levels of ill health, incidents and accidents. Good design can also improve functionality, productivity and cost-effectiveness by reducing the need for costly changes later.

Health and safety by design is not a new approach; Britain's railway safety systems are built on nearly 200 years of learning from incidents. ORR wants the industry to move from learning only after incidents occur to proactively identifying and designing out potential issues before they arise.

Everyone planning new work or changes to existing systems should consider how good design can make their systems inherently safer for passengers, employees and the public, and with less risk to health. In particular, ORR's Vision includes:

### Design leadership



- Industry ownership of HSbD as part of routine business management
- Early and routine application of HSbD to renewal, enhancement and new-build projects

### Risk assessment and decision-making



- Review of risk assessments and controls to inform design decisions
- Updating guidance and standards where necessary
- Using CSM-RA or other credible methods
- Considering reasonably practicable H&S enhancements, including impact of residual risk their introduction could pose
- Reviewing how similar risks are controlled in other sectors
- Recording the optioneering process, including realistic costs and benefits

### Systems view and lifecycle integration



- Taking a holistic view of how different activities and projects interact
- Ensuring HSbD decisions are delivered by the project
- Integrating enhanced controls into equipment, systems and operations
- Reviewing performance after implementation

### Human factors and user involvement



- Iterative human-factors consideration throughout the design and development process
- Active participation of end users, including operators and maintainers

ORR expects designers, clients, manufacturers, contractors and others involved in planning or changing systems to apply health and safety by design consistently across all parts of the railway, including high-speed rail, mainline, metro, light rail, innovative systems and heritage operations.

- → Next 2. Our view of the risk

## 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

## 3. Compliance expectations

### Why compliance matters

Health and safety by design is required by several areas of legislation and must be applied from the earliest stages of planning and design. It is essential for preventing foreseeable risks, improving functionality and reducing the need for costly changes later.

Many of the compliance expectations exist because long-standing challenges continue to restrict good design practice, including restrictive client briefs, insufficient briefing on intended uses, time

and budget limitations, and a tendency to repeat existing solutions rather than consider safer alternatives.

Compliance with health and safety by design is increasingly important as the industry faces new forms of risk, including the growing dependence on digital systems and the need to address cyber security at the design stage.

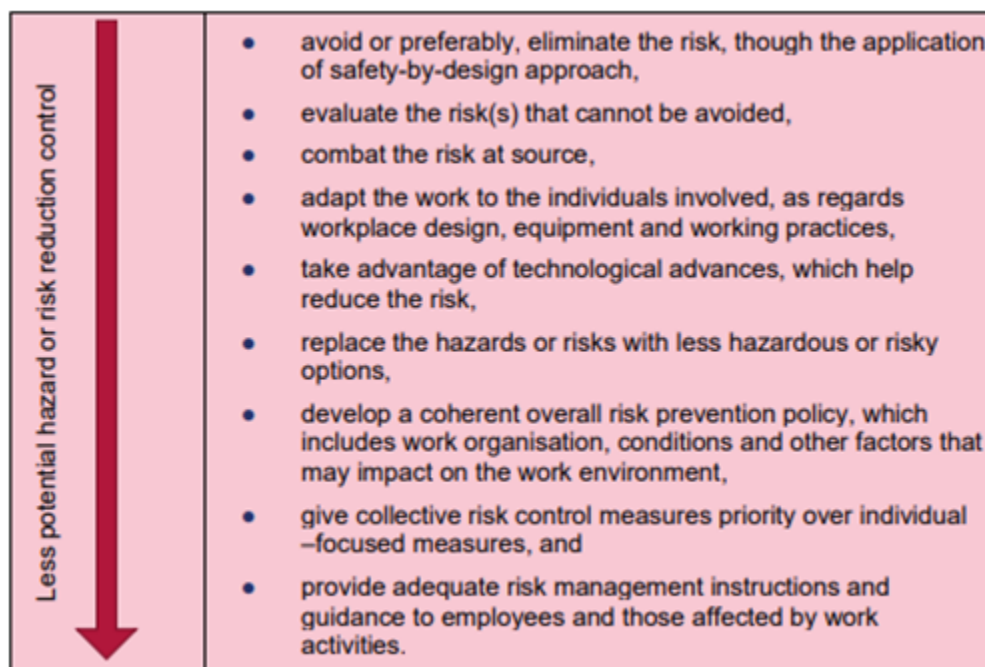
## Legal requirements for health and safety by design

Health and safety by design is covered in several areas of health and safety legislation:

- Health and Safety at Work etc. Act 1974 (HSWA)
- Management of Health and Safety at Work Regulations 1999 (MHSW)
- Construction (Design and Management) Regulations 2015 (CDM)
- Railways and Other Guided Transport Systems Regulations 2006 (ROGS)

MHSW requires suitable and sufficient risk assessment and application of the hierarchy of risk control, including the preference for elimination of risk, combat at source and intrinsic safety.

## Hierarchy of risk control – based on MHSW



CDM requires risks to be eliminated or controlled from the concept stage onward, including during

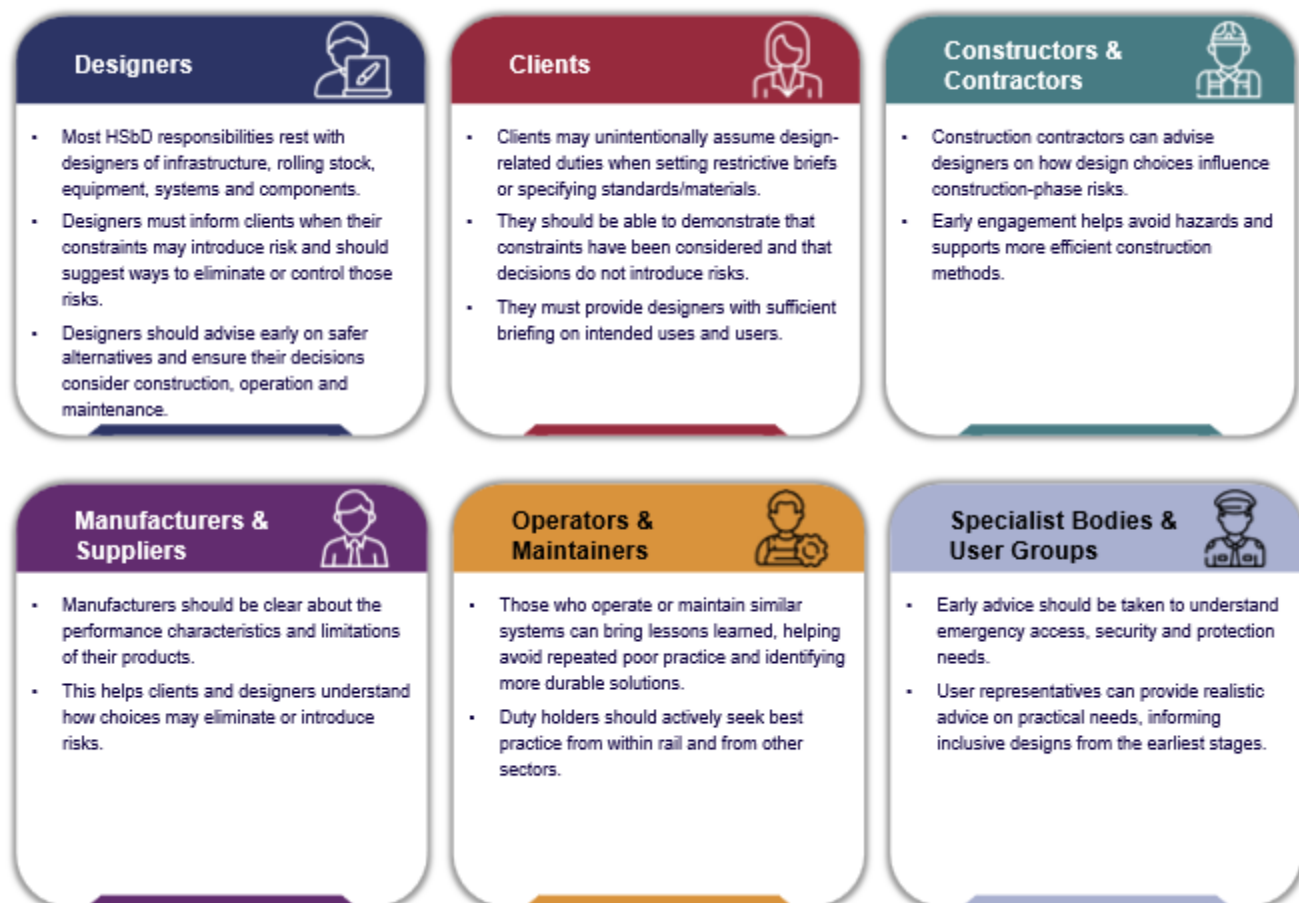
feasibility studies, and requires designers to consider risks to those constructing, operating and maintaining structures. Note that ORR has an agency agreement with the Health and Safety Executive (HSE) on the enforcement of health and safety by design in respect of railways and other guided transport systems, giving ORR an enforcement role from the earliest stages of a project.

ROGS requires use of CSM-RA for significant changes, and requires cooperation between dutyholders on shared risks and interfaces. This covers both basic design compatibility, such as between train and platforms, as well as operational issues, for example ensuring stations are designed with ventilation to ensure operators staff are not exposed to Diesel Engine Exhaust Emissions (DEEE).

More information on 'The Law' is provided in the Appendix.

## ORR's expectations of dutyholders

ORR has established the following priorities grouped by dutyholder role:



# ORR oversight, supervision and enforcement

Under RM3, ORR examines health and safety by design issues under OC5, PI1 and RCS3. Inspectors will continue to challenge dutyholders to show that change is managed proactively using good practice and relevant standards.

ORR's Principles for health and safety on the railway set out minimum design and operational principles.

ORR allocates resources to influence major schemes where no existing dutyholder is in place, such as HS2.

Dutyholders must have design assurance procedures that ensure standards are met, deviations are controlled, and delivered assets match approved designs.

In permissioning functions, ORR will seek evidence that health and safety by design has been applied.

## What ORR expects to see as good practice

Dutyholders should demonstrate:



## Forums, opportunities and success stories

Access relevant forums.

- ← Previous 2. Our view of the risk
- → Next 4. Continuous improvement

## 4. Continuous improvement

### Applying health and safety by design throughout the design process

Health and safety by design should begin at the earliest stages of a project and continue as design choices are made. Designers should regularly evaluate the impact of their decisions across the lifecycle of the works, including construction, operation, maintenance and de-commissioning.

Early decision-making is critical. Safety considerations should be integrated during the initial exploration of options and then examined in progressively greater detail as the design develops, with the aim of identifying and eliminating hazards wherever possible.

Continuous improvement in health and safety by design requires that design decisions are delivered by the project, integrated into equipment, systems and operations, and reviewed after implementation to confirm they are functioning as intended.



## Improving safety, cost and efficiency outcomes

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

Designing out hazards early removes the ongoing cost of managing those hazards and reduces the need for operational controls throughout the asset's life.

Infrastructure, equipment and systems that are simpler to use and maintain are less costly to operate, because of reduced maintenance requirements and lower staffing needs.

Injuries and ill-health create lost time, delays and additional costs, including civil claims or criminal investigations. Better planning of construction and manufacturing work reduces exposure to these risks.

## Strengthening assurance and design processes

Dutyholders should ensure that design standards and procedures that address health and safety by design are consistently applied, with arrangements in place to challenge deviations and verify

that delivered assets match approved designs.

Design assurance should check that industry and company standards are complied with, that deviations are authorised through robust challenge processes, and that changes are fully documented.

Stage-gate processes should include health and safety criteria so risks and assumptions are properly assessed before progressing a design. This reflects the RIBA Plan of Work approach to change control.



## Enhancing risk assessment, human factors and option selection

Dutyholders should monitor safety trends and use learning from incidents and other dutyholders to update guidance and standards.

Proposed designs should take a holistic view of the railway as a system, considering interactions with existing assets and, where relevant, with systems beyond the railway.

Dutyholders should use consistent, proportionate risk assessment, and where relevant apply the Common Safety Method for Risk Assessment (CSM-RA).

Reasonably practicable opportunities to improve conditions should be taken, such as improving platform conditions beyond basic resurfacing.

Recognised human-factors methods should be used to address risks linked to equipment, tasks,

systems and the working environment, including consideration of foreseeable misuse.

Dutyholders should show they have explored a range of reasonably practicable options, identifying the safest overall solution for the whole lifecycle.

Organisations with large programmes of work should use proactive performance indicators to measure how well their design processes function.

BIM and digital modelling should be used to document health and safety by design issues throughout the design and life of assets and ensure this information is used to support risk management.

## Preparing for future change: digital, software and cyber security

Dutyholders must address cyber security issues in the specification, design and purchasing of equipment and systems, using guidance from the Department for Transport and National Cyber Security Centre.

Software risks often arise from poor configuration, planning, version control and maintenance. Continuous improvement requires clear functional specifications for normal, abnormal and emergency conditions.

Design should take account of human-system interfaces, ensuring usability and comprehension, especially where systems support emergency situations and degraded working.

Modification and change of software must follow a structured, planned process, including verification and validation before release and documented traceability.

Standards such as EN 50716:2023 and ISO 9001 / 90003 should be used for software safety and quality assurance.

## Improving Software Safety Over Time



- Strengthen specification and configuration
- Ensure clear version control
- Validate behavioral outcomes
- Address human-factors issues
- Apply EN 50716:2023 and ISO 9001/90003 where relevant

## Recommended resources and industry learning

Dutyholders should draw on relevant resources, including:

- ORR Principles for Health and Safety on the Railway (design and operational principles)
- Safety Verification guidance (non-mainline)
- RSSB resources (Taking Safe Decisions, health-by-design materials, human-factors guidance)
- HSE and CITB CDM resources
- CPNI and NCSC guidance on security and system design

Dutyholders should participate in forums and learning networks such as the HS2 Learning Legacy, Crossrail Learning Legacy and inclusive design/user engagement groups.

- ← Previous 3. Compliance expectations
- → Next 5. Appendix

## 5. Appendix

### Useful sources of information

- Network Rail Safety Central: Prevention through engineering and design
- HSE: The Construction (Design and Management) Regulations 2015
- HSE: Managing construction health risks
- HSE: Costs to Great Britain of workplace injuries and new cases of work-related ill health – 2023 to 2024
- CITB: Strengthening construction through collaboration

- RSSB: The cost benefits of health and wellbeing
- RSSB: Better practice in health by design
- RSSB: Taking safe decisions
- RSSB: Human factors guidance
- ORR: Safety verification guidance
- National Protective Security Authority
- Secured by Design
- The National Cyber Security Centre
- ANSI/ASSP Z590.3-2021: Prevention through Design Guidelines for Addressing Occupational Hazards and Risks in Design and Redesign Processes
- Safe Work Australia: Safe design
- Crossrail Learning Legacy: Healthy by design
- London 2012 Olympics Learning Legacy
- HS2 Learning Legacy
- The RIBA Plan of Work includes a definition of 'change control procedures': RIBA Plan of Work core project strategies

## The law

### Health and Safety at Work etc. Act 1974 (HSWA)

The general duties that arise under sections 2, 3 and 4 of the Act to do what is reasonably practicable to secure the health, safety and wellbeing of employees and others can be interpreted as requiring reasonable consideration of health and safety by design matters and acting on the findings.

Section 6 of the Act has a specific requirement to ensure through design and manufacture that 'articles used at work' do not present safety or health risks during set up, operation or maintenance. This is a relatively narrow duty compared to the generality of 'safety by design' however as 'article' is itself a specific term under the Act and does not encompass the entirety of railway systems, merely some of the items of machinery or equipment that exist within the railway system. For those items in scope however it is very relevant to health and safety by design considerations.

The Act sets out the general duties but perhaps more importantly it creates the power to set up a framework of subsidiary regulations. The following three statutory instruments made under the

Act expand on the general principles and deal more particularly with topics relevant to health and safety by design.

## **Management of Health and Safety at Work Regulations, 1999 (MHSW)**

The MHSW Regulations create a very explicit duty to carry out a suitable and sufficient risk assessment and then undertake prevention of the risks identified. The two key regulations are:

- Regulation 3, which set out the requirements on dutyholders to conduct a suitable and sufficient risk assessment; and
- Regulation 4, which asserts the general principles of prevention, which are then set out in detail in schedule 1 of Regulations – see below. This is commonly referred to as the hierarchy of risk control.

## **Construction (Design Management) Regulations 2015 (CDM)**

The Construction (Design and Management) Regulations 2015 apply to all railway building and construction projects, regardless of their size, duration, and nature.

These regulations place responsibility for the previous 'CDM coordinator' functions in the 2007 regulations on the new 'principal designer' role, including crucially the pre-construction phase responsibilities. This entails taking account of the general principles of risk prevention to eliminate, so far as are reasonably practicable, risks to people using or maintaining a structure, which includes a railway. Where it is not possible to eliminate these risks the designer must, so far as is reasonably practicable, take steps to reduce or control the risks through the subsequent design process. The designer's duties start as soon as designs are prepared which may be used in construction work. This includes the concept design stage and work carried out for feasibility studies. The emphasis is on addressing health and safety issues from the earliest point in a project to eliminate foreseeable risks and avoid costly changes or adaptations later on.

## **Railways and Other Guided Transport Systems Regulations 2006 (ROGS)**

The original 2006 version of ROGS has been amended by several later statutory instruments. The ORR website<sup>6</sup> summarises these and provides an unofficial consolidated version of ROGS for guidance; you should always check actual legislation for the authoritative version of the law.

For all dutyholders, mainline and non-mainline, responsibilities around risk assessment are set in

regulation 19 of ROGS.

ROGS Regulation 5(1)(b) requires that a mainline duty holder's Safety Management System applies the relevant parts of Common Safety Method on risk assessment and evaluation (CSM-RA). The CSM-RA requires that mainline railway dutyholders proposing any significant safety-related technical, operational, or organisational change use a common approach to assess and evaluate the risk posed by the change.

Before any significant proposed change, which is likely to be associated with an opportunity to re-design a product, equipment, process, or organisation, they must demonstrate that the 'risk assessment' principles have been correctly applied, including coordinating and managing the demonstration that the safety requirements are met. This may include assessments made by other organisations as part of larger projects.

The CSM-RA approach covers hazard identification, then risk analysis and evaluation via three main routes: the use of codes of practice or standards, using comparable reference systems, or undertaking explicit risk estimation. This approach also requires the use of an independent Assessment Body (AsBo) to input to and monitor the process.

ROGS Regulation 22 requires all transport operators to cooperate with one another. This can at times be central to the health and safety by design approach when dealing with shared risks or across interfaces between adjacent dutyholders. It covers both basic design compatibility, such as between train and platforms, as well as operational issues, for example ensuring stations are designed with ventilation to ensure operators staff are not exposed to DEEE.

Regulations 3 and 4 of ROGS only require mainline railway dutyholders to have a SMS once train services are operating. For new build mainline railways not associated with an existing infrastructure manager there is therefore no need to have a ROGS compliant SMS in place and the requirement under ROGS to follow CSM-RA is not in place either. In practice this should have minor effect since for a scheme to be Authorised under Interoperability it will have had to follow the CSM-RA process anyway.

For non-mainline railways and other types of transport system, such as metros and tramways, there is a requirement under regulation 6(6) of ROGS that if there is no 'transport operator' in place while a system or project is being developed then a responsible person takes on some of their duties. Those duties are the ones in paragraph 6(4) of ROGS to undertake Safety Verification (SV).

SV is a requirement under ROGS that when non-mainline transport operators (transport undertakings or infrastructure managers) introduce new or altered rolling stock or infrastructure, they need to ensure that health and safety considerations are incorporated into their design processes. SV is therefore entirely compatible with and a part of good health and safety by design practice. The Competent Person required under SV is there to advise and comment on the application of standards and good practice and to help decide on the assessment and acceptance criteria for projects.

SV does not apply to all non-mainline projects, there is a risk and difference test built into the system, but nevertheless whether formal SV is used with a Competent Person, or whether there is advice taken from an Independent Safety Advisor, the function of having some external advice can be a valuable role to help guide a project toward good practice and ensure that this is implemented properly.

There is further guidance on SV and the role of Competent Persons on ORR's website and the broader issues around 'change management are addressed in ORR's separate Strategic Risk chapter on this topic.

- [← Previous 4. Continuous improvement](#)
- [← Previous 3. Compliance expectations](#)
- [→ Next 5. Appendix](#)