

3 ENGINEERING SAFETY MANAGEMENT FUNDAMENTALS

To make sure that a change to the railway is safe and to show this, you must follow a systematic approach to Engineering Safety Management.

You do not need to carry out a full programme of ESM activities if you can show that the change involves only a 'broadly acceptable' level of risk, or no risk. However, you must monitor the risk to check that it stays low.

If the risk comes completely within accepted standards that define agreed ways of controlling it, showing that you have met these standards may be enough to show that the risk is acceptable. For instance the electrical safety of ordinary office equipment is normally shown by certifying it against electrical standards. However, before you decide that just referring to standards is enough, make sure that:

- the equipment is being used as intended;
- all of the risk is covered by the standards; and
- the standards cover your situation.

If you need to carry out an ESM programme, it must have some fundamental features. We can look at these under three headings. These are:

- the **organisation**, including the people who work within it, that will carry out the work;
- the proposed **change** to the railway; and
- the **project**, in other words the collection of activities which will make the change happen.

We use 'organisation' to mean a company, government agency or other corporate group.

Any change to the railway should be managed as a project.

The fundamentals do not just apply to the railway. When we refer to a 'change', this could be a change to any complicated system. In our case, this system will always be the railway, including not just physical parts like the track and trains, but people and procedures as well.

Each fundamental is shown in a box, followed by an explanation and justification.

3.1 Organisations

3.1.1 Safety responsibility

Your organisation must identify safety responsibilities and put them in writing. It must keep records of the transfer of safety responsibilities and must make sure that anyone taking on safety responsibilities understands and accepts these responsibilities. It must make sure that anyone who is transferring responsibility for safety passes on any known assumptions and conditions that safety depends on.

You need a structured organisation with good communications to carry out successful ESM. Everyone should have clear responsibilities and understand them.

In particular, anyone whose work creates a risk should be responsible for managing it. They should have the knowledge they need to understand the implications of that risk and to put controls in place.

Your organisation should identify who is accountable for the safety of work. They will stay accountable even if they pass on responsibility, for parts of the work, to others.

The organisation that takes the lead in introducing a change should make sure that the other organisations are clear on their safety responsibilities. If you hand over infrastructure changes to an infrastructure controller or hand over rolling stock to a train operator, you may also transfer some safety responsibility.

3.1.2 Safety culture

Your organisation must have safety as a primary goal.

The most important factor in achieving safety is creating a safety culture. This means running an organisation so that safety is seen as a primary goal and considered appropriately in every activity. Everyone should understand that achieving safety will help to meet business goals. Setting up safety procedures is not enough. All staff should understand why these procedures are necessary and use them.

3.1.3 Competence and training

Your organisation must make sure that all staff who are responsible for ESM activities are competent to carry them out. Your organisation must give them enough resources and authority to carry out their responsibilities. Your organisation must monitor their performance.

Staff should have the proper training, technical knowledge, skills, experience and qualifications for their job.

3.1.4 Working with suppliers

Whenever your organisation contracts out the performance of ESM activities, it must make sure that the supplier is competent to do the work and can put these fundamentals (including this one) into practice. It must check that they do put them into practice.

A supplier is anyone who supplies your organisation with goods or services. You can share safety responsibilities with your suppliers but you can never transfer them completely.

This fundamental is needed to make sure that the other fundamentals do not get lost in contractual relationships. Your organisation will set specific requirements from these fundamentals, which are relevant to the work being done, before passing the requirements on to the supplier. You do not have to pass them on by writing them into the contract, though this is normally a good idea.

3.1.5 Communicating safety-related information

If your organisation has information that someone else needs to reduce risk, your organisation must pass it on.

This information may include problems you find in someone else's work, or assumptions about someone else's work which are important to safety. Your organisation should pass on any relevant information about hazards and safety requirements to its suppliers.

3.1.6 Co-ordination

Whenever your organisation is working with others on one change, they must co-ordinate their ESM activities.

There are specific legal obligations in this area, for instance regulation 9 of the '*Management of Health and Safety at Work Regulations 1992*'.

3.2 Changes

3.2.1 Defining changes

Before starting work on a change, your organisation must define the aims, extent and context of the change.

This is often done in a requirements specification.

If you are in doubt about the aim, extent or context of the change, you will also be in doubt about claims for its safety.

When you define a change you should also find out which authorities will have to approve your safety case.

3.2.2 Identifying hazards

When your organisation considers change, it must make a systematic and vigorous attempt to identify any possible hazards. Your organisation must consider hazards which could contribute to an accident at any time, from introducing the change into the railway to removing it.

Identifying hazards is the foundation of ESM. If you do not identify a hazard, you can take no specific action to get rid of it or reduce the risk relating to it. However, you may be able to take general actions, such as introducing safety margins.

You should not just consider accidents which might happen during normal operation, but others which might happen at other times, such as installation, track-testing, commissioning, maintenance, emergencies, decommissioning and disposal.

You should consider the people who the change will affect, and design it to help them avoid mistakes.

When identifying hazards, you should consider all the effects of the change on the rest of the railway and its neighbours.

You may identify a possible hazard which you believe is so unlikely to happen that you do not need to do anything to control it. You should not ignore this type of hazard; you should record it together with the grounds for your belief that it is so unlikely to happen.

3.2.3 Assessing risk

Your organisation must assess the effect of any proposed change on overall system risk.

There are legal duties to assess risk.

Risk measures the likelihood that an accident will happen and the harm that could arise. You should consider both factors. Your organisation should also consider *who* is affected.

Some changes are made specifically to make the railway safer, that is to *reduce* risk, at least in the long run. You should still assess them in case they introduce other risks.

3.2.4 Reducing risk

Your organisation must carry out a thorough search for measures which reduce overall system risk, within its area of responsibility. It must decide whether each measure is reasonably practicable and, if so, must take it.

If your organisation finds that risk is still intolerable, it must not accept it.

If the risk is in the broadly acceptable region, you need only consider measures which are clearly reasonably practicable.

There are legal duties to do this.

You should look for:

- ways to get rid of hazards or to reduce their likelihood;
- ways to contain the effects of hazards, if they happen; and
- contingency measures to reduce harm if there is an accident.

You should look for ways of controlling both hazards introduced by the change itself and hazards that are already present in the railway. Even if a change is designed to make the railway safer then you should still see if there are ways that you could make the railway even safer.

3.2.5 Safety requirements

Your organisation must set safety requirements for any change, to reduce the risk associated with the change to an acceptable level.

Safety requirements are requirements that should be met to make sure that the safety risk presented by a change is reduced to an acceptable level. Safety requirements may specify:

- features or functions of the change, including any which help people avoid dangerous mistakes;
- what the change must not do to ensure safety;
- environmental conditions under which the change must operate to stay safe;
- targets for carrying out a function reliably, or reliably avoiding a dangerous state;
- features of the design and build processes; and
- operational procedures and restrictions.

You will set some safety requirements to meet regulations or standards. Others may arise when you identify hazards and assess and reduce risk.

3.2.6 Evidence of safety

Your organisation must convince itself that risk associated with a change has been reduced to an acceptable level. It must support its arguments with objective evidence, including evidence that it has met all safety requirements.

You should normally put these arguments together in a safety case to show that:

- you have adequately assessed the risk;
- you have set adequate safety requirements and met them;
- you have carried out the safety plan; and
- all safety-related work has been done by people with the proper skills and experience.

If other people must take action before a change is safe, the safety case should describe these actions and show that the other people have accepted responsibility for carrying out these actions.

You may include relevant in-service experience and safety approvals as supporting evidence.

If you are working on signalling systems or equipment, CENELEC standard ENV 50129:1998, '*Railway Applications – Safety Related Electronic Systems for Signalling*' is relevant. It places requirements on safety cases.

3.2.7 Authorising changes

No change can be authorised until all necessary safety approvals have been given.

You must get safety approval from the necessary safety authorities. You will usually need approval from both the railway authority (such as Railtrack and London Underground Limited) and the regulatory authority (HMRI in the UK). Safety approval will normally be based on accepting the safety case.

The approving authority will normally produce a certificate, setting out any restrictions on how the work is used.

The approving authority will usually give safety approval at the end of a project, when the change is about to go into service. Some projects make staged changes to the railway in which case each stage will need safety approval. Large or complicated projects may need additional approval before they change the railway, for example for a safety plan or for safety requirements.

3.3 Projects

3.3.1 ESM from start to finish

Your organisation must start ESM activities as soon as possible. It must review the results of these activities, and any assumptions made throughout the project. It must review and extend ESM activities whenever new information makes this necessary. It must monitor information on performance that relates to safety.

You should start early while it is easiest to build safety in. However, you may have little design information early in the project, so you should repeat the hazard analysis and risk assessment activities throughout the project, as the design becomes more detailed.

New information also includes design changes and information on faults.

3.3.2 Safety planning

Your organisation must plan all ESM activities before carrying them out.

You will normally write a safety plan, which should describe how you will put all these ESM fundamentals into practice on your project.

You do not have to write one plan for the whole programme beforehand, but you should plan each ESM activity before you do it.

You should adjust the extent of the safety plan and the ESM activities you carry out according to the extent of the risk.

3.3.3 Systematic processes and good practice

Your organisation must carry out safety-related projects following systematic processes which use good engineering practices. It must write down the processes beforehand.

You should use good systems engineering practice to develop safety-related systems.

Engineering needs a safety culture as much as any other activity. It is true that safety depends on the people who do the work, but it also depends on the way they do their work and the tools they use.

When choosing methods, you should take account of relevant standards. What is and is not good practice will depend upon the requirements.

3.3.4 Configuration management

Your organisation must have configuration management arrangements that cover everything which is important to achieve safety or to demonstrate safety.

You should keep track of the items that the project produces and the relationships between them. This is known as configuration management. Your configuration management arrangements should let you:

- uniquely identify each version of each item;
- record the history and status of each version;
- record the parts of each item (if it has any); and
- record the relationships between the items.

If you are in doubt about any of the above, you cannot be certain that all risk has been controlled.

3.3.5 Records

Your organisation must keep full and auditable records of all project ESM activities.

You should keep records to show that you have followed the safety plan. These records may include the results of design activity, analyses, tests, reviews and meetings. You should keep a hazard log which records all the possible hazards identified and describes the action to be taken to get rid of them, or reduce their likelihood or severity to an acceptable level.

The amount and type of records that you keep will depend on the extent of the risk.

You should keep records until you are sure that nobody will need them to make further changes or to investigate an incident. Often you will have to keep records until the change has been removed from the railway.

3.3.6 Independent professional review

ESM activities you carry out must be reviewed by professionals who are not involved in the activities concerned.

These reviews are normally structured as a series of safety audits and safety assessments. They assure that the work has been carried out safely and provide evidence to support the safety case. How often and how thoroughly each type of review is carried out, and the degree of independence of the reviewer, will depend on the project. They will depend on the amount of risk and novelty and on how complicated the project is.