The principles of the safe management of engineering change: Guidance

Issue 1, May 2012

Disclaimer

Users of documents published by the Rail Safety and Standards Board Limited (RSSB) are reminded of the need to consider their own responsibilities to ensure health and safety at work and their own duties under health and safety legislation. RSSB does not warrant that compliance with all or any documents published by RSSB is sufficient in itself to ensure safe systems of work or operation or to satisfy such responsibilities or duties.

If an organisation has defined processes and procedures to be followed related to the management of engineering change, those processes and procedures should be followed.

Where specific guidance exists, for example in relation to specific legislative requirement, such guidance should be followed in preference to the generic guidance in this document.

Published by:

RSSB
Block 2
Angel Square
1 Torrens Street
London
EC1V 1NY

The principles of the safe management of engineering change: Guidance

1. INTRODUCTION

1.1 Purpose

1.1.1 This guidance on the safe management of engineering change is written for people who are involved in introducing engineering changes to the railway. The guidance is intended to assist them in making sure that their work contributes to maintaining or improving safety.

1.1.2 The safe management of engineering change is commonly called 'Engineering Safety Management' (ESM) and this term is used in the guidance.

1.1.3 Introducing engineering changes to the railway always includes considering issues outside engineering and usually includes people who are not engineers, so the guidance is written for a wider audience than engineers only.

1.2 Definitions

1.2.1 In general this guidance is written in plain language, but a few specialised terms are used. In this guidance they have the following meanings.

a) **Hazard** – a condition that could lead to an accident.
Hazards should be eliminated wherever practicable, but this is not always the case. Where a hazard cannot be completely eliminated there will be some residual risk.

b) **Risk** – the rate of occurrence of accidents and incidents resulting in harm (caused by a hazard) and the degree of severity of that harm.
In many cases, risk cannot be eliminated entirely. We need to accept this if we are to continually improve safety.

c) **Maintenance** is used in its ordinary English sense of "keeping something fit for service" including, where necessary, replacing a worn-out part of the railway with a new part. So in this guidance maintenance includes what some people call 'renewals', 'alterations', 'upgrades' and 'enhancements'.

1.2.2 Something is considered to be **safe** when the risk associated with it is controlled to an acceptable level.

1.2.3 UK legislation places duties on employers to ensure safety 'so far as is reasonably practicable' (SFAIRP). When these duties are considered in relation to risk management, this is sometimes described as a requirement to reduce risk to a level that is 'as low as reasonably practicable' (ALARP). These terms therefore express the same concept in different contexts and for all practical purposes should be considered to be synonymous.

1.2.4 Other countries have different regulations for determining what level of safety or risk is acceptable.

1.2.5 The acceptable level of risk may reduce as technological advances make it practicable to reduce risk even further.

1.2.6 **Sub-system** means one of the specific areas of the railway. This term is used in the European Technical Specifications for Interoperability (TSIs). The sub-systems are divided into **structural sub-systems** (Energy; Infrastructure; Rolling Stock; Control, Command & Signalling (Trackside); Control, Command & Signalling (On-board); Rolling Stock) and **functional sub-systems** (Traffic Operation & Management; Maintenance; Telematics).

1.3 The role of standards

1.3.1 Use of standards is one of the ways to control risk. You will need to show that the standards you used were relevant for the control of the hazards under consideration.

1.3.2 Sometimes the risk from a particular activity is adequately controlled by accepted standards that define agreed ways of controlling it.

1.3.3 However, before you decide that applying standards is sufficient to control the risk from your activities, you should make sure that:

a) the equipment or process is being used as intended;

b) all of the risk is covered by the standards;

c) the standards cover your situation; and

d) there are no obvious and reasonably practicable ways of reducing risk further.

1.3.4 In cases where the risk is not adequately controlled by accepted standards, it may be necessary to undertake an explicit risk assessment; or to compare what you are doing with a ‘reference system’, proven in-use to have an acceptable safety level; or to use a combination of the two.

1.4 Human behaviour

1.4.1 Even the most highly automated equipment is designed, installed, operated and maintained by people. Everybody makes mistakes. People’s behaviour plays a part in most accidents. If you have not considered people’s behaviour in your work, it will be difficult to show that you have controlled risk properly. Understanding how people behave, including when things go wrong, is important in understanding the risk.

1.4.2 Remember that people can prevent accidents as well as contribute to them, and you should also take this into account.

1.4.3 You should consider all the people whom your work will affect when applying each of the principles. This should include customers, the general public, installers, operators and maintainers.

2. GUIDANCE ON THE PRINCIPLES OF THE SAFE MANAGEMENT OF ENGINEERING CHANGE

2.1 Introduction

2.1.1 A systematic approach to ESM plays an essential part in making sure that the railway is safe.

2.1.2 You do not need to carry out a full programme of ESM activities if you can show that your work involves only a very low level of risk, or no risk, or that the risk is adequately covered by standards. However, you should monitor the risk to check that this remains the case.

2.1.3 If you need to carry out an ESM programme, it should have some basic features. These are structured under the following headings:

a) **organisation:** the general features needed by any organisation whose work affects safety;

b) **process:** methods of working that affect safety;

c) **risk assessment:** identifying hazards and assessing risk; and

d) **risk control:** controlling risk and showing that it is acceptable.

2.1.4 The principles set out in this document identify, at a high level, what needs to be done to ensure the safe management of engineering change. They do not identify who is responsible for what. You need to work out what responsibilities your organisation has and plan your work to meet them.

2.1.5 If your work involves introducing a railway product or sub-system that has been used elsewhere, you may find that some of these principles were not put fully into practice beforehand, or, if they were, that you do not have evidence of it. On the other hand you may have direct evidence that the product has performed safely in the past in similar circumstances. You will need to balance these two factors and consider their effect on risk in order to decide how far you need to apply the risk control and risk assessment principles. You should take account of any differences between the way the product was used before and the way you are planning to use it.

2.1.6 Each principle is shown in a box, followed by an explanation and some guidance.

2.2 Organisation principles

2.2.1 Safety responsibility

Your organisation should identify post holders with responsibilities for safety and put these responsibilities in writing. It should keep records of the transfer of these responsibilities and should make sure that anyone taking on responsibilities for safety understands and accepts these responsibilities. It should make sure that anyone who is transferring responsibility for safety passes on any known assumptions and conditions that are required for the safe management of the project or other activities.

2.2.1.1 Any organisation whose work might contribute to an accident will have a corporate responsibility for safety. This will cover the safety of everyone who might be affected by its activities, which may include workers, passengers and members of the public. Your organisation should be set up so that its people work together effectively to meet this corporate responsibility.

2.2.1.2 Everyone within your organisation should have clear responsibilities and understand them. Your organisation should identify who is accountable for the safety of work. This should normally be the person who is accountable for the work itself. They stay accountable even if they ask someone else to do the work for them.

2.2.1.3 The organisation that takes the lead in changing, maintaining or operating some aspect of the railway should make sure that the other organisations are clear about their safety responsibilities and that these responsibilities cover everything that needs to be done to ensure safety. Transfer of information between organisations is a very important part of this process.

2.2.1.4 For each part of the railway, someone should be identified as being responsible for keeping up-to-date information about how it is built, how it is maintained, how safely and reliably it is performing, how it was designed and why it was designed that way, and for using that information to evaluate changes.

2.2.2 Organisational goals

Your organisation should have safety as a primary goal.

2.2.2.1 The people leading your organisation should make it clear that safety is a primary goal. They should set targets for safety, together with other primary goals, and allocate the resources needed to meet them.

2.2.3 Safety culture

Your organisation should make sure that all staff understand and respect the risk related to their activities and their responsibilities, and work effectively with each other and with others to control it.

2.2.3.1 The people leading your organisation should make sure that:

a) staff understand the risk arising from their activities and keep up-to-date with the factors that affect safety;

b) staff are prepared to report safety incidents and near misses (even when it is inconvenient or exposes their own mistakes), and that their managers respond effectively;

c) staff understand what is acceptable behaviour, are reprimanded for reckless or malicious acts, and are encouraged to learn from mistakes;

d) the organisation is adaptable enough to deal effectively with abnormal circumstances; and

e) the organisation learns from past experiences and uses the lessons to improve safety.

2.2.4 Competence and training

Your organisation should make sure that all staff who are responsible for activities which affect safety are competent to carry them out. It should give them enough resources and authority to carry out their responsibilities. It should monitor their performance.

2.2.4.1 The people leading your organisation should be competent to define safety responsibilities and objectives for the organisation.

2.2.4.2 Your organisation should set requirements for the competence of staff who are responsible for activities which affect safety. It should work out what training, technical knowledge, skills, experience and qualifications they need. You should then select and train staff to make sure that these needs are met.

2.2.4.3 You should monitor the performance of staff who are responsible for activities which affect safety and check that they are in fact meeting these requirements.

2.2.5 Working with suppliers

Whenever your organisation contracts out the performance of activities that affect safety, it should make sure that the supplier is competent to do the work and can put these principles into practice. It should check that they do put them into practice effectively.

2.2.5.1 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. In applying the principle on '**safety responsibility'** at 2.2.1, you should be clear about what safety responsibilities you are sharing.

2.2.5.2 Your organisation should set specific requirements based on the principles that are relevant to the work being done, before passing these requirements on to your suppliers. You also need to check that your suppliers are competent to pass requirements to their suppliers.

2.2.6 Communicating safety-related information

If someone tells you or your organisation something that suggests that risk is too high, you should take prompt and effective action. If you have information that someone else needs to control risk, you should pass it on to them and take reasonable steps to make sure that they understand it.

2.2.6.1 This information may include:

a) information about the current state of the railway;

b) information about how sub-systems and assets are used in practice;

c) information about the current state of work in progress – especially where responsibility is transferred between shifts or teams;

d) information about changes to standards and procedures;

e) information about an incident;

f) problems you find in someone else's work; and

g) assumptions about someone else's work which are important to safety.

2.2.6.2 Communications within an organisation should be two-way. In particular, the people leading your organisation will need to make sure that they get the information that they need to take good decisions about safety and then make sure that these decisions are communicated to the people who need to know about them.

2.2.6.3 Your organisation should pass on any relevant information about hazards and safety requirements to its suppliers and customers.

2.2.7 Co-ordination

Whenever your organisation is working with others on activities that affect the railway they should co-ordinate their safety management activities.

2.2.7.1 Most countries have specific legal obligations in this area.

2.2.8 Continuing safety management

Your organisation should continue to put these principles into practice as long as its activities and responsibilities affect the safety of the railway.

2.2.8.1 The earlier you start to manage safety, the easier and less expensive it will be to build safety into your activities and the sooner you will see the benefits in reduced risk.

2.2.8.2 However, things never stay exactly the same. Just because you successfully controlled risk to an acceptable level in the past does not mean that you can assume that it will stay acceptable. You need to be alert to any change in the risk associated with your organisation's activities and react to it for as long as you are responsible for the safety of part of the railway.

2.2.8.3 This principle is related to the principle on '**monitoring risk'** at 2.4.5.

2.3 Process principles

2.3.1 Safety planning

Your organisation should plan all engineering safety management activities before carrying them out.

2.3.1.1 Your plans should be detailed enough to put the principles into practice.

2.3.1.2 You may cover everything in one plan, but you do not have to. You may write different plans for different aspects of your work at different times, but you should plan each activity before you do it.

2.3.1.3 You may have plans at different levels of detail. You may, for example, have a strategic plan for your organisation which starts with an analysis of the current situation and sets out a programme of activities to achieve your objectives for safety. You may then plan detailed safety management activities for individual tasks and projects.

2.3.1.4 You may include safety management activities in plans that are also designed to achieve other objectives. For example, safety management activities should normally be taken into account as part of the planning process for maintenance activities. The output of this planning process may be called something other than a ‘plan’ – for example, a ‘specification’ or a ‘schedule’. This does not matter as long as the planning is done.

2.3.1.5 You should adjust the extent of your plans and the safety management activities you carry out according to the extent of the risk. You should review your plans in the light of new information about risk and alter them if necessary.

2.3.1.6 If there is a possibility that you may become involved in an emergency on the railway, you should have plans to deal with it.

2.3.2 Systematic processes and good practice

Your organisation should carry out activities which affect safety by following systematic processes which use recognised good practice. It should write down the processes beforehand and review them regularly.

2.3.2.1 Your organisation should use good systems engineering practice to develop and maintain safety-related systems.

2.3.2.2 Safety depends on the awareness and competence of the people who do the work, but it also depends on the processes and tools they use. The people leading your organisation should be aware of relevant good practice and encourage staff to adopt it.

2.3.3 Configuration management

Your organisation should have configuration management arrangements that cover changes to all the assets, processes and procedures that are needed to achieve or demonstrate the safe management of engineering change.

2.3.3.1 Your organisation should keep track of changes to all the assets, processes and procedures that are needed to achieve or demonstrate the safe management of engineering change, and of the relationships between these items. This is known as configuration management. Your configuration management arrangements should help you to understand:

a) **what** assets, processes and procedures you have;

b) **how** each item has developed into its current modification state, version or issue; and

c) **why** each item has developed into its current modification state, version or issue.

2.3.3.2 To do this, the configuration management arrangements should let you:

a) uniquely identify each modification state, version or issue of each item;

b) record the history and status of each modification state, version or issue of each item;

c) record the parts of each item (if it has any);

d) record the relationships between the items; and

e) define precisely actual and proposed changes to items.

2.3.3.3 You should decide the level of detail to which you will go: for example, whether you will keep track of the most basic components individually or assemblies of components. You should go to sufficient detail so that you can demonstrate that your activities are being managed safely.

2.3.3.4 If you are maintaining part of the railway, your configuration management arrangements should cover that part of the railway and the information that you need to maintain it.

2.3.4 Records

Your organisation should keep full and auditable records of all activities which affect safety.

2.3.4.1 Your organisation should keep records to support your conclusions that risk has been controlled to an acceptable level. You should also keep records which allow you to learn from experience and so contribute to better decision-taking in the future.

2.3.4.2 Your records should include evidence that you have carried out the planned safety management activities. These records may include (but are not limited to):

a) the results of design activity;

b) safety analyses;

c) tests;

d) review records;

e) records of near misses, incidents and accidents;

f) maintenance and renewal records; and

g) records of decisions that affect safety.

2.3.4.3 The number and type of records that you keep will depend on the extent (scope and severity) of the risk you are managing.

2.3.4.4 You should also create a hazard record which records the hazards identified and describes the action to remove them or control risk to an acceptable level. The hazard record should be kept up-to-date.

2.3.4.5 You should keep records securely until you are confident that nobody will need them. For example, the records may be required to support further changes or to investigate an incident. Often, if you are introducing an engineering change to the railway, you will have to keep records until the change has been removed from the railway. You may have to keep records even longer in order to fulfil your contract or meet standards.

2.3.5 Independent review

Safety management activities that your organisation carries out should be reviewed by people who have an appropriate degree of independence from the activities concerned.

2.3.5.1 Review of safety-related work by independent people can be an important contribution to your and others' confidence in the work you are undertaking. An organisation can instigate a review at any time during the project.

2.3.5.2 Your organisation should decide if an independent review is required, based on the following factors:

a) the extent (scope and severity) of the risk from the activities, and

b) the novelty of the work being undertaken, and

c) the complexity of the work being undertaken.

2.3.5.3 If your organisation decides that an independent review is required, the factors in 2.3.5.2 should also be taken into account when deciding the frequency and type of review, and the degree of independence of the reviewer.

2.3.5.4 These reviews may be structured as a series of safety audits and safety assessments. Audits provide evidence that you are following your plans for safety. Assessments provide evidence that you are meeting your safety requirements.

2.3.5.5 Your organisation should check the competence of the reviewer, based on the factors described in the principle on **'competence and training'** at 2.2.4.

2.4 Risk assessment principles

2.4.1 Introduction

2.4.1.1 Risk assessment provides information on which to base good decisions about safety. For projects, these decisions will include whether or not to put a new part of the railway into service and under what conditions. For maintenance, these decisions will include whether or not to take unscheduled action to prevent failure. In both cases, these decisions involve balancing the risk arising from doing the work against the risk arising from not doing the work. Both may include risk to railway operation and risk to the people doing the work.

2.4.2 Defining your work

Your organisation should define the extent and context of its activities.

2.4.2.1 You should be clear about the extent and context of your organisation's activities, and the boundaries of these activities with the activities of other organisations.

2.4.2.2 If you are changing the railway or developing a product, the extent and context of these activities are often defined in a contract or a requirements specification.

2.4.2.3 These documents may be based on assumptions. If so, you should check these assumptions as soon as possible.

2.4.3 Identifying hazards

Your organisation should make a systematic and vigorous attempt to identify all possible hazards related to its activities and responsibilities.

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

2.4.3.2 When you identify a hazard relating to your activities and responsibilities, you should make sure that you understand how you might contribute to the hazard when carrying out your activities and responsibilities.

2.4.3.3 You should not only consider accidents or incidents which might happen during normal operation, but also accidents or incidents which might happen:

a) when things go wrong, or

b) during periods of abnormal or degraded operations, or

c) at other times, such as installation, testing, commissioning, maintenance, decommissioning and disposal.

2.4.3.4 When identifying hazards, you should consider:

a) the people and organisations whom your activities and products will affect; and

b) the effects of your activities and products on the rest of the railway and its neighbours.

2.4.3.5 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 reasons you believe it is so unlikely to happen, and review it regularly.

2.4.4 Assessing risk

Your organisation should assess the effect of its activities and responsibilities on overall risk on the railway.

2.4.4.1 Most countries have specific legal obligations in this area.

2.4.4.2 Risk is defined as the rate of occurrence of accidents and incidents resulting in harm (caused by a hazard) and the degree severity of that harm. You should consider both factors – rate of occurrence and severity. Your organisation should also consider who is affected.

2.4.4.3 Some activities are undertaken specifically to make the railway safer. You should still assess these activities in case they introduce other risks that need to be controlled.

2.4.4.4 Your risk assessment should take account of the results of the activities described in the principle on **'monitoring risk'**, described at 2.4.5.

2.4.5 Monitoring risk

Your organisation should take all reasonable steps to check and improve its management of risk. It should look for, collect and analyse data that it could use to improve its management of risk. It should continue to do this as long as it has responsibilities for safety, in case circumstances change and this affects the risk. It should act where new information shows that this is necessary.

2.4.5.1 The type of monitoring you should perform depends on the type of safety-related work you do. To the extent that it is useful and within your area of responsibility, you should monitor:

a) how safely and reliably the railway as a whole is performing;

b) how safely and reliably parts of the railway are performing;

c) how closely people are following procedures and the effectiveness of those procedures; and

d) the circumstances within which the railway operates.

2.4.5.2 You should consider collecting and analysing data about:

a) incidents, accidents and near misses;

b) suggestions and feedback from your staff;

c) failures to follow standards and procedures;

d) faults and wear and tear; and

e) anything else which may affect your work.

2.4.5.3 If safety depends on assumptions and you have access to data which you could use to check these assumptions, then you should collect and analyse these data. If you analyse incidents, accidents and near misses, you should look for their root causes because preventing these may prevent other problems as well.

2.4.5.4 You should ask your staff to tell you about safety problems and suggest ways of improving safety.

2.4.5.5 If you are a supplier, you may not be able to collect all of this data yourself. If so, you should ask the organisations using your products and services to collect the data you need and provide them to you.

2.4.5.6 This principle is related to the principle on **'continuing safety management'** described at 2.2.8.

2.5 Risk control principles

2.5.1 Reducing risk

Your organisation should carry out a thorough search for measures which control overall risk on the railway, within its area of responsibility. It should decide whether it is reasonable to take each measure. It should take all measures which are reasonable or required by law. If it finds that the risk is still too high after it has taken all measures, it should not accept it.

2.5.1.1 In order of priority, you should look for:

a) ways to get rid of hazards or to reduce their likelihood;

b) ways to contain the effects of hazards; and

c) contingency measures to reduce harm if there is an accident.

2.5.1.2 When searching for measures to reduce risk, you should bear in mind that safety is highly dependent on how well people and equipment do their job. You should avoid relying completely for safety on any one person or piece of equipment.

2.5.1.3 You should look for ways of controlling hazards introduced by your work as well as hazards that are already present in the railway. Even if your work is designed to make the railway safer, you should still look for measures you could take to improve safety even further.

2.5.2 Safety requirements

Your organisation should set and meet safety requirements to control the risk associated with the work to an acceptable level.

2.5.2.1 Safety requirements may specify:

a) actions to control risk;

b) specific functions or features of a product, sub-system or part of the railway;

c) features of maintenance or operation practices;

d) features of design and build processes; and

e) tolerances within which something must be maintained.

2.5.2.2 You may have requirements at different levels of detail. For example, you may set overall targets for risk within your area of responsibility and then define detailed technical requirements for individual pieces of equipment.

2.5.2.3 You should make sure that your safety requirements are realistic and clear, and that you can check they have been met. You should check they are being met. If they are not being met, you should do something about it.

2.5.3 Evidence of safety

Your organisation should satisfy itself that risk associated with its activities and responsibilities has been controlled to an acceptable level. It should support its arguments with objective evidence, including evidence that it has met all safety requirements.

2.5.3.1 You should show that:

a) you have adequately assessed the risk;

b) you have set adequate safety requirements and met them;

c) you have carried out the safety management activities that you planned; and

d) all safety-related work has been done by people with the proper skills and experience.

2.5.3.2 You should check that the evidence for your conclusions is reliable. You should record and check any assumptions on which your conclusions are based. If you rely on other people to take action to support your conclusions, you should write these actions down. You should do what you reasonably can to make sure that the other people understand what they have to do and have accepted responsibility for doing it.

2.5.3.3 You should take account of the activities described in the principle on **'monitoring risk'** at 2.4.5.

2.5.4 Checking and approval / authorisation

Your organisation should obtain all necessary checks and approvals / authorisations before it does any work which may affect the safety of the railway.

2.5.4.1 You may need approval for your work from the railway safety authority (ORR in the UK). In some cases the safety authority may approve your organisation's overall processes, described in your safety management system, and then allow you to approve your own work.

2.5.4.2 If you are making a major or complex change to the railway, you may need authorisation before you bring the change into service. In these cases, the changes will need to be independently verified before authorisation.

2.5.4.3 You will also need to agree with the organisation that manages the infrastructure or those that operate trains that the proposed changes are compatible with the system into which they are being introduced.

2.5.4.4 If you are maintaining the railway, you may need to get your maintenance plans and procedures approved before you put them into action. You may also need approval to put equipment you have been working on back into service or to bring plant and equipment onto the railway

3. FURTHER GUIDANCE

3.1 Guidance for organisations involved in the GB mainline railway system can be found on RSSB's website. This takes the form of a process map to help organisations to navigate their way through the relevant legislation, and available guidance that supports the legislation, in the most efficient and cost-effective manner.

3.2 Detailed guidance on hazard identification, risk assessment and risk reduction will be available, in the form of Rail Industry Guidance Notes, from early September 2012 via rgsonline.co.uk