

Chapter 12

Safety Planning and Good Practice

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

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

12.1 Guidance from volume 1

12.1.1 Safety planning

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.

12.1.2 Systematic processes and good practice

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 may depend upon the requirements.

12.2 Background

The Yellow Book recommends that any significant change to the railway should be run as a project. A Safety Plan should be produced for each safety-related project.

The Safety Plan performs two main functions:

- 1 it provides a detailed schedule of how safety risks will be reduced to an acceptable level (or shown already to be at an acceptable level); and
- 2 it provides a means of demonstrating that this has been done.

The Safety Plan should describe a programme of work which will ensure the Safety Requirements are identified and met. It should also state and justify the allocation of key staff and resources to carry out this programme.

The Safety Plan is an evolutionary document. For example, early in the project a Preliminary Safety Plan will describe the safety analysis activities needed to derive Safety Requirements. As the project progresses, a Safety Plan will describe activities to meet these Safety Requirements.

This chapter describes the different types of Safety Plan that may be required during a project, the process for preparing a Safety Plan, and its content.

The other chapters of this volume describe good practice in ESM activities, such as safety analysis and preparing a Safety Case. However, you should also use good practice if you are carrying out mainstream engineering work, such as civil, electronic and software engineering.

What constitutes good practice is relative and depends on:

- the type of work that you are doing;
- the Safety Integrity Level (SIL) of the system or equipment; and
- the current standard of good practice, which will change with time.

This chapter does not attempt to define what is and is not good practice for a wide range of engineering disciplines, but it does provide guidance on researching good practice and documenting and justifying your choices.

This chapter is written for:

- anyone responsible for preparing a Safety Plan,
- anyone who will need to endorse a Safety Plan, and
- anyone involved in performing, auditing or assessing ESM activities.

12.3 Relevant Safety Authorities

When planning or implementing a change to the railway, it is necessary to gain approval for the change from certain Safety Authorities. Approval may be needed from the following organisations:

- your own organisation,
- the railway authority (for instance, Railtrack or London Underground Ltd),
- the regulatory authority (HMRI in the UK).

To find out if the change needs approval from these organisations, you should in the first instance:

- Check your own organisation's requirements.
- Consult the railway authority's procedures (for example, Railway Group Standards).
- Consult the guidance provided by the regulatory authority (for example, HMRI's document '*Guide to the Approval of Railway Works, Plant, and Equipment*' [F.18]).

Unless you know definitely that you do not require approval from any of the above organisations, then you should seek advice from them.

In the rest of this chapter, 'relevant Safety Authority' means any organisation from which approval is required.

12.4 The depth of safety planning

The size and depth of the Safety Plan will depend on the complexity and level of risk presented by the project. For simple and low-risk projects a brief Safety Plan defining the project personnel and justifying a simple approach may be sufficient. Note that, if you assume a project is low-risk, you should make this assumption explicit and take action to confirm it. The Safety Plan should be endorsed by the relevant Safety Authorities, regardless of the level of complexity or risk.

The Safety Plan may permit reliance on previous work to demonstrate acceptable risks. You would not normally do this unless:

- the previous work used good practice, and
- it covered all of the project risk, and
- there is no novelty in development, application or use.

The last condition may be relaxed slightly, to allow limited novelty for low-risk projects.

12.5 The safety planning process

The Project Manager is responsible for preparing the Preliminary and full Safety Plans. The Project Manager may delegate the preparation of these documents to suitably qualified and competent personnel but should retain overall responsibility.

The relevant Safety Authorities are responsible for endorsing Safety Plans.

A typical approach to the safety planning process is as follows:

- 1 Develop a Preliminary Safety Plan to set out an overall approach to managing safety on the project. In particular, the Preliminary Safety Plan should describe the approach for carrying out a full Safety Analysis and justify the competencies of key staff allocated to undertake these activities.
- 2 Seek endorsement of the Preliminary Safety Plan from the relevant Safety Authorities.
- 3 Carry out the Safety Analysis and produce a set of Safety Requirements.
- 4 Prepare a Safety Plan to describe how the Safety Requirements are to be met.
- 5 Seek endorsement of the Safety Plan from the relevant Safety Authorities.
- 6 Update this version of the Safety Plan as appropriate and seek re-endorsement

Note: it may save time to seek comments from the Safety Auditor before submitting a strategy or plan to the Safety Authority.

The Safety Plan should be scoped according to the information available and the organisation of the project. It may be split into smaller plans that cover particular stages of the lifecycle, activities to be carried out by particular disciplines or the entire project. However, every project safety activity should be covered by a Safety Plan.

The Safety Plan should be updated throughout the project to reflect any changes to the planned activities that arise as a result of undertaking safety activities. Following significant updates, the Safety Plan should be re-submitted for endorsement.

The Safety Plan should state and justify the ESM approach to be applied to the project, so that it may be considered and endorsed.

The Safety Plan may be combined with reliability, maintainability and availability plans into a System Assurance Plan. However, it is usually kept separate so that it may be submitted to the relevant Safety Authorities, who will want to focus on the safety aspects of the project and do not need to see other plans.

12.6 Content of a Preliminary Safety Plan

This section describes the information that should be contained within a Preliminary Safety Plan.

The Preliminary Safety Plan will be a short, high-level version of the Safety Plan, produced as early in the project as possible, and describing the overall strategy and approach to reducing safety risks.

The following structure is recommended:

- 1 Introduction and background;
- 2 Safety analysis;
- 3 Key staff;
- 4 Safety audit and assessment;
- 5 Safety documentation;
- 6 Safety engineering.

Each section should be brief; detailed planning will be carried out after Safety Requirements have been set, and documented in the Safety Plan.

The **Introduction and background** should describe the aims, extent and context (see chapter 7) of the change to be made to the railway.

The **Safety analysis** section should describe the techniques to be adopted to determine the risk presented by the system or equipment and to establish Safety Requirements. This section should detail the competencies of key staff allocated to carry out hazard identification and analysis activities.

The **Key staff** section should identify those members of staff proposed for key safety roles and justify their competence.

The **Safety audit and assessment** section should identify the competence and independence requirements for auditors and or assessors. If they are known, they should be identified and shown to meet the requirements.

The **Safety documentation** section should detail the documentation that will be produced. The list should include Hazard Log, Safety Plan and the Safety Analysis documentation and also state whether an incremental or non-incremental Safety Case is to be used.

The **Safety engineering** section should describe, at a high-level, mainstream engineering steps that are being taken to reduce risk (such as redundancy, protection systems, fail-safe design principles).

12.7 Content of a Safety Plan

This section describes the information that should be contained within a full Safety Plan. The following structure is recommended:

- 1 Introduction;
- 2 Background and requirements;
- 3 ESM activities;
- 4 Safety controls;
- 5 Safety documentation;
- 6 Safety engineering;
- 7 Validation of external items.

A more detailed suggested outline for the Safety Plan is provided in appendix B. If another structure is used, it should cover the information described for each of the sections listed above.

For large or complex projects it may be appropriate to prepare separate plans covering one or more of these sections.

12.7.1 Introduction

This should describe the aim, purpose, scope and structure of the Safety Plan.

12.7.2 Background and requirements

This section should:

- a) justify the approach taken, with reference to ESM guidance such as this book and safety policy;
- b) describe or reference a description of any safety principles underpinning the approach to safety;
- c) describe the aims, extent and context (see chapter 7) of the change to be made to the railway and provide or refer to a summary of the system or equipment, including interfaces to other systems or projects;
- d) state or provide a reference to the Safety Requirements Specification;
- e) briefly describe the risk assessment criteria that will be used to derive targets for risk tolerability;
- f) describe or reference the process for assigning safety functions to system elements; and
- g) list any assumptions or constraints on the project or system.

Items c) and d) may be omitted from early issues, but should be included when the appropriate activities have been carried out.

12.7.3 ESM Activities

This section should address the following ESM issues, to the extent necessary:

- 1 Safety roles and responsibilities,
- 2 Safety lifecycle,
- 3 Safety analysis,
- 4 Safety deliverables,
- 5 Safety standards,
- 6 Safety assessment,
- 7 Safety audit,
- 8 Safety case and safety approval,
- 9 Supplier management,
- 10 Configuration management,
- 11 Project safety training,
- 12 System operation, modification and maintenance,
- 13 Decommissioning and disposal

The following sections describe what the Safety Plan should say about these issues.

12.7.3.1 Safety roles and responsibilities

This section should identify the key safety personnel of the project, their roles, responsibilities, qualifications and experience and the reporting lines between them.

Note: the Project Manager retains overall accountability for safety even if he or she delegates responsibilities for ESM activities.

In particular, this section should identify the personnel allocated to manage and perform the following safety activities:

- defining safety requirements;
- leading the design, implementation or validation activities;
- performing safety analysis;
- liaising with regulatory bodies such as HMRI.

Note: suppliers will normally liaise with HMRI via the railway operator.

The Project Manager should be responsible for:

- producing a Safety Plan;
- submitting the Safety Plan to the relevant Safety Authorities;
- where necessary, attending the safety endorsement meeting;
- ensuring safety documentation is produced as planned;
- commissioning Safety Audits and Assessments as planned;
- initiating ESM activities, as planned;
- ensuring that all project staff have read and understood the Safety Plan;
- obtaining and allocating sufficient resources to implement the Safety Plan;

- ensuring competence of key staff; and
- co-ordinating safety activities with other parts of the organisation, and with the client.

If there is a Project Safety Manager, they will typically be delegated responsibility for:

- producing a Safety Plan;
- submitting the Safety Plan to the relevant Safety Authorities;
- where necessary, attending the endorsement meeting;
- ensuring safety documentation is produced as planned;
- commissioning Safety Audits and Assessments as planned; and
- initiating ESM activities, as planned.

This section should define the specific safety responsibilities of the Safety Auditor and Safety Assessor.

The Safety Auditor should audit the project to check for adequacy of the Safety Plan and compliance with the Safety Plan and any referenced standards or procedures.

The Safety Assessor should assess the project to check the adequacy of the Safety Requirements and that the Safety Requirements are being met.

Chapter 2 provides guidance on safety roles and responsibilities and chapter 14 provides guidance on carrying out Safety Audits and Assessments.

12.7.3.2 Safety lifecycle

This section should define a project lifecycle that describes the major phases of the project, and a safety lifecycle that specifies the order in which the safety tasks are to be carried out. The safety lifecycle should be derived from the guidance given in chapter 11 on scheduling ESM activities, and should be tailored to the specific requirements of the project. The relationship between the project and safety lifecycles should be specified (that is, at what points in the project the safety activities will be performed).

12.7.3.3 Safety analysis

This section should define the process of safety analysis to be used to determine the Safety Requirements for the project. The process should be tailored to each individual project.

Guidance on performing safety analysis is provided in chapter 8 of this handbook.

For each safety analysis activity, this section should provide details of responsibilities, documentation and timing of deliverables. This section should also state the criteria used to establish the tolerability for the identified risks.

12.7.3.4 Safety deliverables

This section should detail the safety-related items (other than Safety Documentation, see section 12.7.5) that are to be delivered during the project. They should include safety-related hardware and software, but may also include other items such as maintenance procedures.

12.7.3.5 Safety standards

Any safety-related work should be performed within a defined Quality Management System (QMS), which is compliant with an ISO-9000 series standard.

This section should state the procedures and standards to be followed by the project. Procedures may include references to project quality and technical plans and industry, national or international standards. The plan should state the order of precedence of these procedures and standards, in case they are in conflict.

12.7.3.6 Safety assessment

This section should schedule a series of Safety Assessments to provide an authoritative, independent opinion on whether or not a project will meet its Safety Requirements. The Safety Assessor should be independent of the development team. Chapter 14 provides guidance on commissioning Safety Assessments and the independence of the Safety Assessor.

This section should address the Safety Assessment of suppliers, where suppliers are involved in safety-related work for the project.

Table 12-1 below provides guidance on when to schedule Safety Assessments for a typical system development project, depending on the Safety Integrity Level (SIL, see chapter 9). Safety Assessments are denoted as highly recommended (HR), recommended (R) or no recommendation (-).

Note that more frequent assessments than shown below may be appropriate for very large or very lengthy projects.

Activity	SIL 1	SIL 2	SIL 3	SIL 4
Production of Preliminary Safety Plan	-	-	-	-
Establishment of Safety Requirements	R	R	R	HR
Production of Full Safety Plan	-	HR	HR	HR
Implementation	-	-	R	HR
Production of Safety Case	R	R	R	HR
Operation and Maintenance	-	-	-	HR
Decommissioning and Disposal	-	-	-	R

Table 12-1 - Guidance on scheduling Safety Assessments

12.7.3.7 Safety audits

This section should schedule a series of Safety Audits to check compliance of the safety processes with the Safety Plan. The Safety Auditor should be independent of the development team. This section should also address the Safety Audit of suppliers, where suppliers are involved in safety-related work for the project. Chapter 14 provides guidance on commissioning Safety Audits and the independence of the Safety Auditor.

Table 12-2 below provides guidance on when to schedule Safety Audits for a typical system development project, depending on the Safety Integrity Level (SIL). Safety Audits are denoted as highly recommended (HR), recommended (R) or no recommendation (-).

Note that more frequent audits than shown below may be appropriate for very large or very lengthy projects.

Activity	SIL 1	SIL 2	SIL 3	SIL 4
Production of Preliminary Safety Plan	-	-	-	-
Establishment of Safety Requirements	-	-	-	-
Production of Full Safety Plan	HR	HR	HR	HR
Implementation	-	R	R	R
Production of Safety Case	-	R	R	R
Operation and Maintenance	-	R	HR	HR
Decommissioning and Disposal	-	-	-	R

Table 12-2 - Guidance on scheduling Safety Audits

12.7.3.8 Safety case and safety approval

This section should provide or reference the completion criteria for the safety-related aspects of the project. This should include the procedures and approvals mechanisms to be adopted.

This section should make provision for the safety approval of the system. An endorsed Safety Case is required for safety approval and this section should state who will write the Safety Case, when it should be written, and which Safety Authorities will need to endorse it.

The project may agree to deliver evidence of safety in some form other than a Safety Case. For example, it is possible that a third-party safety certificate and a safety assessment report may be sufficient. Any such agreement should be recorded here.

Note: if the project is developing a product, it may not be possible to identify all Safety Authorities who will approve its application in advance.

12.7.3.9 Supplier management

This section should make provision for ensuring that the work of suppliers is managed such that the parts of the system for which they are responsible meet the overall safety requirements. Suppliers should certify their products as compliant with the appropriate specifications. Their test plans should adequately demonstrate safety features. Where appropriate, references to test plan documentation should be made from the certification documentation.

Contracted items should be subject to the same safety analyses as those built in-house. Analyses and assessments conducted by suppliers should be used as an input to system level analyses. Safety targets for contracted work should be set by the Project Manager and agreed by the supplier. The Project Manager should require the supplier to produce a Safety Plan compliant with this guidance, which the Project Manager should endorse.

This section should schedule Safety Audits and Safety Assessments of suppliers. It should include activities for assessing suppliers' ESM and Quality Management Systems where work is being carried out under the suppliers' systems, to ensure that they are of an acceptable standard. Chapter 5 provides guidance on discharging safety responsibilities through suppliers.

12.7.3.10 Configuration management

This section should specify how configuration of system deliverables will be managed, normally referring to a separate configuration management plan for detail. This section should specify how systems, components and other equipment will be labelled to ensure that safety is not compromised by the use of faulty or untested equipment. Chapter 13 provides guidance on configuration management.

12.7.3.11 Project safety training

This section should define any training requirements of personnel scheduled to perform safety-related activities and provide a plan or programme of training that meets the requirements.

12.7.3.12 System operation, modification and maintenance

This section should outline processes for analysing system operation to ensure compliance with requirements. It should also describe the process and approval mechanisms for system modification and maintenance. A checklist of items to consider is provided in appendix C.

12.7.3.13 Decommissioning and disposal

This section should outline plans for safely decommissioning the system at the end of its life and disposing of it. A checklist of items to consider is provided in appendix C.

12.7.4 Safety controls

This section should specify all aspects of quality controls that contribute to safety, normally referring to a separate quality plan for detail. It should identify any requirements for the use of equipment in restricted areas or restrictions to be imposed on the use of equipment in open areas. These requirements may cover training, security clearance or the use of specific safety-related procedures or controls.

This section should also record the signatories for each safety deliverable produced by the project. The signatories should include:

- the originator of the deliverable;
- the approver (that is, the person who professionally accepts the technical work in the deliverable); and
- the authoriser (that is, the person who is managerially responsible, normally the Project Manager).

12.7.5 Safety documentation

This section should specify whether an incremental or non-incremental Safety Case is to be used and list the safety documentation to be produced. It should also specify when it is to be produced and the personnel to be responsible for producing it. This section should provide or reference a specification of the form, content, distribution and required endorsement for each document.

12.7.6 Safety engineering

This section should specify mainstream engineering steps that are being taken to reduce risk (such as redundancy, protection systems, fail-safe design principles). The engineering activities specified should be appropriate to the Safety Integrity Level of the system.

For each phase of the project, this section should identify the methods to be used, describe how traceability, verification and validation will be addressed and identify the documentation to be produced. Each phase should be concluded with a planned verification activity (for example a programme of testing, a review or an inspection). Appendix C provides checklists for further guidance.

If the details above are specified in a separate quality plan, then this section should just refer to that plan.

The provision of specific engineering guidance is beyond the scope of this guidance. The Project Manager should draw on his engineering experience and competence to determine the appropriate engineering tasks for a particular project, and on best practice engineering as defined in the relevant standards.

This section should describe how a Data Reporting Analysis and Corrective Action System (DRACAS) will be implemented. This is a system for reporting, collecting, recording, analysing, investigating and taking timely corrective action on all incidents. It should be applied from the point at which a version of the system approximating to the final, operational version is available until the system is decommissioned. It should be used by suppliers, although the supplier may implement their own DRACAS. Appendix E describes a DRACAS.

12.7.7 Validation of external items

This section should specify adequate controls to ensure that the risk arising from safety-related external items (such as tools, equipment and components that have been previously developed or purchased) has been reduced to an acceptable level.

This section should specify an approval procedure for the use of external items. The procedure should include the following steps:

- 1 determine the extent to which the item in question will be used in a safety-related manner;
- 2 obtain all documentation relevant to the item;
- 3 assess the documentation;
Note: Railway Group Code of Practice GK/RC/0701 [F.10] has an example checklist in figure E1 which may be of value in guiding this assessment.;
- 4 identify the item's capabilities and limitations with respect to the project's requirements;
- 5 test the item's safety-related features both with, and independent to, the new system;
- 6 perform a risk assessment of the use of the item;
- 7 perform a Safety Assessment of the supplier of the item.

The use of external items not subject to such an approval procedure should be justified in the Safety Plan. Non-approval may be justified in the following cases:

- non-safety-related items justified as such by the reference to the Hazard Log;
- items for which there is extensive operational experience under the same conditions as the current system or equipment; or
- items for which the relevant railway authority has granted safety approval in the application in question.

A similar procedure should apply to approving the upgrade or modification of previously approved external items already in use on the project.

This section should describe the means for ensuring that any tools and equipment, on which safety relies, have been approved. It should specify any analyses, tests or demonstrations by the supplier of any external items that are carried out to satisfy the approval procedure requirements listed above. It should also identify personnel responsible for approving the specified approach to evaluating previously developed or purchased components.

12.8 Related guidance

Chapter 2 provides further guidance on safety roles and responsibilities.

Chapter 3 discusses the topic of a Safety Culture.

Guidance on performing the safety analysis activities described by the Safety Plan is provided in chapters 7 through 10.

Chapter 9 provides guidance on Safety Integrity Levels.

Chapter 11 provides guidance on the safety lifecycle.

Chapter 13 provides guidance on Safety Documentation.

Chapter 14 deals with the independent professional review of the Safety Plan.